УДК 621.396.6.019.3 + 004.056 Вестник УрФО № 2(28) / 2018, с. 5–10

Колкк А. А.

РАДИОЭЛЕКТРОННАЯ БОРЬБА В ИНФОРМАЦИОННОМ ПРОТИВОБОРСТВЕ

В статье показана необходимость совершенствования средств радиоэлектронной борьбы в целях обеспечения выполнения задач информационного противоборства. Рассмотрены вопросы применения элементов искусственного интеллекта в системах распознавания типов радиоэлектронных средств (РЭС). Дано понятие «нечеткого» распознавания типа радиоэлектронных средств.

Ключевые слова: *информационная война, комплексы радиоэлектронного подавления, нечёткая логика, оптимальная фильтрация.*

Kolkk A. A.

ELECTRONIC WARFARE IN INFORMATION CONFRONTATION

Need of improvement of means of radio-electronic fight for ensuring performance of problems of information confrontation is shown in article. Questions of application of elements of artificial intelligence in the systems of recognition of types of radio-electronic means (RES) are considered. The concept of "fuzzy" recognition like radio-electronic means is given.

Keywords: *information war, complexes of radio-electronic suppression, fuzzy logic, optimum filtration.*

Информационное противоборство. Развитие мирового сообщества наглядно демонстрирует, что в последнее время критически важным государственным ресурсом, оказывающим все большее влияние на национальную безопасность, становится информация, циркулирующая в автоматизированных системах управления и связи. Данные системы являются неотъемлемым компонентом структуры управления государством, экономикой, финансами и обороной.

В сложившейся обстановке ряд развитых западных государств, и в первую очередь США, в начале 90-х годов вплотную приступили к изучению и проработке проблем, связанных с противоборством в информационной сфере, или так называемой «информационной войной» (ИВ) [1].

«Информационная война» – это комплексное воздействие на систему государственного и военного управления противостоящей стороны, ее политическое и военное руководство, которое уже в мирное время приводило бы к принятию благоприятных решений в интересах государства, а в ходе войны полностью парализовало структуру

управления противника. В ИВ кроме наступательной составляющей не менее важной является необходимость обеспечить надёжную защиту своей информационной структуры [2].

Победа в информационной войне иногда даже более значима, чем на поле боя. Множество вооружённых конфликтов начиналось с информационного противостояния. Первым этапом, которого являлась подготовка мировой общественности о необходимости решения «назревших проблем» в деятельности какого-либо государства, путём вброса дезинформации в мировые СМИ о нарушение данным государством существующих договоров, демократических основ, нарушение прав меньшинств и т.д. (Ирак, Ливия, и др.) Пропаганда со стороны США своей политики, насаждение своего понимания демократии, вмешательство во внутренние дела государств, применение вооружённых сил без санкции ООН – всё это требует ответных действий в информационной сфере со стороны России и других государств.

После окончания боевых действий информационная война продолжается и результат её иногда даже более важен, чем победа в вооружённом конфликте.

В наши дни мы являемся свидетелями того, что наряду с термином информационная война всё чаще применяется словосочетание «гибридная война» Это понятие отражает имеющиеся в наличии реалии применения инструментов борьбы и последних достижений в сфере соперничества стран.

«Гибридная война» – вид военного противоборства отдельных государств, которое вовлекает в вооруженный конфликт, кроме или вместо регулярной армии – спец миссии и спецслужбы, партизанские и наемные силы, террористические атаки, протестные массовые беспорядки [3]. При этом основной целью чаще всего является не оккупация и присвоение территории, а перемена политического режима или устоев государственной политики в стране, подвергаемой атаке. В качестве примера можно привести международные события последнего десятилетия (события вокруг Сирии, Украины).

Использование радиоэлектронных средств и ВТ может обеспечить военное превосходство на поле боя и нарушить все сферы жизни общества. Специалисты ставят средства информационной войны (ИВ) на второе место после оружия массового поражения (ОМП) по степени их разрушительного действия. Зарубежные эксперты считают, что в настоящее время нет готовых решений в организации надежной защиты от возможных средств радиоэлектронного воздействия.

Воздействие на радиоэлектронные объекты информационных систем противника осуществляется двумя путями – электромагнитным излучением и воздействием на информационные базы данных и специальное программное обеспечение ЭВМ в АСУ войсками и оружием. Обеспечивается традиционным оружием – средствами РЭБ.

Меры по обеспечению ИБ становятся все более необходимыми по мере расширения использования компьютеров и компьютерных сетей. Структура компьютерных сетей сейчас настолько сложна, что практически отсутствует возможность уверенно идентифицировать всех, имеющих к ним доступ.

Если противник выберет в качестве объекта атаки не военные, а незащищенные гражданские сети и банки данных, то последствия будут катастрофическими. Более 90% потоков передачи данных и телефонных разговоров Министерства обороны различных государств, в том числе США идет по гражданским системам телефонной связи. Весьма значительными могут быть также и экономические потери от информационной атаки на телефонные системы.

Роль и место радиоэлектронной борьбы в информационном противоборстве. Насыщенность радиоэлектронного оборудования (РЭО) в системах управления оружием, в том числе и высокоточного оружия (ВТО), повышает значимость РЭБ как вида боевого обеспечения. Спектр задач РЭБ расширяется и, сливаясь с другими боевыми задачами, ведет к перерастанию РЭБ в «информационную войну».

Анализ основных тенденций развития вооруженной борьбы позволил установить, что 30% рассматриваемых сегодня задач информационного противоборства мирного времени и не менее 60% задач военного времени взаимосвязаны с задачами, традиционно решаемыми радиоэлектронной борьбой. В большей степени, чем раньше, пересекаются объекты информационного воздействия и радиоэлектронной борьбы, так как первооснову перспективных информационных систем составляют радиоэлектронные средства – традиционные объекты РЭБ, следователь-

но, одно из доминирующих мест в информационном противоборстве принадлежит радиоэлектронной борьбе.

Целями радиоэлектронной борьбы в системе информационного противоборства являются:

– дезорганизация функционирования информационных систем противника, обеспечение устойчивой работы своих информационных систем;

– снижение возможностей противника по сбору информации о войсках, объектах базирования ВС, информационных системах с помощью технических средств.

В мирное время цели РЭБ это завоевание и удержание превосходства в информационной сфере, а в военное время – повышение эффективности боевых действий войск. Возникает необходимость совершенствования средств радиоэлектронного подавления (РЭП). Развитие средств РЭП идет в тесном взаимодействии с развитием радиоэлектронной техники и характеризуется постоянной технической и научной конфронтацией. Любое совершенствование радиоэлектронной техники, связанное с повышением ее эффективности, надежности и помехоустойчивости, вызывает ответную реакцию в области РЭП.

Перспективные радиоэлектронные системы снабжаются устройствами искусственного интеллекта, позволяющими в процессе работы анализировать электронную обстановку и вырабатывать наиболее оптимальные решения в отношении режимов работы.

Вместе с тем, используемая в современных системах (РЭП) логика управления обычно ограничивается заданными, (фиксированными) алгоритмами, которые при появлении новых, прогрессивных радиоэлектронных средств часто становятся бесполезными. Отсюда вытекает необходимость применения искусственного интеллекта в организации систем РЭП, в том числе бортовых, работающих в реальном режиме времени. Поэтому в перспективное оборудование РЭП желательно включать устройства, которые бы обладали способностью самообучения и подстройки алгоритмов в соответствии с изменяющейся обстановкой.

Одним из вариантов применения искусственного интеллекта в организации работы бортового комплекса РЭП является применение теоретических основ и прикладных методов современного научного направления – нечёткой логики.

Областью внедрения алгоритмов нечеткой логики являются всевозможные экспертные системы, в том числе: контроль над производственными процессами, самообучающиеся системы, исследование критических ситуаций; ***распознавание образов*** и др.

В отличие от традиционной математики, требующей на каждом шаге моделирования точных и однозначных формулировок закономерностей, нечеткая логика предлагает иной уровень, подход, при котором постулируется лишь минимальный набор закономерностей.

Нечеткие числа, получаемые в результате «не вполне точных измерений», во многом аналогичны распределениям теории вероятностей. В пределе, при возрастании точности, нечеткая логика приходит к стандартной, Булевой. По сравнению с вероятностным методом, нечеткий метод позволяет резко сократить объем производимых вычислений, что, в свою очередь, приводит к увеличению быстродействия нечетких систем.

Для комплексов РЭП одним из важных элементов является система радиотехнической разведки. Основной задачей данной системы является распознавание типа облучающей РЛС, т.е. идентификация объекта (РЛС). Решение данной задачи предполагается комплексированием методов фильтрации Калмана и нечёткой логики (НЛ).

На рис.1 представлена структурная схема станции радиотехнической разведки, использующей комплексирование методов ОФК и НЛ.

Пусть в некотором районе (информационном пространстве) обнаружена работа группы радиоэлектронных средств. Для каждого известного РЭС в соответствующей базе данных определены диапазоны возможной перестройки частоты и другие параметры. Для использования аппарата оптимальной фильтрации необходимо разработать динамико-стохастическую модель процесса эволюции параметров и модель процесса измерения [4].

Уравнения записываются для каждого типа РЭС из базы данных, и формируется так называемый банк фильтров Калмана. Обработка принятых сигналов происходит параллельно. Фильтр, параметры которого соответствуют принятому сигналу, даёт сходящуюся оценку при минимуме ковариационной матрицы и невязки (обновляющего процесса).

Для разрешения ситуации неопределенности, когда координаты вектора измерения

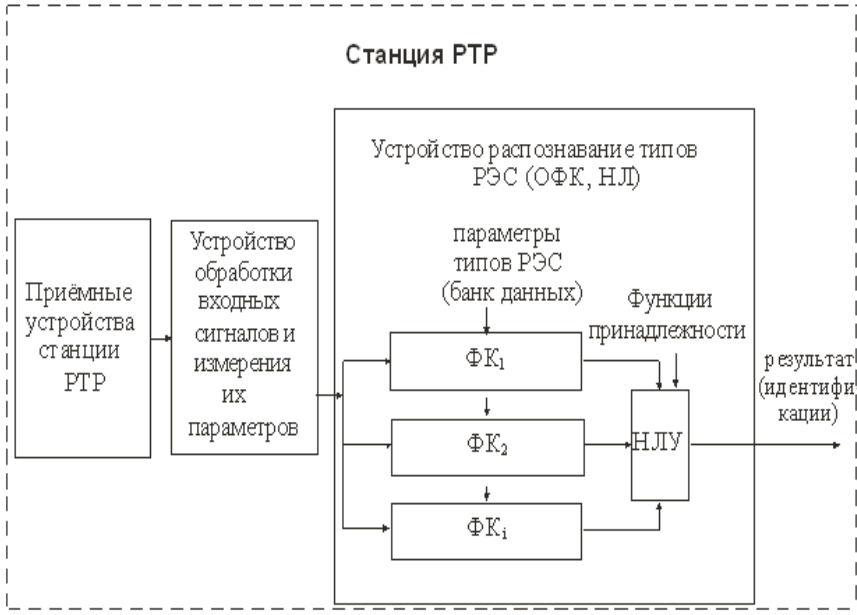

Рис. 1. Структурная схема станции радиотехнической разведки с устройством распознавания типов, использующего комплексирование методов ОФК и НЛ

попадают одновременно в несколько областей предполагаемых РЭС предлагается использовать методы нечёткой логики.

Рассмотрим понятие «нечеткой» идентификации объекта, как следствие, «нечеткого» распознавания типа РЭС, которое понимается как попадание вектора состояния в пространство принадлежности РЭС, относящееся к 2 типам РЭС одновременно. Понятие нечеткой идентификации объекта достаточно хорошо отражает сложившийся на практике экспертный подход [4]. Действительно, эксперт, руководствуясь значением вектора состояния, который определяет принадлежность к тому или иному типу, может считать, что объект принадлежит к типу А или принадлежит к «другому» типу, если значение вектора состояния находится вне пространства принадлежности данному РЭС. Причем в зависимости от конкретного значения разности между измеренными параметрами вектора состояния и параметрами, заложенными в банке экспертов для данного типа, можно считать, что объект принадлежит к типу А или не принадлежит данному типу соответственно в разной степени [5].

Определим нечеткую идентификацию объекта по вектору состояния как лингвистическую переменную, характеризующуюся, например, двумя термами (нечеткими множествами) – тип А или «другой» тип, которые описываются соответствующими функциями принадлежности $\mu^0_{v_i}$ и $\mu^1_{v_i}$.

На рис.2 приведена иллюстрация понятий «четкой» (а) и «нечеткой» (б) идентификации объекта. В первом случае области значений вектора состояния *xi*, соответствующие типу А и не соответствующие типу А (на рисунке они обозначены прямоугольниками разной окраски), разделены четкой границей. Во втором случае эти области пересекаются (область пересечения отмечена штриховкой) и описываются соответствующими функциями принадлежности с параметрами «a» и «b». В результате при любом значении вектора $x = xi$ состояние процесса (распознавания) может быть соотнесено как с нечетким множеством типа А ($\mu^0_{v_i} = 0{,}8$) , так и с нечетким множеством, не принадлежащим типу А ($\mu^1_{v_i} = 0{,}3$).

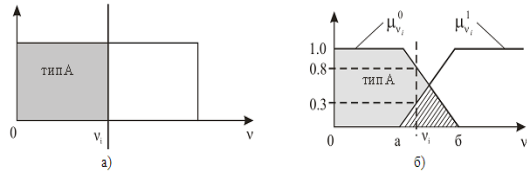

Рис.2. Иллюстрация понятий а) «чёткой» и б) «нечёткой» идентификации объекта

Заметим, что в настоящей работе рассмотрение ограничено использованием кусочно-линейных функций принадлежности, таких как трапецеидальная, треугольная и в данном случае Z- образная

Предполагается, что невязка *vi, i=0,N*, формируемая на выходе *i*-го фильтра Калма-

$$\mu^0_{\nu_i} = \begin{cases} 1. & 0 \le f \le a. \\ \dfrac{b-f}{b-a}. & a \le f \le b. \\ 0. & äðóãîå \end{cases} \quad \mu^1_{\nu_i} = \begin{cases} 0. & 0 \le f \le a. \\ \dfrac{f-a}{b-a}. & a \le f \le b. \\ 1. & äðóãîå \end{cases}$$

на (ФК), может быть представлена лингвистической переменной, например, с двумя термами – «малая» и «большая», для которых заданы функции принадлежности $\mu^0_{\nu_i}$ и $\mu^1_{\nu_i}$ *i= 0, N* [6].

Терм «малая» соответствует ситуации, когда на выходе фильтра невязка мала, т.е. измеренный вектор состояния близок вектору состояния предполагаемого типа РЭС. Появление хотя и малого, но не нулевого значения этой невязки объясняется переходными процессами, сопровождающими оценивание, отсутствием на практике полной адекватности используемой при синтезе наблюдателя модели системы распознавания, неучтенными возмущениями ее динамики или выхода. Терм «большая» соответствует ситуации, когда измеренный вектор состояния, существенно отличается от вектора состояния ФК і-го наблюдателя. Так бывает, если, например, на вход ФК і-го наблюдателя поступает сигнал с параметрами присущими j–му наблюдателю. При этом параметры *{ai,bi | i = 0,N}* функций принадлежности определяются равенствами:

$$a_i = \min_i \left\{ \nu_i \middle| S_j, j \ne i \right\},$$

$$b_i = \max_i \left\{ \nu_i \middle| S_j, j = i \right\}$$

С помощью элементов нечёткой логики в программных средах MatLab (расширение Fuzzy Logic Toolbox) и FuzzyTECH создана нечёткая модель «Распознавание типов РЭС», основанная на базе знаний экспертов, учитывающая изменения оперативной обстановки и появление новых РЭС, а также позволяющая принимать решение по каждому полученному сигналу (измеренным его параметрам).

Совершенствование комплексов РЭП, в том числе методами нечёткой логики, необходимо для поддержания паритета в области ИВ (гибридных) и, далее обеспечить преимущество в ведении информационного противоборства, в решении его задач по дезорганизации функционирования систем управления и защите своих аналогичных систем.

Литература

1. Гриняев С. Н. Взгляды военных экспертов США на ведение информационного противоборства/ С. Н. Гриняев //Зарубежное военное обозрение, 2001. – № 8. – С. 10–12.

2. Жуков В. Взгляды военного руководства США на ведение информационной войны. / В. Жуков. //Зарубежное военное обозрение, 2001. – № 1. – С. 2–9.

3. Позубенков П. С., Позубенков С. П. Гибридные войны в современном информационном пространстве /П. С. Позубенков // Научно-методический электронный журнал «Концепт», 2016. – Т. 11. – С. 1121–1125.О.

4. Горнов А.Ю., Даровских С.Н., Жолудев А.И., Тятюшкин А.И., Хаютин М.И., Ширяев В.И. Опыт применения пакета прикладных программ к задаче оптимального управления маневрирующим летательным аппаратом. //Интеллектуализация программных средств. – Новосибирск: Наука. Сиб. Отд-ние, 1990. – С. 152-160.

5. Безмен Г.В., Колесов Н.В. Функциональное диагностирование динамических систем с использованием нечетких правил анализа и принятия решений об отказе / Г.В. Безмен // Известия РАН. Теория и системы управления, 2011. – № 3. – С. 3–12.

6. Колкк А.А., и др. Об алгоритмах распознавания типов радиоэлектронных средств в бортовых комплексах разведки: сб. науч. ст. по материалам II Всероссийской НПК «АВИАТОР» (11-13 февраля 2015г.) Актуальные вопросы исследований в Авионике: теория, обслуживание, разработки: В 2-ух т. Т.2. Воронеж: ВУНЦ ВВС «ВВА», 2015. – С. 86-92.

References

1. Grinyaev S. N. Vzglyady voennyh ehkspertov SSHA na vedenie informacionnogo protivoborstva/ S. N. Grinyaev //Zarubezhnoe voennoe obozrenie, 2001 – no 8. – pp. 10–12.

2. Zhukov V. Vzglyady voennogo rukovodstva SSHA na vedenie informacionnoj vojny. / V. Zhukov. // Zarubezhnoe voennoe obozrenie, 2001. – no 1. – pp. 2–9.

3. Pozubenkov P. S., Pozubenkov S. P. Gibridnye vojny v sovremennom informacionnom prostranstve /P. S. Pozubenkov // Nauchno-metodicheskij ehlektronnyj zhurnal «Koncept», 2016. – vol. 11. – pp. 1121–1125.

4. Gornov A.YU., Darovskih S.N., Zholudev A.I., Tyatyushkin A.I., Hayutin M.I., Shiryaev V.I. Opyt primeneniya paketa prikladnyh programm k zadache optimal'nogo upravleniya manevriruyushchim letatel'nym apparatom. //Intellektualizaciya programmnyh sredstv. – Novosibirsk: Nauka. Sib. Otd-nie, 1990. – pp. 152-160.

5. Bezmen G.V., Kolesov N.V. Functional Diagnosis of Dynamic Systems Using Fuzzy Rules Analysis and Decision Making on Refusal/ G.V Bezmen //Izvestiya RAN. Theory and Control Systems, 2011. – no. 3. – pp. 3–12.

6. Kolkk A.A., i dr. Ob algoritmah raspoznavaniya tipov radioehlektronnyh sredstv v bortovyh kompleksah razvedki: sb. nauch. st. po materialam II Vserossijskoj NPK «AVIATOR» (11-13 fevralya 2015g.) Aktual'nye voprosy issledovanij v avionike: teoriya, obsluzhivanie, razrabotki: v 2-uh t. vol.2. Voronezh: VUNC VVS «VVA», 2015. – pp. 86-92.

КОЛКК Андрей Александрович, преподаватель 13 кафедры авиационных комплексов и конструкции летательных аппаратов филиала ВУНЦ ВВС ВВА в 454015 г. Челябинск, E-mail: kandidatyra@mail.ru

KOLKK Andrey, lecturer of the Department of 13 aircraft systems and aircraft design branch VUNTS VVS VVA 454015 in Chelyabinsk. E-mail: kandidatyra@mail.ru