При восстановлении секрета участник предъявляет пару верифицируемых значений $\{e_i, s_i(x)\}$. Остальные участники протокола убеждаются в том, что:

$$(D_i(x))^{e_i} \equiv (S(x))^{d_i e_i} = S(x) \bmod p_i(x) = s_i(x),$$

$$g^{e_i} = E_i.$$

Построенный таким образом протокол верификации пороговой полиномиальной модулярной СРС работает про условии честности дилера, который корректно распределяет исходные и проверочные данные схемы. При этом, никакой участник не сможет предъявить неверные данные для проверки. Действительно, для того, чтобы подделать значение $s_i(x)$, ему также необходимо подобрать соответствующий ключ e_i, что невозможно сделать, поскольку это значение проверяется при помощи опубликованной дискретной экспоненты.

Обоснование стойкости протокола проверки. При публикации дилером дополнительных значений $\{D_i, E_i\}$ защищенность схемы может уменьшиться, поскольку при помощи этих данных участники могут попытатьсяполучить дополнительную информацию о значении $s(x)$. В частности, злоумышленник может попытаться сократить множество перебора значений $s(x)$. В самом деле,

$$s_i(x) = (D_i(x))^y \bmod p_i(x), y = 1,2,\ldots,k_i,$$

где k_i – порядок подгруппы, порожденной $D_i(x)$. Таким образом, частичный секрет $s_i(x)$ выбирается из множества мощности k_i. Для определения $s(x)$ требуется выбрать не менее t частичных секретов. Меньшее количество не дает информации о секрете в силу совершенности схемы [4]. Поскольку порядок подгруппы делит порядок группы, то для успешной атаки надо, чтобы $k_1 k_2 \ldots k_t < \left(MinDiv\left(2^n - 1\right)\right)^t$. А значит, для того чтобы отыскать секрет таким методом требуется перебрать не менее $\left(MinDiv\left(2^n - 1\right)\right)^t$ наборов $s_1(x) \cdot s_2(x) \ldots s_t(x)$. Однако, согласно условию (1) такой перебор не имеет смысла, поскольку значений основного секрета также $2^n - 1$. Таким образом, публикация значений $\{D_i\}$ не уменьшает защищенность схемы. Публикация $\{E_i\}$ не нарушает защищенность схемы при правильном выборе циклической группы.

Для того, чтобы определить, подходит ли набор неприводимых полиномов для построения протокола верификации, требуется проверить условие (1). Это зависит от факторизации чисел Мерсенна $2^n - 1$. Таблицы факторизации чисел такого вида известны, в частности, до $n < 1200$. Этого достаточно, чтобы удовлетворить условию (1). Очевидно, что наиболее подходящими для обеспечения стойкости опубликованных значений являются простые числа Мерсенна, т.е. числа вида $2^n - 1$, где n = 2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107, 127, 521, 607, 1279 и т.д. (см. [9]). Размер исходного ключа при этом целесообразно выбирать не менее 128 бит, а значит, $n \geq 127$. Порядок циклической группы для генерации значений $\{E_i\}$, в которой задача нахождения дискретного логарифма является вычислительно трудной, при этом должен быть не менее $2^{127} - 1$.

Заключение. В работе предложен протокол верификации частичных секретов пороговой полиномиальной модулярной схемы. Обоснована его криптографическая стойкость, в частности, указано, что перебор с участием опубликованных проверочных значений не дает преимуществ в сравнении с перебором исходных данных схемы. Указаны условия, при которых секрет схемы остается защищенным независимо от опубликованных значений.

СПИСОК ЦИТИРОВАННЫХ ИСТОЧНИКОВ

1. Asmuth C.A., Bloom J. A modular approach to key safeguarding // IEEE Transactions on Information Theory. – 1983. – Vol. 29. – P. 156–169.
2. Feldman P. A practical scheme for non-interactive verifiable secret sharing // IEEE Symposium on Foundations of Computer Science – 1987 – P. 427-437.
3. Galibus T. Matveev G. Generalized Mignotte Sequences in Polynomial Rings // ENTCS – 2007. – Vol. 186.
4. Galibus T. Matveev G. Shenets N. Some structural and security properties of the modular secret sharing // Proc. of SYNASC'08. – IEEE Comp. soc. press, Los Alamitos – 2009 – P. 197-200.
5. Iftene S. Secret sharing schemes with applications in security protocols. Technical Report TR 07-01 // University Alexandru Ioan Cuza of Iasi, Faculty of Computer Science. - 2007.
6. Kaya K., Selcuk A. A Verifiable Secret Sharing Scheme Based on the Chinese Remainder Theorem. // LNCS – 2008 – Vol.5365. – P.288-305.
7. Mignotte M. How to share a secret // Advances in cryptology – Eurocrypt'82, LNCS. – 1982. – P. 371–375.
8. Qiong L., Zhifang W., Xiamu N., Shenghe S. A non-interactive modular verifiable secret sharing scheme // Proc. of ICCCAS'05 – 2005 – Vol.1. – P. 84-87.
9. *The online encyclopedia of integer sequences: sequence* A000043 (*Mersenne primes)*, Available at: https://oeis.org/A000043 (accessed 19 November 2014).

Материал поступил в редакцию 23.12.14

GALIBUS T.V. **Verification of the participants of the polynomial modular secret sharing over the binary field**

We construct a verification of the shares of polynomial modular secret sharing in the case of the binary field. The verification is effective in the presence of honest dealer and malicious participants who wish to submit the false shares. The privacy of the verification is based on the perfectness of the threshold scheme and the hardness of discreet logarithm computation. We provide the restrictions on the degree of polynomials, field size and threshold that guarantee the privacy of the verification.

УДК 004.032.26,004.4

Ганченко В.В., Марушко Е.Е.

АРХИТЕКТУРА ПРОГРАММНОГО КОМПЛЕКСА ИДЕНТИФИКАЦИИ РЕЖИМОВ ФУНКЦИОНИРОВАНИЯ ПОДСИСТЕМ КОСМИЧЕСКИХ АППАРАТОВ

Введение. Программный комплекс (ПК) идентификации режимов функционирования подсистем космических аппаратов (КА) и детектирования нештатных и аварийных ситуаций является одним из основных структурных составляющих экспериментального образца нейросетевой системы мониторинга состояния и поведения подсистем космических аппаратов по телеметрическим данным (ЭО СМ СПКА) [1]. Основной его задачей является контроль за состоянием и режимами функционирования бортового оборудования на основе нейросетевых технологий

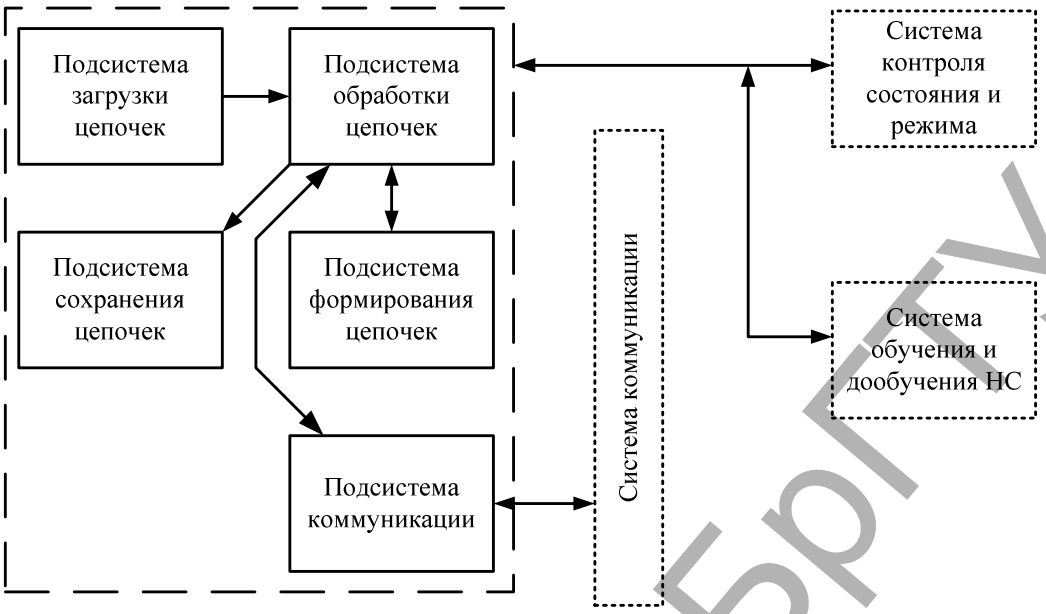

Рис. 1. Схема архитектуры ПК идентификации режимов функционирования подсистем КА и детектирования нештатных и аварийных ситуаций, штриховой линией определена система управления

обработки временных рядов значений телеметрических (ТМ) параметров (температуры давления жидкости и газа, электрического тока, положения и ориентации КА, уровня жидкости).

ПК предназначен для обеспечения контроля следующих подсистем КА:

- корректирующая двигательная установка;
- система энергетического обеспечения в составе солнечной батареи и аккумуляторной батареи;
- целевая аппаратура.

Основные системы ПК идентификации. Опираясь на выполняемые задачи, в составе комплекса выделяются следующие системы:

- контроля состояния и режимов функционирования бортового оборудования на основе нейросетевых технологий, на основе сегментации временного ряда значений ТМ-параметров, а также других методов и средств искусственного интеллекта;
- обучения искусственных нейронных сетей (НС) и их безопасного дообучения;
- управления, предназначенная для запроса данных и отправки результатов обработки, обмена запросами с другими ПК в составе ЭО СМ СПКА, управления процессом обработки, включая обучение и дообучение НС;
- коммуникации, предназначенная для взаимодействия с другими ПК в составе ЭО СМ СПКА.

Таким образом, архитектуру ПК анализа можно представить в виде, представленном на рисунке 1.

Система обучения и дообучения НС система предназначена для обучения и дообучения НС различного типа, используемых для обработки данных в системе контроля состояния и режима. Система содержит в себе набор реализаций НС, каждая из которых содержит функции для обучения, дообучения и переобучения НС. Помимо управления состоянием реализаций НС реализована связь с системой контроля состояния и режима, которая и использует имеющиеся НС.

Система управления предназначена для функционального связывания систем комплекса для выполнения различных задач обработки ТМ-информации. Система осуществляет передачу данных и параметров их обработки модулям, реализующим алгоритмы обработки. Сама обработка осуществляется на основе последовательного вызова модулей алгоритмов обработки. Для организации сложных алгоритмов обработки используются списки вызовов алгоритмов, представляющие собой цепочки описаний вызовов более простых алгоритмов с указанием параметров работы, а также данных, передаваемых на входы алгоритмов и получаемые в качестве результатов обработки.

Система контроля состояния и режимов функционирования бортового оборудования строится на основе НС и алгоритмов сегментации временного ряда значений ТМ-параметров (рис. 2).

Нейросетевые алгоритмы идентификации. Для осуществления идентификации состояний подсистем КА разработаны следующие алгоритмы:

- алгоритм обучения нейросетевых модулей системы идентификации состояний подсистем КА;
- алгоритм синтеза многослойного персептрона;
- алгоритм идентификации нештатных ситуаций с использованием нейронных сетей;
- алгоритм идентификации этапов функционирования подсистем КА с использованием нейронных сетей;
- алгоритм инкрементного дообучения нейросетевых модулей системы идентификации состояний подсистем КА.

На основе описания режимов функционирования и допустимых диапазонов значений датчиков, формируется обучающая выборка для модулей нейросетевой идентификации состояний систем КА.

В качестве предварительной обработки данных проводится регуляризация по времени не регулярно представленных данных, с использованием аппроксимации значений, либо кусочно-линейным образом.

Далее осуществляется преобразование исходных данных с учетом характера и типа проблемы, отображаемой нейросетевой моделью, и выбираются способы представления информации. Эффективность нейросетевой модели повышается, если диапазоны изменения входных и выходных величин приведены к диапазону [-1; 1].

При выборе алгоритма обучения:

1) Выполняется оценка сложности задачи, необходимого объема памяти и вычислительной сложности.
2) Проводится испытательное обучение НС по каждому алгоритму для общего набора данных, оценивается скорость обучения и точность результата.
3) На основании полученных характеристик производится выбор, предпочтение отдается алгоритму с достаточной точностью и высокой скоростью обучения.

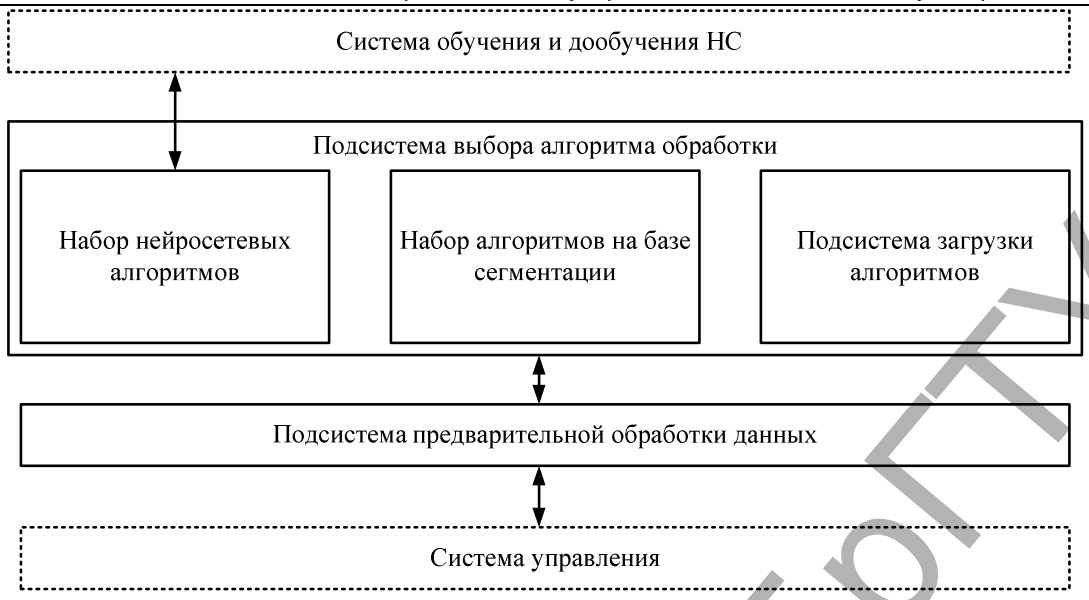

Рис. 2. Структура системы контроля за состояния и режима

Выбор алгоритма обучения НС зависит от многих факторов, включая сложность задачи, число элементов обучающего множества, число настраиваемых параметров сети и конечную ошибку [2, 3]. Для сетей, которые содержат до нескольких сотен параметров, алгоритм LM имеет самую быструю сходимость. Это преимущество особенно значимо, если требуется высокая точность обучения. Алгоритмы методов Ньютона и секущих плоскостей занимают следующее место для НС умеренных размеров. Алгоритм BFGS требует значительного объема памяти для хранения матрицы Гессе, но при этом значительно превосходит по быстродействию алгоритмы метода сопряженных градиентов. Алгоритм RPROP не требуют использования процедур одномерного поиска и предъявляют незначительные требования к памяти. Работает достаточно быстро и может быть использован для решения задач большой размерности.

При решении практических задач рекомендуется начинать с алгоритма LM. Если при этом требуется слишком много памяти, то следует перейти к алгоритму BFGS или одному из алгоритмов метода сопряженных градиентов. Далее применить алгоритм RPROP, который также характеризуется высоким быстродействием по сравнению с другими алгоритмами обратного распространения ошибки. Обучение подразумевает использование двух тестовых наборов обучающих данных, с финальной оценкой точности на валидационном наборе данных.

Формирование нейросетевых модулей производится для каждого режима подсистем КА. Автоматическое решение задачи нахождения субоптимальной структуры предлагают конструктивные алгоритмы синтеза НС [3]. Блок схема представлена на рисунке 3. При предположениях о репрезентативности обучающей выборки, возможной исходной избыточности набора независимых признаков задачи и старте синтеза структуры сети с минимального размера в качестве меняющих структуру НС операций предлагается следующий алгоритм синтеза нейронной сети:

1) Анализ параметров задачи (включая сложность задачи, число элементов обучающего множества) и выбор соответствующего алгоритма обучения НС.

2) Добавление нейрона в сеть

a) Создание сети увеличенного размера, замещающей исходную, или использование одного шага конструктивного алгоритма роста сети как способа одновременного автоматического нахождения того слоя НС, рост числа нейронов в котором приведет к максимальному улучшению точности решению задачи.
b) Обучение сети увеличенного размера.
c) Оценка ошибкой обобщения.
d) Повтор п.a, если не достигнуты необходимые свойства сети

3) Редукция некоторого числа избыточных синапсов или нейронов НС.

В п.2 изменение размера сети происходит:

a) при достижении асимптоты или локального минимума критериев Бартлетта или Мураты-Амари [3], характеризующих обобщающие свойства модели (при достижении минимума прогностической ошибки обобщения выполняется переключение на операции, снижающие избыточность НС).

b) при превышении ошибкой обобщения (рассчитанной на независимой тестовой выборке или на основе критериев Бартлетта или Мураты-Амари) заданного пользователем максимально допустимого уровня ошибок.

В коридоре между значениями максимально допустимых ошибок обучения или обобщения и нулевым уровнем таких ошибок и ведется адаптация структуры НС при заданных критериях вторичной оптимизации (требование минимизации числа нейронов и т.п.).

Нейросетевые модули, добавляемые в процессе функционирования на этапе дообучения, для одинаковых режимов организуются в ансамбли.

Ансамбль нейронных сетей – представляет собой набор нескольких одиночных НС, независимо решающих задачу. Частные решения одиночных НС поступают на обобщающий модуль (Gating module), который выдает окончательное решение.

В качестве обобщающего модуля, согласно алгоритму инкрементного дообучения, используется модуль взвешенного суммирования выходов отдельных нейронных сетей, веса при этом определяются на основании точности каждой нейронной сети [4].

Алгоритм идентификации этапов функционирования включает следующие шаги:

1. На основе данных массивов ТМ-информации формируется входной вектор X для обученных модулей нейросетевой идентификации набора.
2. На основе командно-программной информации и информации от подсистемы имитационного моделирования о текущем режиме определяется ансамбль модулей нейросетевой.
3. По входному вектору ансамблем вычисляется выходной вектор.
4. Из выходного вектора извлекается идентификатор этапа циклограммы.

Алгоритм инкрементного дообучения нейросетевых предназначен для обучения нейросетевых модулей в процессе функционирования, с целью учета изменений ТМ-информации со временем, вызванных дрейфом целевого значения Понятие дрейф значений относится к изменению значения определения с течением времени, и, следовательно, изменению в распределении данного значения. Среда, из которой эти значения получены, не является стационарной средой. Сдвиг в вероятности может указывать на то, что определения событий также могут изменяться.

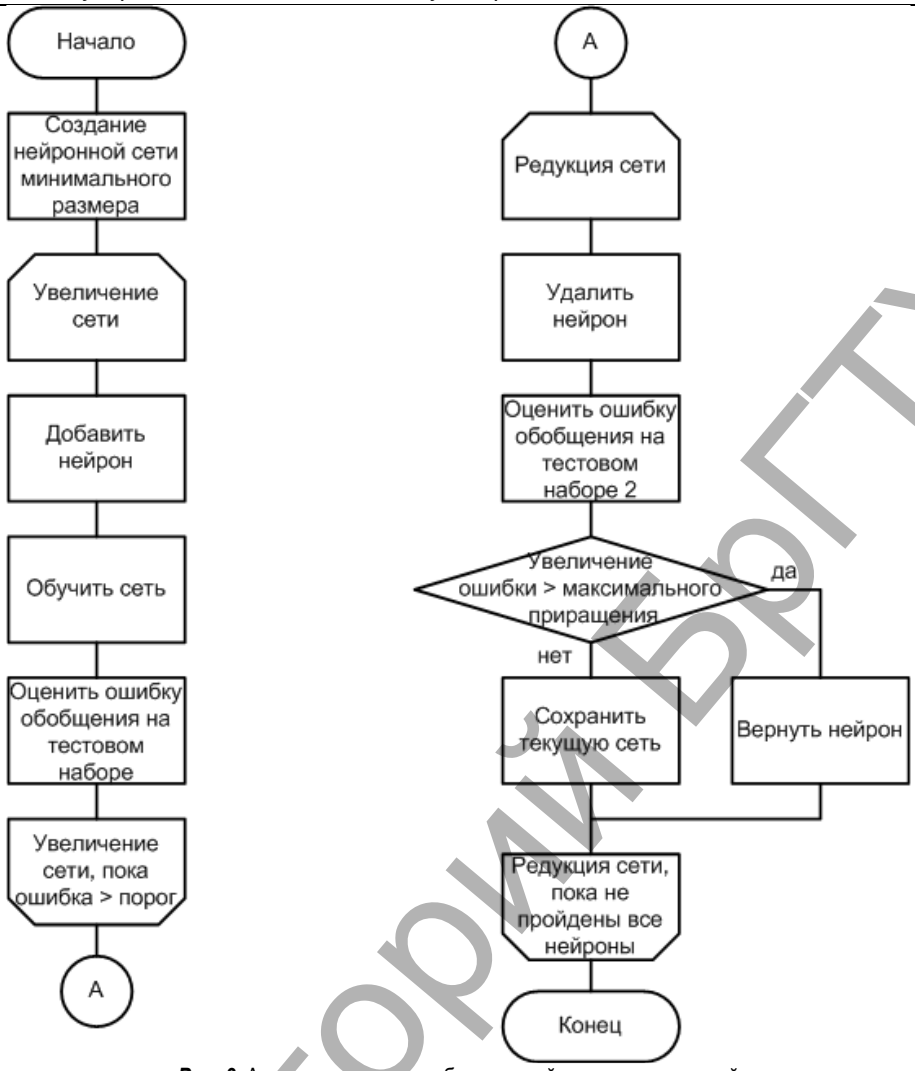

Рис. 3. Алгоритм синтеза и обучения нейросетевых модулей

Общим знаменателем в алгоритмах детектирования дрейфа выступает ансамбль экспертов, которые постепенно обучаются (без доступа к предыдущим данным) на входных данных, в сочетании с некоторой формой взвешенного голосования для получения финального решения. Правила выбора данных для последующего обучения членов ансамбля, и механизм для определения веса голосования являются отличительными чертами различных алгоритмов.

Алгоритм инкрементного дообучения нейросетевых модулей идентификации состояний включает следующие шаги [4]:

1. Производится оценка точности ансамбля модулей нейросетевой идентификации путем сравнения точности результата на предыдущем шаге функционирования и текущем.
2. Если точность не изменилась, либо изменилась в заранее заданном диапазоне, алгоритм завершает работу.
3. Иначе формируется набор обучающих данных, который включает все накопленные данные с последнего дообучения.
4. Производится формирование и обучение нового нейросетевого модуля согласно алгоритму обучения нейросетевых модулей системы идентификации состояний ЦА.
5. Сформированный модуль добавляется в ансамбль.
6. Для всех нейросетевых модулей ансамбля производится пересчет весовых коэффициентов на основании их точности на последний данных.

Процедура дообучения повторяется для всех ансамблей.

Организовав АНС в два уровня [5, 6] можно реализовать гетерогенность нейросетевого комплекса, где первый уровень структуры представляет собой набор ансамблей разнородных сетей, а второй представлен одним обобщающим модулем. На первом уровне могут использоваться различные алгоритмы обучения (BFGS, Левенберга-Марквардта, RPROP); подобные сети, с различными параметрами анализируемых данных (шаг дискретизации, горизонт прогнозирования); подобные сети с различными параметрами обучения, разнородные сети. Такая архитектура может использоваться для поиска оптимальных параметров нейросетевой модели.

В качестве эксперта второго уровня может использоваться ансамбль или одиночная сеть супервизор, обрабатывающие выходные значения всех элементов первого уровня.

Нейросетевая модель анализа временного ряда с различным шагом дискретизации представлена на рисунке 4.

Тестирование алгоритмов нейросетевой идентификации. Важной особенностью анализируемых данных является неравномерное по времени получение показаний датчиков. Сам опрос датчиков осуществляется 10 раз в секунду, но выдача данных осуществляется только при изменении показаний более, чем на некоторый порог. Данная особенность может значительно затруднить дальнейшую обработку данных и поэтому создает необходимость выполнения дополнительного ресемплирования данных для получения данных в виде удобном для обработки. Ресемплирование выполняется для преобразования исходной временной структуры данных к более удобной для обработки структуры, в которой данные «измеряются» в конце каждого временного интервала и формируют собой таблицу. Суть алгоритма ресемплирования состоит в последовательном продвижении от времени самого раннего съема данных ко времени самого позднего съема данных с заданным шагом, при этом данные текущего состояния датчиков сохраняются в новые массивы (рис. 5).

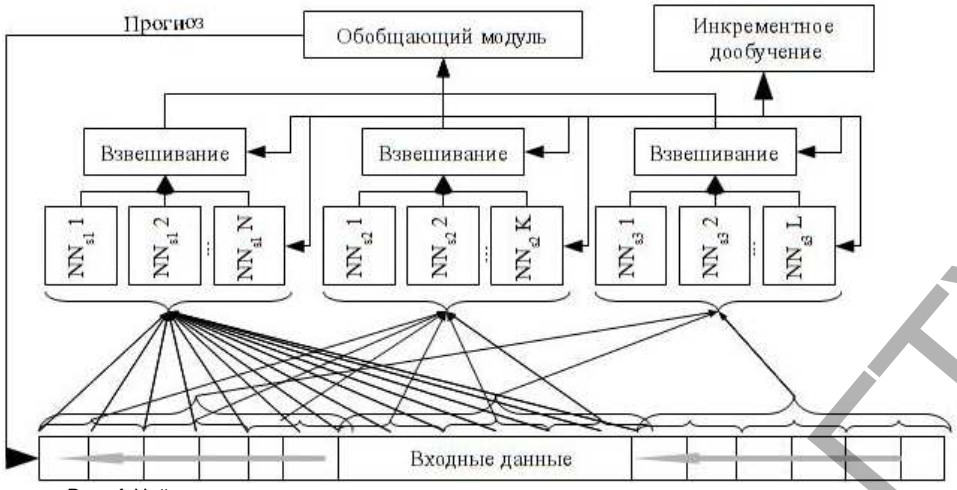

Рис. 4. Нейросетевая модель анализа временного ряда с различным шагом дискретизации

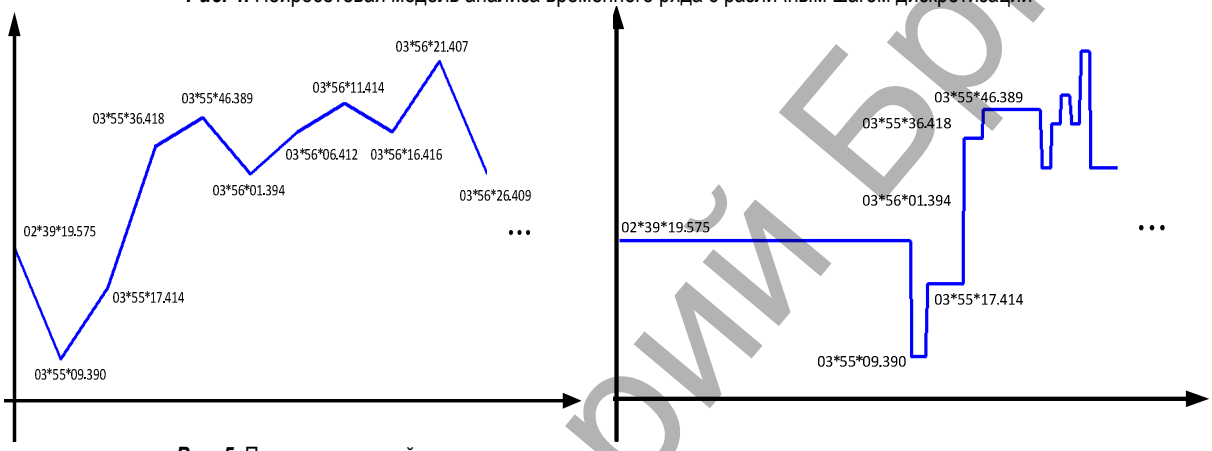

Рис. 5. Пример показаний датчика, слева оригинальные данные, справа - ресемплированные

Исследовалась двухуровневая модель прогнозирования с различным временным масштабом. В качестве нейронной сети использовалась нейронная сеть прямого распространения со скрытым слоем.

На первом этапе обучения исследовались 4 масштаба дискретизации (элемент входного временного ряда содержал 1, 2, 4, 8). В большинстве случаев, масштабы 4 и 8 не вносили дополнительной точности, поэтому были отброшены. Также только небольшая часть одиночных нейронных сетей отбрасывалась для начального временного ряда, это говорит о том, что прогнозируемое значение зависит от всех данных окна прогнозирования.

Далее обобщающий модуль обучался на выходах всех ансамблей первого уровня (выходах взвешивающих модулей). Результатом работы данного модуля является кратковременный прогноз для временных рядов.

Инкрементное дообучение использовалось в минимальной степени, так как в процессе обработки не возникало значительного падения точности прогнозирования.

Сравнивались точности прогнозирования одиночных нейронных сетей, ансамблей нейронных сетей и предлагаемой двухуровневой модели. Ансамбль нейронных сетей показал точность на уровне лучшей одиночной нейронной сети, при этом обучение и выбор архитектуры не потребовали больших временных затрат. Тогда как для определения лучшей нейронной сети обучались 600 одиночных сетей с варьированием размера скрытого слоя (без использования синтеза многослойного персептрона) и параметров алгоритма обучения.

Двухуровневая модель показала результат сходный с результатом АНС, показав улучшение только в некоторых точках за счет использования второго масштаба.

Заключение. В статье рассмотрены архитектура и алгоритмы программного комплекса (ПК) идентификации режимов функционирования подсистем КА и детектирования нештатных и аварийных ситуаций. Тестирование ПК на реальных ТМ-данных (получаемых от работающего БКА) имеет определенные сложности из-за низкой вероятности появления сбоя или нештатных ситуаций, что не позволяет сформировать достаточный набор обучающих данных для всех предполагаемых ситуаций.

СПИСОК ЦИТИРОВАННЫХ ИСТОЧНИКОВ

1. Ганченко, В.В. Нейросетевая модель обработки ТМ-данных для анализа состояния подсистем БКА / В.В. Ганченко и [др.] // VI Белорусский космический конгресс, 28-30 октября 2014 г. – Минск, 2014.
2. Оссовский, С. Нейронные сети для обработки информации / Пер. с пол. И.Д. Рудинского. – М.: Финансы и статистика, 2002. – 344 с.: ил.
3. Царегородцев, В.Г. Конструктивный алгоритм синтеза структуры многослойного персептрона // Вычислительные технологии, 2008. Т.13 // Вестник КазНУ им. Аль-Фараби, серия "математика, механика, информатика", 2008. №4 (59). (Совм. выпуск). Часть 3. – С. 308–315.
4. Parikh, D. An ensemble-based incremental learning approach to data fusion / D. Parikh, R. Polikar // IEEE Trans Syst Man Cybern B Cybern. 2007 Apr. – 37(2). – P. 437–450.
5. Michael I. Hierarchical Mixtures of Experts and the EM Algorithm / Michael I. Jordan, Robert A. Jacobs // Neural Computation. – 1993. – Т. 6. – С. 181–214.
6. Marushko, Y. Using Ensembles of Neural Networks with Different Scales of Input Data for the Analysis of Telemetry Data / Y. Marushko // Proc. of the XV International PhD Workshop OWD 2013, Wisla, 19–22 October 2013. – Gliwice: Silesian University of Technology, 2013. – P. 386–391.

Материал поступил в редакцию 23.12.14

GANCHENKO V.V., MARUSHKO E.E. **Architecture of software system of identification of functioning modes of spacecraft subsystems**

Architecture and algorithms of software system of identification of functioning modes and abnormal situations of spacecraft subsystems are proposed.

УДК 62-519. 621.391

Татур М.М.

ПЕРСПЕКТИВЫ И ПРОБЛЕМЫ СОЗДАНИЯ ОТЕЧЕСТВЕННЫХ МОБИЛЬНЫХ РОБОТОТЕХНИЧЕСКИХ КОМПЛЕКСОВ

Введение. Робототехнический мобильный комплекс – это машина, которая может перемещаться в пространстве и выполнять определенные функции, обусловленные ее специализацией. Под это определение подпадают все беспилотные летательные, наземные (подземные), надводные (подводные) аппараты, и исключаются роботы-станки и роботизированные производственные линии. Минимальной полезной функциональной нагрузкой мобильного робота, как правило, является фото и видеосъемка, а в дополнение могут быть: транспортировка грузов; забор проб грунта, воздуха, воды; проведение дегазации и дезинфекции и т.п. Для обеспечения таких функций машина-робот оснащается соответствующим навесным оборудованием. Таким образом, робототехнические комплексы различаются в первую очередь по своему назначению и по классам: от сверхлегких (до 100 кг) до тяжелых (десятки донн) и сверхтяжелых. В качестве примера дифференциации робототехнических мобильных комплексов приведем один из последних ГОСТов Российской Федерации «Мобильные робототехнические комплексы для проведения аварийно-спасательных работ и пожаротушения» [1], в котором выполнена детальная градация эксплуатационно-технических характеристик, таких как время и режимы работы, средства дистанционного управления, способы привода, температурные ограничения и т.п. Аналогичные классификационные документы существуют (или находятся в стадии разработки) для других видов беспилотных аппаратов.

В настоящей работе будет изложен взгляд автора на состояние и перспективы развития мобильных робототехнических комплексов наземного применения в нашей стране. В первую очередь необходимо сделать следующие замечания.

1. Ряд отечественных компаний и организаций активно осуществляют свою деятельность по производству беспилотных летательных аппаратов, а значит, накоплен достаточный опыт и потенциал по созданию и применению средств дистанционного управления.
2. Отрасли машиностроения и приборостроения представлены крупными НИИ, НПО, заводами и уверенно занимают лидирующие позиции в промышленном производстве.
3. Мобильные робототехнические комплексы наземного (подземного) назначения востребованы в различных сферах жизнеобеспечения, в первую очередь таких как, ликвидация последствий чрезвычайных ситуаций, противодействие терроризму, точное земледелие, горнодобывающая промышленность, в целом там, где может возникнуть угроза здоровью и жизни персонала.

Аналоги. Разработка и построение мобильных робототехнических комплексов развивается в двух направлениях: первое основано на создании уникальных (механизированных) платформ, второе – на применении серийных шасси или изделий в целом. Очевидно, что мобильные комплексы второго направления более конкурентоспособны по экономическим показателям, а первого направления – по тактико-техническим, т.к. разрабатываются под конкретное применение. Примерами робототехнических комплексов на специализированных шасси могут служить: изделие «Адунок» [2] (Беларусь), многофункциональный робот для служб аэропорта QinetiQ (Великобритания) [3], Brokk -роботы для демонтажа строительных конструкций, могут применяться при ликвидации последствий чрезвычайных ситуаций (Швеция) [4].

Из мобильных роботов альтернативного направления можно привести роботизированные машины большинства автоконцернов. Одним из первых отечественных производителей работы по обеспечению дистанционного управления своих машин осуществил БелАЗ в рамках инновационного проекта компании VIST Mining Technology «Интеллектуальные карьер» [5]. Однако, несмотря на приведенные замечания, отечественных мобильных робототехнических комплексов серийного или мелкосерийного производства, доступных для массового применения в сельском, коммунальном хозяйствах и/или силовых ведомствах, пока нет.

Постановка задачи и элементы системного проектирования. Процесс создания сложного технического изделия, к которому без сомнения относится робототехнический комплекс, состоит из ряда этапов, среди которых можно выделить следующие:

- разработку концепции изделия;
- разработку и изготовление прототипа (в данном случае концепткара);
- разработку и изготовление экспериментального образца;
- разработку конструкторской документации и изготовление опытного образца;
- изготовление технологической документации и изготовление промышленного образца;
- постановку изделия на производство.

Содержание большинства названных этапов – общеизвестно и стандартизовано. Наименее формализованным из них является первый, который по сути представляет собой технико-экономическое обоснование концепткара. В ходе данного этапа предстоит корректно сформулировать задачу, наложить реалистичные ограничения и определить оптимальный (или хотя бы рациональный) путь решения. Продемонстрируем сказанное на конкретном примере. (Будем полагать, что маркетинговые исследования проведены, потенциальный потребитель определен, объем поставок не гарантирован, а в худшем случае – слабо предсказуем). Приведенные исходные данные в современных условиях нашей экономики являются почти типовыми для большинства случаев создания инновационных наукоемких продуктов. Поэтому и вариантов стратегий выхода на рынок не столь много. В качестве ответного, опять же, типового варианта стратегии может рассматриваться следующий: создание собственными силами (с минимальным привлечением внешнего финансирования) опытного образца, а затем продвижение его на рынок в виде технологии и/или завершенного продукта с организацией заказного (или мелкосерийного) производства.

При разработке концепции оригинального робототехнического комплекса перед инженером возникает ряд нетривиальных задач, связанных с системным проектированием. Процесс системного проектирования (или, как иногда его называют, использование комплексного подхода в проектировании) можно представить в виде треугольника, где вершинами являются: «Спецификация функций», «Обоснование ограничений» и «Генерация (выбор) технических решений» (рис. 1). Понятно, что решение этих задач взаимозависимо, причем проблема «Спецификации функций», часто является определяющей.

Так например, в нашем случае необходимо создать робототехнический комплекс для ликвидации последствий чрезвычайных ситуаций, тушения пожаров особой сложности и разведывания подо-

Татур Михаил Михайлович, *заведующий кафедрой ЭВМ Белорусского государственного университета информатики и радиоэлектроники, директор ООО «Интеллектуальные процессоры».*
Беларусь, 220013, г. Минск, ул. П. Бровки, 6.