DOI: 10.17117/na.2016.11.02.116

<http://ucom.ru/doc/na.2016.11.02.116.pdf>

Поступила (Received): 03.11.2016

Ерохин В.В., Елисеева Е.В.

Верификация данных в инфокоммуникационных сетях

Erokhin V.V., Eliseeva E.V.

Verification of data in infocommunication networks

В статье рассматриваются современные подходы к контроллингу правильности функционирования инфокоммуникационных сетей, являющихся базисом информационных систем различного назначения. Авторами проанализированы такие подходы к контроллингу, как тестирование, теоретико-доказательный подход и верификация моделей программных средств. Основное внимание в работе уделяется рассмотрению различных методов верификации моделей программных средств и выделению наиболее перспективных, к которым авторы отнесли методы, базирующиеся на поиске инвариантов и символьные методы

Ключевые слова: данные, сети, инфокоммуникации, верификация

Ерохин Виктор Викторович

Доктор технических наук, профессор
Брянский государственный университет им. И.Г. Петровского
г. Брянск, ул. Бежицкая, 14

Елисеева Елена Владимировна

Кандидат технических наук, профессор
Брянский государственный университет им. И.Г. Петровского
г. Брянск, ул. Бежицкая, 14

In article modern approaches to controlling of correctness of functioning of the infocommunication networks which are basis of information systems of different function are considered. Authors have analysed such approaches to controlling as testing, teoretiko-evidential approach and verification of models of software. The main attention in work is paid to consideration of various methods of verification of models of software and allocation of the most perspective to which authors have carried the methods which are based on search of invariants and symbolical methods

Key words: data, networks, infokommunikation, verification

Erokhin Victor Viktorovich

Doctor of Technical Sciences, Professor
Bryansk state university of a named I.G. Petrovsky
Bryansk, Bezhitskaya st., 14

Eliseeva Elena Vladimirovna

Candidate of Technical Sciences, Professor
Bryansk state university of a named I.G. Petrovsky
Bryansk, Bezhitskaya st., 14

Развитие телекоммуникационных технологий меняет подход к проектированию, модернизации и построению большинства корпоративных инфокоммуникационных сетей (ИС), которые становятся более масштабными и сложными относительно их инфраструктуры, функциональности и используемых сервисов. ИС решают задачи по бесперебойной и безопасной передаче и обработке информационных данных, содержащих коммерческую (а иногда и государственную) тайну.

Настоящая статья является продолжением серии публикаций авторов, посвященных проблемам внедрения и обеспечения безопасности информационных систем на современном производстве, в экономике, образовании [4], [5], [6].

Эффективность и качество ИС как правило определяются аппаратурной надежностью, надежностью программного инструментария защиты информации (ЗИ), а значит проблема обеспечения верификации ИС, являющихся базисом информационных систем различного назначения, является актуальной [4].

Экспоненциальный рост сложности аппаратного и программного обеспечения в ИС приводит к повышению требований для бездефектного проектирования программных средств. Все современные ИС обязательно должны в себя включать программные, методологические и инструментальные средствами мониторинга эксплуатируемой ИС на всех её этапах жизненного цикла. Как правило, актуальными являются проблемы, связанные с обеспечением надежной эксплуатации ИС.

На современном этапе эксплуатации ИС сложилось несколько подходов к контроллингу правильности её функционирования: тестирование, теоретико-доказательный подход и верификация моделей программных средств.

Наиболее применяемым подходом является тестирование. При тестировании на вход программного средства даются заблаговременно сгенерированные тестовые данные и контролируется соответствие результата, выданного программным средством, ожидаемому. Базисной характеристикой при тестировании является детерминированность алгоритма. В случае распределённой ИС, применяющего несколько процедур и исполняющейся на нескольких ЭВМ, поведение программного средства может быть неоднозначным. В этом случае для контроля поведения программного средства в ходе эксплуатации ИС используются средства трассировки.

Контроллинг ИС с использованием верификации моделей программных средств направлен на доказательство утверждений о характере или результатах работы программного средства [2].

Методы верификации, применяющие теоретико-доказательный подход, базируются на программных средствах автоматического доказательства теорем («theoremprover»). Программное средство ИС и её спецификация описывается в виде совокупности логических утверждений. Программный инструментарий «theoremprover» генерирует доказательство исполнимости спецификации ИС, исходя из утверждений, описывающих контролируемое программное средство. В этом методе может понадобится участие эксперта. Одной из наиболее сложных задач в этом методе является генерирование инварианта цикла, который требуется при контроле выводимости постусловия процесса из предусловия.

Верификация ИС с применением логических утверждений, спроектированных непосредственно на базисе исходных кодов, повышает сложность процедуры доказательства. Некоторые фрагменты кода могут быть несущественными для контроля анализируемых характеристик ИС. Характеристики ИС могут быть проконтролированы на более простой модели ИС, чем исходное ИС. Верификация упрощенных моделей (Model Checking) является компромиссным

подходом между полноценной верификацией ИС и тестированием, использующим формальный контроллинг свойств ИС.

Верификации подлежат следующие ИС, параметризованные по количеству взаимодействующих компонентов [3]:

- распределённые алгоритмы: обнаружения завершения (termination detection), волновые алгоритмы согласованного принятия транзакции (distributed commit), взаимного исключения доступа к критической секции, распределения ресурсов, избрания лидера (leader election);

- сетевые протоколы: протоколы маршрутизации, кольцо с маркером, протоколы обеспечения качества процедур ИС, широковещательные протоколы;

- аппаратные схемы: аппаратные схемы управления доступом к шине для разного количества распределённых узлов ИС, протоколы обеспечения когерентности кэшей.

При конструировании модели распределённой ИС, которая может потенциально в себя включать любое количество однотипных сетевых узлов, ограничиваются моделью с фиксированным или небольшим количеством процедур. Предполагается, что характеристики ИС, проконтролированные на модели с фиксированным количеством процедур, автоматически масштабируются для моделей с большим количеством процедур.

Однако такой приём не является как правило верным: известны ИС, когда спецификация была верна на модели с одним количеством процедур и нарушалась при изменении количества процедур.

Это означает, что для верификации упрощённых моделей ИС недостаточно осуществить контроллинг спецификации на нескольких моделях с фиксированным количеством процедур.

Требуется обоснование подобия проконтролированной спецификации на остальные модели ИС. Так как количество процедур в моделях ИС не ограничивается, то контроллинг спецификации может быть осуществлён на бесконечной совокупности упрощённых моделей ИС с конечным количеством её состояний [1].

Наиболее перспективными методами, настраиваемыми на различные виды топологии упрощённых моделей ИС, являются методы, базирующиеся на поиске инвариантов, и символьные методы.

Символьные методы верификации упрощённых моделей ИС могут потребовать участия эксперта для проработки её модели и указания дополнительных экспертных пояснений. Применение этого метода позволяет сохранить базисное преимущество – автоматическую верификацию модели ИС.

Список используемых источников:

1. Аверченков В.И., Ерохин В.В. Система обеспечения безопасности Российской Федерации. Брянск: БГТУ, 2005. 120 с.
2. Аверченков В.И., Ерохин В.В. Системы организационного управления. Брянск: БГТУ, 2012. 208 с.
3. Аверченков В.И. Структура системы обеспечения безопасности Российской Федерации / В.И. Аверченков, В.В. Ерохин, М.Ю. Рытов, О.М. Голембиовская. Брянск: БГТУ, 2012. 140 с.

4. Ерохин, В.В. Безопасность информационных систем/ В.В. Ерохин, Д.А. Погоньшева, И.Г. Степченко. М.: ФЛИНТА, 2015. 84 с.
5. Современные информационно-коммуникационные технологии в образовании: монография/ Е.С.Рогальский, Е.В.Елисеева, С.Н.Злобина и др.; под общей редакцией Н.В.Лалетина. Красноярск: Центр информации, 2012. 220 с.
6. Результаты социально-экономических и междисциплинарных научных исследований XXI века: монография. Самара: ООО «Офорт», 2016. 260 с.

© 2016, Ерохин В.В., Елисеева Е.В.

Верификация данных в инфокоммуникационных сетях

© 2016, Erokhin V.V., Eliseeva E.V.

Verification of data in infocommunication networks