

ПОДХОД К ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ ЗАЩИЩЁННОСТИ РАСПРЕДЕЛЁННОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ АВТОМАТИЗАЦИИ РЕШЕНИЯ ЗАДАЧ УПРАВЛЕНИЯ

М.Ф. Степанов¹, А.М. Степанов², М.А. Пахомов¹, А.А. Жеронкина¹, Л.С. Михайлова³

¹ Саратовский государственный технический университет имени Гагарина Ю.А.

² Институт проблем точной механики и управления РАН

³ Электростальский политехнический институт Московского государственного машиностроительного университета (МАМИ)

Рассматривается задача защиты информации в распределённой системе автоматизации проектирования систем автоматического управления ГАММА-3. Представлена структурная схема распределённой информационной системы. Разработан протокол обмена сообщениями между компонентами распределённой системы, использующий криптографические средства защиты информации. Приведена укрупненная схема обработки сообщений. Приведен пример решения задачи синтеза и анализа закона управления вертолета.

Ключевые слова: Распределенная информационная система, протокол обмена информацией прикладного уровня.

Введение

Бурное развитие информационных технологий, расширение областей применения автоматического управления, как следствие, обусловило создание средств автоматизации решения задач проектирования и исследования систем автоматического управления. Необходимость создания открытых систем [1] автоматизации решения задач, допускающих расширение классов решаемых задач в процессе эксплуатации таких систем определило тенденцию к системной организации в виде распределённой информационной системы. Однако на пути их создания возникли новые проблемы, одна из которых связана с необходимостью обеспечения информационной защищённости таких систем [2]. Проблема обусловлена осуществлением передачи данных между компонентами распределённой информационной системы по открытым каналам связи, что создает предпосылки для несанкционированного доступа к передаваемой информации [3]. Учитывая тот факт, что проектируемые системы управления могут относиться к новым разработкам, то защита информации выходит на первый план [4].

1. Структурная организация системы ГАММА-3

Отличительными архитектурными особенностями системы автоматизации решения задач управления ГАММА-3 [1] являются:

- использование трёхуровневого представления знаний и данных, базирующегося на введении структурных знаний (знаний о знаниях), разделении декларативных и процедурных знаний, явного использования процедур конструирования, наследования и означивания знаний и данных;
- системная организация в виде распределённой информационной системы, в состав которой входят клиентские приложения, осуществляющие интерактивное взаимодей-

- ствие с пользователями, серверные приложения, обеспечивающие единое представление знаний и данных, а также их обработку в ходе решения задач пользователей;
- автоматическая генерация экранных форм для представления знаний и данных на основе имеющихся в системе структурных знаниях (знаний о знаниях).

Построение распределенных информационных систем требует применения безопасных архитектурных решений [5]. Рассмотрение этих вопросов для систем автоматизации решения задач управления проведено в работах [6], [7].

Распределенный вариант реализации системы автоматического решения задач управления ГАММА-3 [8] в базовой комплектации позволяет решать ряд задач идентификации, синтеза и анализа систем автоматического управления [9], [10], [11]. При этом клиентское приложение реализует пользовательский интерфейс, а все вычислительные операции по решению задач, хранению и обработке данных осуществляют серверные компоненты системы.

В связи с организацией системы ГАММА-3 в виде распределённой информационной системы (рис. 1) возникает необходимость обеспечения её информационной защищённости, включающая: обеспечение информационной защищённости клиентских приложений; сервера-посредника; специализированных серверов.

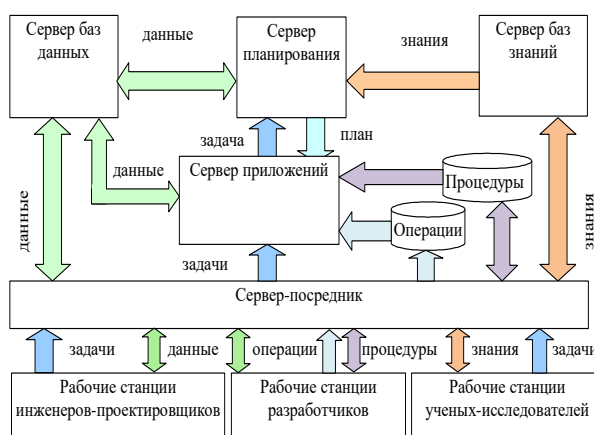


Рис.1. Укрупнённая структурная схема распределённой системы автоматического решения задач ГАММА-3

2. Подход к обеспечению информационной безопасности системы ГАММА-3

Понятие «информационная защищённость» мы будем рассматривать в достаточно узком смысле – только по отношению к соответствующему компоненту системы ГАММА-3 (программное обеспечение + данные), полагая, что безопасность узла вычислительной сети, на котором данный компонент функционирует обеспечивается операционной системой. В таком случае оказывается достаточно средств прикладного уровня модели взаимодействия открытых систем. Традиционным приёмом для обеспечения информационной защищённости на прикладном уровне является использование средств идентификации и аутентификации пользователя, шифрование информации. При этом можно выделить следующие направления применения средств шифрования в системе автоматизации решения задач [12]: 1) Хранение информации в базах данных; 2) Передача информации по сети; 3) Хранение служебной информации в реестре операционной системы; и т.д.

Среди средств обеспечения информационной безопасности распределённой системы автоматического решения задач теории автоматического управления ГАММА-3 выделяются: архитектурные; функциональные; криптографические.

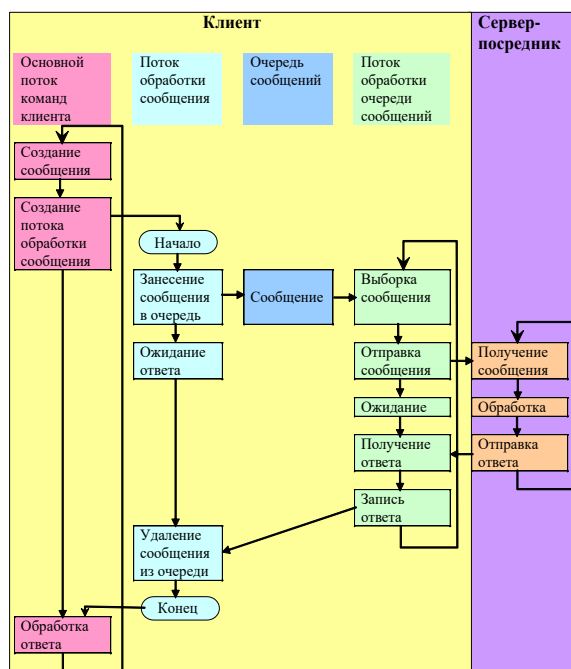


Рис.2. Укрупнённая схема обработки сообщений

К архитектурным средствам обеспечения информационной безопасности системы ГАММА-3 относятся: 1) выделение сервера-посредника, осуществляющего контроль легитимности компонентов системы в процессе их взаимодействия. При этом сообщения нелегитимных компонентов уничтожаются; 2) выделение клиентских приложений, назначением которых являются организация интерфейса с пользователем и связь с сервером-посредником.

К функциональным средствам обеспечения информационной безопасности системы ГАММА-3 относятся: классификация функциональных задач по категориям; выделение для каждой категории задач специальных серверов, задачи которым поступают от сервера-посредника.

К криптографическим средствам обеспечения информационной безопасности системы ГАММА-3 относятся: использование шифрования пересылаемой по сети информации; использование шифрования хранимой в базах данных информации. Реализация криптографических средств защиты информации в системе ГАММА-3 в соответствии с «Алгоритмом криптографического преобразования ГОСТ 28147-89». В состав криптографических средств защиты информации системы ГАММА-3 входят следующие функции, размещённые в библиотеке динамической загрузки mfsCripto.dll: mfsCodeGostCH – шифрование текста произвольной длины на случайном ключе; mfsDecodeGostCH – дешифрование текста произвольной длины, зашифрованного на случайном ключе; createKeyUL – генерация случайного ключа.

Порядок взаимодействия компонентов протокола обмена сообщениями приведен на рис. 2. В состав программной реализации протокола обмена сообщениями, размещённой в библиотеке динамической загрузки MFStpMSG.dll, входят: класс TMFStpMessage, в котором локализована информация конкретного сообщения; класс TMFStpMessageAndReplyList, реализующий очередь сообщений; класс отдельного потока команд (нити) TMFStpMessageThread, реализующий размещение нового сообщения в очереди сообщений; класс отдельного потока команд (нити) TMFStpWorkMessageAndReplyThread, реализующий действия по доставке сообщений и получению ответа для всех сообщений из очереди сообщений.

3. Пример решения задачи синтеза и анализа закона управления

В системе ГАММА-3 в дополнение к средствам решения неструктурированных поставленных задач имеются возможности решения задач в традиционном стиле – посредством указания (задания) процедуры её решения. Для этого разработан проблемно-ориентированный язык ГАММА, ориентированный на матричное представление информации. Базовым элементом представления данных является трехмерная комплексная матрица. Это позволяет представлять матричные полиномы также просто, как и прямоугольные матрицы.

В качестве иллюстрации приведем пример решения задачи синтеза и анализа закона управления вертолета Ми-4 в режиме стабилизации продольного движения в связанной системе координат.

Для исследования траекторных задач допускается использование линеаризованной математической модели в нормальной системе координат [13] x (движение вдоль продольной оси вертолета), y (высота), z (боковое смещение).

Линеаризованные уравнения в отклонениях, описывающие продольное движение вертолета в связанной системе координат в безразмерном виде имеют вид [13]:

$$\dot{x} = Ax + Bu + Mf \quad (1)$$

$$y = Cx + Du + Gv \quad (2)$$

где $x \in R^n$ - вектор состояния объекта управления, $u \in R^m$ - вектор управляющих воздействий, $f \in R^l$ - вектор внешних возмущений, $y \in R^r$ - вектор измеряемых переменных, $v \in R^k$ - вектор шумов измерительной системы.

```

ГАММА-3: Система автоматического решения задач управления - [Проект]
Проект: Проект
Имя: САУ Ми-4
Наименование: САУ продольного движения Ми-4
Аннотация: САУ продольного движения Ми-4
Процедуры:
Программа: Функция
Имя: mi4_stab_xoz
Наименование: САУ Ми-4
Аннотация: Стабилизация продольного движения Ми-4 в нормальной системе координат x, y, z
Вводные: Текст | Заключение
x' = A*x + B*u + M*f
y = C*x + D*u + G*v
x(1) = 0;
x(2) = 0;
x(3) = 0;
x(4) = 0;
x(5) = 0;
x(6) = 0;
x(7) = 0;
x(8) = 0;
x(9) = 0;
x(10) = 0;
x(11) = 0;
x(12) = 0;
x(13) = 0;
mat = "Mi-4: Движение в связанной системе координат в нормальной системе координат";
disp('A');
A = [0.0208 -0.0180 -0.0077 -0.0066 -0.0080 1.3100 0.0 0.0 -9.1
-0.0127 -0.6600 0.0029 -1.2780 -0.2670 -80.3000 -0.1810 0.2710 0.3841];

```

Рис. 3. Текст программы синтеза САУ Ми-4

На рис. 3, 4, 5 приведены экранные формы клиентского приложения в процессе решения задач синтеза и анализа закона управления вертолета Ми-4 в режиме стабилизации продольного движения в связанной системе координат.

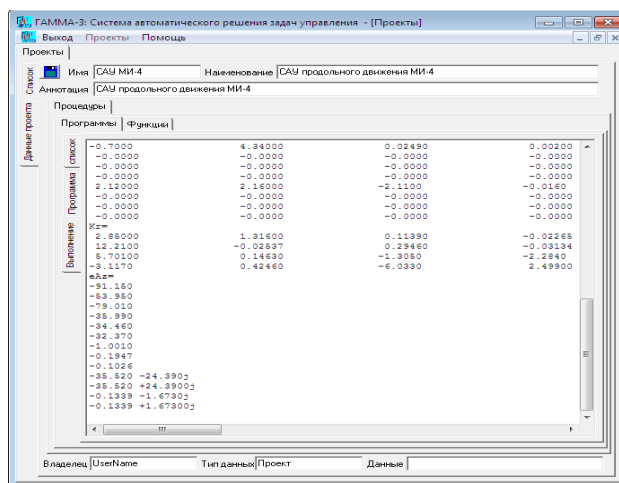


Рис. 4. Протокол решения задачи синтеза

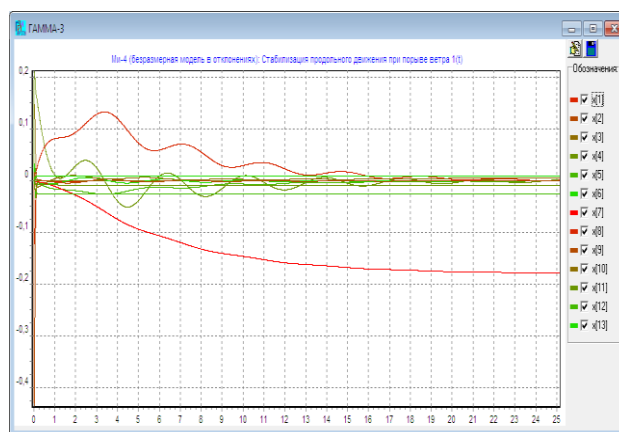


Рис. 5. Графики переходных процессов САУ продольного движения Ми-4 при порыве ветра. Переменные $x(11)$, $x(12)$, $x(13)$ – отклонение в продольном перемещении, изменение высоты и боковое смещение соответственно

Благодарности

Работа выполнена при поддержке Российского фонда фундаментальных исследований (проект 15-07-99684-а).

Литература

1. ГОСТ Р ИСО/МЭК 7498-1-99. Взаимосвязь открытых систем. Базовая эталонная модель. 4.1. Базовая модель. -М.: Госстандарт России, 1999. 62 с.
2. ГОСТ Р ИСО/МЭК 18044-2007. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности.
3. Сердюк В.А. Организация и технология защиты информации. Обнаружение и предотвращение информационных атак в автоматизированных системах предприятий. -М.: Гос. ун-т -Высшая школа экономики, 2011. -572 с.
4. Шаньгин В.Ф. Защита компьютерной информации. Эффективные методы и средства. -М.: ДМК Пресс, 2010. -544 с.
5. Грушо А. Безопасные архитектуры распределенных систем / Грушо А., Грушо Н., Тимонина Е., Шоргин С. //Системы и средства информатики, 2014. Т. 24. № 3. С. 18-31.

6. Степанов М.Ф. О развитии концепции автоматического решения задач теории управления в системе ГАММА-3 / А.Г.Александров, Л.С.Михайлова, М.Ф.Степанов, Т.М.Брагин, А.М.Степанов // Мехатроника, автоматизация, управление. №9, 2011. С. 14 - 19
7. Степанов М.Ф. Исследование и оптимизация архитектуры распределенной системы автоматического решения задач проектирования систем автоматического управления / М.Ф.Степанов, А.М.Степанов // Восьмая Всероссийская мультиконференция по проблемам управления (28 сентября – 3 октября 2015 г. с. Дивноморское, Геленджик, Россия): Материалы 8-й Всероссийской мультиконференции: в 3 т. Т.3. – Ростов-на-Дону : Издательство Южного федерального университета, 2015. - С. 58 - 60
8. Александров А.Г. Система ГАММА-3 и ее применение / А.Г.Александров, Л.С.Михайлова, М.Ф.Степанов // Автоматика и телемеханика, 2011, № 10. С. 19 – 27
9. Степанов М.Ф. Автоматизация построения и исследования управления динамическими объектами на основе технологии нечёткой логики в системе ГАММА-3 / Л.С. Михайлова, М.А. Пахомов, А.М. Степанов, М.Ф. Степанов // Вестник Саратов. гос. техн. ун-та. № 4. Саратов, 2015
10. Степанов М.Ф. Подход и методика автоматизации решения задач нейроруливания в системе ГАММА-3 / М.Ф.Степанов, А.М.Степанов, Л.С.Михайлова, А.А.Жеронкина // Системы проектирования, технологической подготовки производства и управления этапами жизненного цикла промышленного продукта (CAD/CAM/PDM – 2015). Труды 15-й международной конференции. Под ред. А.В.Толока. М.: ООО «Аналитик». – 2015. С. 317 – 320.
11. Степанов М.Ф. Подход и методика автоматизации конечно-частотной идентификации в системе ГАММА-3 / А.Г.Александров, М.Ф.Степанов, А.М.Степанов, Л.С.Михайлова, О.Н.Пименова // Системы проектирования, технологической подготовки производства и управления этапами жизненного цикла промышленного продукта (CAD/CAM/PDM – 2015). Труды 15-й международной конференции. Под ред. А.В.Толока. М.: ООО «Аналитик». – 2015. С. 326 – 329.
12. Путинцев Г.В. Автоматизированная система обнаружения инцидентов информационной безопасности корпоративных сетей передачи данных / Путинцев Г.В., Монахова М.М. // Имитационное моделирование. Теория и практика Седьмая всероссийская научно-практическая конференция, труды конференции в 2 томах. Институт проблем управления им. В.А. Трапезникова РАН; Под общей редакцией С.Н. Васильева, Р.М. Юсупова. 2015. С. 297-301.
13. Кожевников В.А. Автоматическая стабилизация вертолета. М.: Машиностроение, 1977. – 152 с.