Математическая модель алгоритмического обеспечения перспективных изделий запрос-ответной аппаратуры

П. И. Тутубалин[1], С. В. Новикова[2], А. Ю. Александров[3]
Казанский национальный исследовательский технический университет им. А.Н.Туполева-КАИ
[1]ptyt@ya.ru, [2]sweta72@bk.ru, [3]uralex86@mail.ru

***Аннотация*. В статье рассматриваются основополагающие принципы создания и функционирования систем опознавания нового поколения. Определяются принципы повышения достоверности принятия решений по опознаванию различных объектов. Приводится алгоритмика модели использования протокола с открытыми сеансовыми ключами при эксплуатации перспективной запросной и ответной аппаратуры.**

Ключевые слова: анализ; модель системы; открытый ключ; проектирование; защита информации; запрос-ответная аппаратура

I. Введение

В настоящее, как и ранее, существует задача решение которой претерпевает изменения в ходе развития современной науки и техники – это задача проектирования и разработки перспективных образцов изделий запрос-ответной аппаратуры.

При том нужно отметить, что такого рода изделия получили своё распространение не только в сфере военных и оборонных технологий, но также и в сфере гражданских технологий, например, технологий, касающихся проведения электронных платежей через интернет или гражданских пассажирских и грузоперевозок.

Это требует при проектировании и разработке новых образцов такой техники специальных подходов, основополагающих принципов, отличных от существующих на сегодняшний день. Такого рода разработки естественно вести на основе использования надёжно зарекомендовавших себя математических моделей и методов.

Естественно заявить, что рассматриваемый круг задач выводит на необходимость построения достаточно сложных моделей систем и естественно процессов, которые протекают в них. Заслуживающие внимания подходы к моделированию сложных систем, приводятся, например, в работе [1] посвящённой исследованию вопроса построения модели нейронной сети для мониторинга газотурбинных двигателей, в работе [2], отражающей решение вопросов связанных с моделированием работы систем массового обслуживания.

Язык жизненных обстоятельств даёт ясно понять, что в любых современных системах, следует применять достаточно надёжные средства защиты информации. Естественно, что если заходит речь об образцах запрос-ответной аппаратуры и тех обстоятельствах, в которых они используются, то становится невозможно обойти вниманием необходимость применения надёжных средств и подходов к обеспечению информационной безопасности.

Для решения обозначенных задач обеспечения безопасности будет полезным обратить внимание на следующую работу [3], в которой рассмотрены вопросы по применению криптографии в практической деятельности, также заслуживают внимания подходы и методы, отмеченные в работах [4] и [5].

В настоящее время ясно обозначилась необходимость разработки системы опознавания нового поколения. Очевидно, что в основе такой разработки должны лежать, прежде всего, единообразно понимаемые принципы, которые обеспечили бы длительное и эффективное функционирование разрабатываемой системы.

Перечислим и поясним эти принципы.

II. Принципы функционирования системы системы опознавания нового поколения

Пойдем в их перечислении от более общих и важных к относительно частным и второстепенным в смысле очерёдности в последовательности их учёта при осуществлении работ по проектированию и разработке систем опознавания нового поколения.

1. Использование при опознавании тех или иных объектов данных, получаемых от возможно большего количества существующих средств опознавания и использование этих данных в совокупности.

2. Повышение достоверности принятия решений по опознаванию тех или иных объектов путём использования специальных алгоритмов цифровой обработки поступающей в систему комплексной информации.

3. Использование в составе аппаратуры опознавания современных микропроцессорных средств для параллельной обработки первичной и вторичной

информации в совокупности с цифровыми каналами обмена данными.

4. Применение специальных программно-аппаратных средств для обеспечения помехозащищённости и открытости работы средств системы.

5. Создание с помощью средств системы единого информационного пространства опознавания в текущей области функционирования системы с широкими возможностями прямого защищённого доступа к нему всех «своих» потребителей информации опознавания.

6. Использование единой (унифицированной) программируемой аппаратуры опознавания, обработки и выдачи информации для воздушных, наземных и надводных и подводных носителей.

7. Широкое использование при создании системы блочно-модульного принципа построения аппаратуры и магистрально-модульного принципа обмена данными с использованием интерфейсов, применяемых в перспективных образцах запрос ответной техники.

Учитывая современный научно-технический уровень и оценивая перспективные возможности развития электронной, радиоэлектронной и др. техники, можно выделить основные способы реализации перечисленных принципов:

1. Определение полного перечня источников входной информации и потребителей результатов работы системы.

2. Описание характеристик входных сигналов системы от существующих и перспективных источников информации.

3. Разработка требований к сигналам, выдаваемым системой существующим и потенциальным потребителям информации опознавания с учётом существующих и перспективных каналов связи с ними.

4. Разработка математических методов и быстродействующих алгоритмов:

- кодирования запросных сообщений и декодирования ответных сообщений;
- принятия решения «свой-чужой» с использованием байесова подхода, принципов "голосования", гарантированного результата, экспертных систем и других подходов для повышения достоверности опознавания;
- формирования выходной информации блоков и модулей аппаратуры опознавания с учётом выбранных интерфейсов внутриаппаратного обмена информацией и выдачи результатов опознавания потребителям;
- отображение информации опознавания на терминалах аппаратуры системы и её пользователей в том числе с использованием электронных карт воздушной, наземной и надводной обстановки в текущей области функционирования системы;
- защиты входной, промежуточной и выходной информации системы от действия пассивных помех, несанкционированного доступа и активного противодействия её нормальному функционированию;
- контроля и диагностирования состояний системы в процессе её подготовки, функционирования и проведения технического обслуживания.

5. Разработка унифицированной программируемой аппаратуры опознавания на базе современных отечественных микропроцессорных средств высокой производительности для установки на воздушные, наземные, подводные и надводные объекты, включающей в себя:

- антенные системы на базе фазированных антенных решёток;
- программируемые приёмники/передатчики широкополосных сигналов;
- микропроцессорные модули сбора и обработки информации опознавания, управления функционированием аппаратуры, контроля и диагностирования состояний её компонент;
- программируемые блоки приёма/передачи данных в требуемых форматах от/на поставщиков/потребителей информации опознавания.

6. Определение правил построения и структуры реконфигурируемой в режиме реального времени информационно-вычислительной системы опознавания.

Неотъемлемой частью создания системы опознавания нового поколения является разработка перспективной запрос-ответной аппаратуры (ЗОА).

Основными требованиями к перспективной ЗОА являются следующие:

- малые габариты и энергопотребление;
- высокая гибкость, позволяющая оперативно сменять методы и средства кодирования применяемых в системе опознавания сигналов;
- высокая помехозащищённость и имитостойкость;
- возможность циркулирования в системе дополнительной информации, кроме «свой-чужой», и как следствие этого – обеспечение удобного интерфейса с другими системами соответствующего образца запросно ответной техники.

Рассмотрим пути эффективной реализации перечисленных требований.

III. Структурные схемы запрос-ответной аппаратуры

Для реализации представленных требований в перспективной ЗАО должны найти широкое применение

современные микропроцессорные средства и системы. Одним из основных направлений использования микропроцессоров является создание на их основе основного блока ЗОА – микропроцессорного блока (МПБ), осуществляющего кодирование/декодирование запросных и ответных сигналов, а также управление другими блоками аппаратуры.

Перспективная аппаратура (ЗАО) должна включать в себя:

- запросчик, представляющий собой специальную радиолокационную станцию (РЛС), работающую в импульсном режиме;
- ответчик, являющийся специальным приемопередатчиком.

Согласно новым задачам, стоящим перед перспективной ЗОА в составе запросчика наряду с традиционными блоками: антенна передатчика (АПРД); передатчик (ПРД); антенна приёмника (АПРМ); приёмник (ПРМ); пульт ввода и отображения информации (ПВОИ). Должны быть предусмотрены такие новые блоки, как приёмник спутниковой системы навигации GPS/ГЛОНАСС (ПРМ ССН) и блок интерфейса с внешними системами (БИВС).

Отметим, что при необходимости микропроцессорные средства могут встраиваться в состав традиционных блоков запросчика. Структурная схема перспективного запросчика представлена на рис. 1.

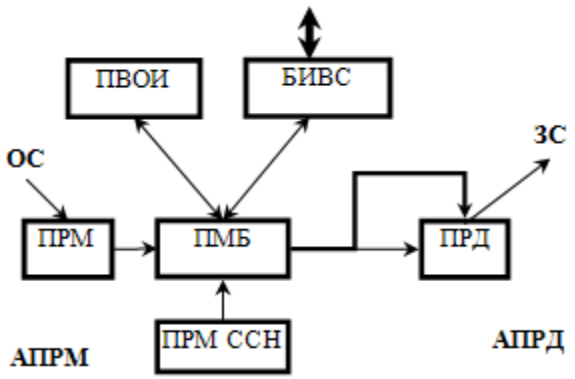

Рис. 1. Структурная схема перспективного запросчика

В состав ответчика наряду с такими традиционными блоками, как ПРМ, ПРД и ПВОИ включаются антенный переключатель (АП) и блок ПРМ ССН. Первый используется для реализации через одну антенну приёма запросных сигналов (ЗС) и передачи ответных сигналов (ОС).

Блок ПРМ ССН необходим для автоматического определения координат ответчика с их последующим включением в состав ОС. Структурная схема перспективного ответчика представлена на рис. 2.

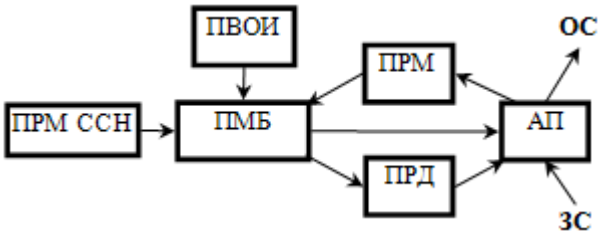

Рис. 2. Структурная схема перспективного ответчика

Для некоторых образцов возможно создание совмещённого запрос-ответчика, структурная схема которого приведена на рис. 3.

Здесь ПРМ и ПРД – соответственно приёмник для получения ОС и ЗС от других запросчиков, а также двухрежимный передатчик для ЗС и ОС. Для синхронизированной передачи этих сигналов используется специальная антенна (АПРД) запрос-ответчика.

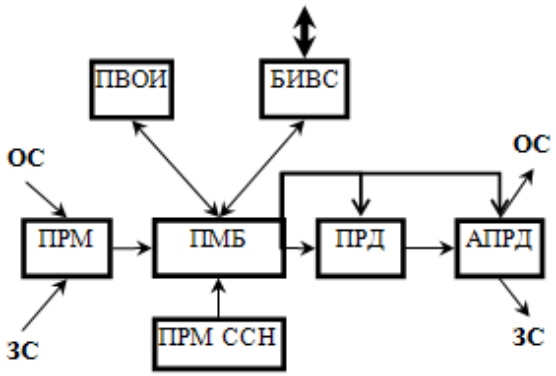

Рис. 3. Структурная схема совмещённого запросчика и ответчика

Перспективная ЗОА должна быть построена по магистрально-модульному принципу, при котором все блоки аппаратуры (Бл. 1… Бл. 6) взаимодействуют по мультиплексному каналу информационного обмена (МКИО). Общая структура рассмотренных выше типов ЗОА приведена на рис. 4.

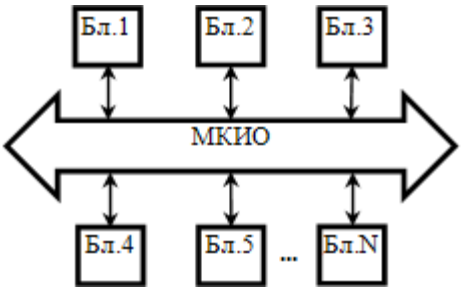

Рис. 4. Общая структура рассматриваемых типов запросной и ответной аппаратуры

IV. Алгоритмы функционирования перспективной запрос-ответной аппаратуры

В связи с тем, что основным модулем в образцах ЗОА является микропроцессорный блок, рассмотрим общие

алгоритмы его работы в составе запросчика, ответчика и запрос-ответчика.

A. Алгоритм работы запросчика

1.°Контроль работоспособности изделия.

2. Ввод исходных данных для кодирования ЗС и декодирования получаемых ОС.

3. Получение от ПРМ ССН данных о местоположении запросчика.

4. Кодирование ЗС в соответствии с данными п. 2°.

5. Включение и работа АПРД.

6. Включение ПРД и передача ему закодированных данных по ЗС.

7. Работа ПРД.

8. Блокировка ПРД и включение ПРМ.

9. Прим ОС и блокировка ПРМ.

10. Декодирование ОС.

11. Обработка информации и принятие решения по каждому отдельному объекту.

12. Вывод решений на ПВОИ и(или) через БИВС на ЭВМ внешних систем.

13. Переход к п. 3° до выключения изделия.

B. Алгоритм работы ответчика

1. Встроенный контроль работоспособности блоков изделия.

2. Ввод данных для декодирования ЗС и кодирования ОС.

3. Приём данных о местоположении от ПРМ ССН.

4. Включение ПРМ.

5. Приём и декодирование ЗС.

6. Кодирование ОС.

7. Включение ПРД.

8. Излучение ОС.

9. Ввод и передача дополнительной информации.

10. Переход к п. 3° до выключения изделия.

C. Алгоритм работы запрос-ответчика

1. Встроенный контроль работоспособности.

2. Ввод данных для кодирования и декодирования запросных и ответных сигналов.

3. Приём информации о местоположении от ПРМ ССН.

4. Включение ПРМ.

5. Приём поступающих сигналов.

6. Распознавание принятых сигналов

7. Работа в режиме ответчика, если принятые сигналы являются запросными и в режиме запросчика при наличии ответных сигналов.

8. Включение ПРД и излучение соответственно ответных или запросных сигналов.

9. Переход к п. 3° до выключения изделия.

При этом этап 7° алгоритма реализуется с помощью последовательности действий, приведённых в алгоритм работы запросчика.

Использование более эффективных по достоверности алгоритмов опознавания объектов и применение гибкой и более стойкой системы кодирования и декодирования запросной и ответной информации может быть обеспечено использованием протокола открытых сеансовых ключей.

Достаточно хорошее приближение к выполнению требований абсолютной стойкости дают криптографические протоколы с сеансовыми ключами [3].

V. Выводы

В статье предложен метод использования протокола с открытыми сеансовыми ключами при эксплуатации перспективной запросной и ответной аппаратуры и отвечающие этому методу алгоритмы функционирования запросной и ответной аппаратуры.

Список литературы

[1] Novikova, S.V. Structural optimization of the neural network model for the gas turbine engine monitoring // Russian Aeronautics, 2016, Vol. 59, Is. 2, pp. 263-270 DOI:10.3103/S1068799816020185.

[2] Yakimov, I., Kirpichnikov, A., Mokshin, V., Yakhina, Z., Gainullin, R. The comparison of structured modeling and simulation modeling of queueing systems. Communications in Computer and Information Science (CCIS) volume 800. Springer. 2017. P. 256-267. DOI: 10.1007/978-3-319-68069-9_21.

[3] Alfred J.Menezes, Paul C. van Oorschot, Scott A. Vanstone. Handbook of Applied Cryptography. 1996.

[4] Information Security Practice and Experience. 12th International Conference, ISPEC 2016, Zhangjiajie, China, November 16-18, 2016, Proceedings.

[5] Tutubalin Pavel Innokentievich, Mokshin Vladimir Vasilevich. (2017) The Evaluation of the cryptographic strength of asymmetric encryption algorithms. 2017 Second Russia and Pacific Conference on Computer Technology and Applications (RPC), 25-29 Sept. 2017, Vladivostok, Russia. pp. 180–183. DOI: 10.1109/RPC.2017.8168094, Publisher: IEEE.