ЭЛЕКТРОМАГНИТНАЯ СОВМЕСТИМОСТЬ И БЕЗОПАСНОСТЬ ОБОРУДОВАНИЯ

УДК 004.72

КОЛИЧЕСТВЕННЫЕ ХАРАКТЕРИСТИКИ БЕЗОПАСНОСТИ ФУНКЦИОНИРОВАНИЯ СЛОЖНЫХ ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ

Фалин М.Н.

Предложены количественные характеристики безопасности функционирования сложных телекоммуникационных систем, согласно которым может быть принято решение о безопасности функционирования.

Ключевые слова: сложные телекоммуникационные системы, безопасность функционирования, показатели безопасности функционирования.

Введение

На современном этапе ключевая роль в инфраструктуре информатизации отводится системам телекоммуникаций, возрастают требования к телекоммуникационному оборудованию. Все это приводит к появлению сложных телекоммуникационных систем (СТКС), которые объединяют в себе множество взаимодействующих структур и средств, предназначенных для передачи больших объемов информации между пользователями системы, ключевым условием внедрения которых является безопасность функционирования.

Под безопасностью функционирования СТКС будем понимать, согласно [3], свойство системы противодействовать появлению аварийных ситуаций, влияющих на жизнедеятельность человека и среду его обитания при функционировании системы в соответствии с целевым назначением. К настоящему времени существуют подходы к повышению безопасности функционирования устройств и систем, однако числовых показателей, позволяющих оценивать безопасность функционирования СТКС, пока нет. В статье делается попытка ввести количественные показатели безопасности функционирования СТКС.

Перечень свойств, необходимых для оценки безопасности функционирования СТКС

Для проведения оценки безопасности функционирования можно представить безопасность функционирования СТКС через набор свойства (характеристики), по которым можно сделать вывод о безопасности функционирования системы [1]:

$$Safe = F\{x_{i1}, x_{i2}, \ldots x_{in}\},$$

где F – функция, определяющая безопасность функционирования системы; x_i – свойства (характеристики) телекоммуникационных систем, определяющих их безопасность.

В качестве примера приведем возможный набор свойств, предназначенных для оценки безопасности функционирования СТКС.

Функциональность системы. Данное свойство включает описание входной информации, результатов ее обработки, а также используемые для получения необходимого результата процессы и их характеристики. Основной задачей контроля является проверка характеристик функционирования системы, ориентированных на получение конечного результата.

Надежность системы. Данное свойство характеризует способность системы выполнять определенные задачи в определенных условиях эксплуатации. Надежность характеризуется вероятностью безотказной работы или вероятностью отказа в заданном интервале времени. Надежность является одной из главных проблем, которые необходимо решить для обеспечения функционирования СТКС.

Масштабируемость системы. Данное свойство характеризует возможность ее наращивания и развития (улучшения), что позволяет выделить такие показатели, как совместимость или расширяемость.

Управляемость системы. Данное свойство характеризует возможность прямого управления системой, ее мониторинга, а также изменения и даже создания новых функциональных характеристик. Чем выше управляемость, тем выше вероятность обеспечения наилучшего ее функционирования. Управляемость определяется как жесткостью заложенных в нее механизмов, так и наличием стандартизированных средств (или интерфейсов) доступа к управлению, так как при примитивных средствах доступа и модификации управляемость системы не может быть высокой, даже при наличии развитых механизмов управления.

Производительность системы. Данное свойство отражает максимальную скорость обработки

информации, показывает, как быстро система выполняет поставленные перед ней задачи и сколько задач может выполнить одновременно.

Мобильность системы. Данное свойство отражает возможность переноса программ, данных при модернизации или замене аппаратных платформ системы, и возможность работы с ними специалистов, пользующихся информационными технологиями, без их переподготовки при изменениях системы.

Информационная безопасность системы. Данное свойство определяет меры по обеспечению ценности системы, защищенности и гарантированной точности и целостности информации и позволяет минимизировать разрушения, которые могут иметь место, если информация будет модифицирована или разрушена. Информационная безопасность требует учета всех событий, в ходе которых информация создается, модифицируется, распространяется или к ней обеспечивается доступ.

Экономичность системы. Данное свойство системы отражает возможность осуществлять свои функции с минимумом затрат при наличии определенных ограничений.

Набор свойств, необходимых для оценки безопасности функционирования СТКС, также зависит от мнения лица, принимающего решение (ЛПР). Это предполагает, что разработчик или пользователь системы будет самостоятельно выбирать перечень свойств, по его мнению, отражающих безопасность функционирования исследуемой СТКС. Тем самым результаты оценки безопасности функционирования одной и той же СТКС разными ЛПР могут варьироваться.

Разработка универсального перечня свойств для оценки безопасности функционирования СТКС может стать задачей самостоятельного исследования.

Детализация выделенных свойств СТКС

Проведя анализ свойств, предложенных для оценки безопасности функционирования СТКС, можно сделать вывод, что для полной и точной оценки необходима детализация выделенных свойств. Предлагается представить каждое выделенное свойство (характеристики) системы через совокупность его составляющих, каждую из которых будем называть частным показателем свойства. Тогда согласно [1]

$$x_i = F\{y_{i1}, y_{i2}, \ldots y_{in}\};$$

где x_i – по-прежнему характеристика системы, например, определяющая ее безопасность; $\{y_{i1}, y_{i2}, \ldots y_{in}\}$ – множество частных показателей соответствующего свойства.

Для выбранных ранее свойств, характеризующих степень безопасности СТКС, можно предложить вариант детализации, который иллюстрирует таблица 1.

Таблица 1. Возможный вариант детализации свойств СТКС, необходимых для оценки безопасности их функционирования

№	Свойства системы	Детализированные единицы свойств
1	Функциональность системы	- количество типов выполняемых задач при обработке информации - функциональность выполняемых, решаемых задач при обработке информации - уровень совместимости набора функций, реализуемых исследуемой системой, с функциями смежных систем
2	Надежность системы	- устойчивость к неисправностям - время восстановления
3	Масштабируемость системы	- возможность увеличения числа пользователей системы без существенных изменений в её структуре - возможность взаимодействия с другими системами
4	Управляемость системы	- удобство интерфейса - возможность прямого управления системой
5	Производительность системы	- максимальная скорость обработки информации - количество одновременно выполняемых задач - среднее время выполнения одной поставленной задачи
6	Мобильность системы	- способность системы адаптироваться к изменениям - возможность работы специалистов без их переподготовки при изменениях системы
7	Информационная безопасность системы	- количество типов угроз безопасности - удобство управления средствами повышения степени защиты
8	Экономичность системы	- стоимость модификации системы - стоимость поддержки системы

Таблица 2. Принцип определения интервалов значений свойств, определяющих безопасность функционирования СТКС

№ интервала	Характеристика интервала
Количественные интервалы значений свойств, прямо пропорционально определяющих безопасность функционирования	
1	Интервалы самых малых значений
2 и 3	Интервалы промежуточных значений (значения 2-го интервала < значений 3-го)
4	Интервалы самых больших значений
Количественные интервалы значений свойств, обратно пропорционально определяющих безопасность функционирования	
1	Интервалы самых маленьких значений
2 и 3	Интервалы промежуточных значений (значения 2-го интервала < значений 3-го)
4	Интервалы самых больших значений

Таблица 3. Балльная оценка значимости для ЛПР свойств, определяющих безопасность функционирования СТКС

Важность свойств	Определение важности свойства
1	Абсолютно не значимо
2	Значимо слабо
3	Существенно или сильно значимо
4	Абсолютно значимо

Таблица 4. Соответствие значений свойств, определяющих безопасность функционирования исследуемой системы, выделенным интервалам оценки (пример)

Свойство системы	Интервал, соответствующий значению свойства системы	Допустимые интервалы значений
x_1	Третий интервал	Только четвертый и третий
x_2	Четвертый интервал	Только четвертый
x_3	Третий интервал	Только четвертый и третий

Количественные характеристики безопасности функционирования СТКС

В данной работе будем рассматривать исследуемую систему в аспекте требований, предъявляемых ЛПР. Для учета индивидуальных требований ЛПР введем интервальную оценку значений каждого свойства, определяющего безопасность функционирования исследуемой СТКС. Интервалы предлагается пронумеровать в соответствии с принципом нумерации значений свойств, определяющих безопасность функционирования СТКС (см. таблицу 2) [2].

Оценку степени значимости для ЛПР свойств, определяющих безопасность функционирования СТКС, предлагается проводить на основе баллов значимости (см. таблицу 3).

Допустимые интервалы значений свойств, характеризующих безопасность функционирования СТКС, предлагается определять в зависимости от балльной оценки ЛПР значимости данных свойств. Принцип определения допустимых интервалов представлен в [2] и на рис. 1.

Пусть значения свойств, определяющих безопасность функционирования исследуемой СТКС, отнесены к следующим интервалам, согласно принципам нумерации интервалов свойств, определяющих безопасность функционирования и соответствующих таблицам 2 и 4.

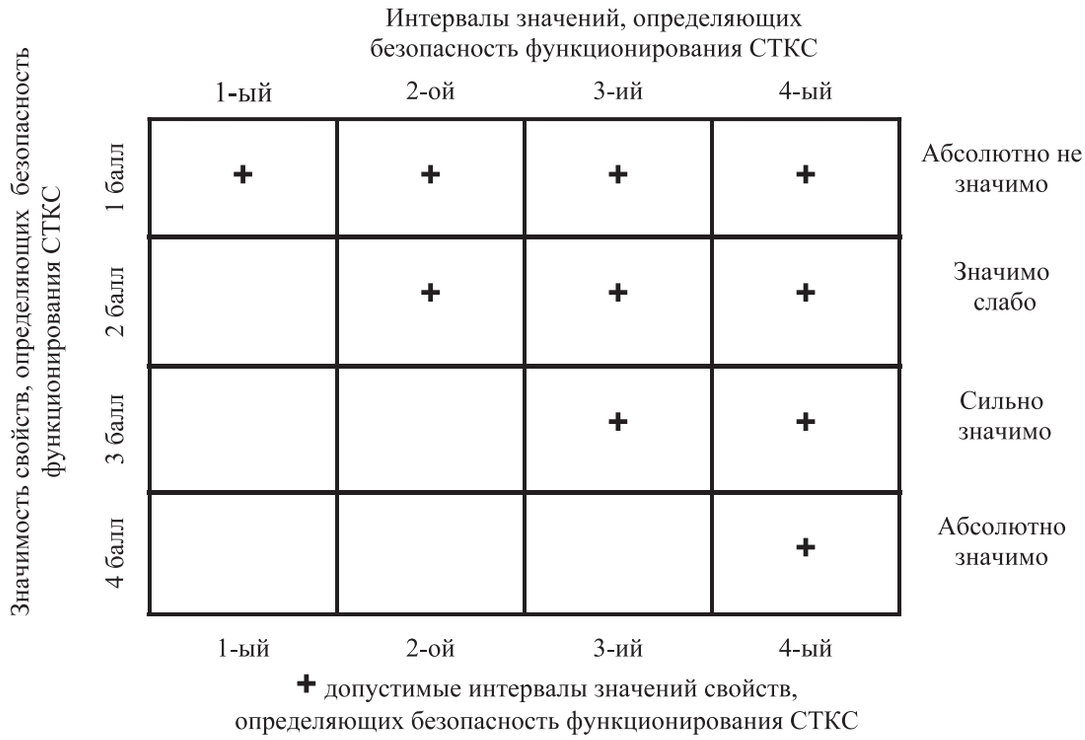

Рис. 1. Матрица определения допустимых интервалов значений свойств, определяющих безопасность функционирования СТКС, – согласно принципам нумерации интервалов свойств, определяющих безопасность функционирования (см. таблицу 2)

Как видно из таблицы 4, рассматриваемая система полностью соответствует интервалам допустимых значений, определяющих безопасность функционирования. Таким образом, рассматриваемая система может использоваться в дальнейшем, т.к. она удовлетворяет требованиям безопасности функционирования.

Заключение

Предложен один из возможных способов количественной оценки безопасности функционирования СТКС. Оценка безопасности функционирования СТКС основана на методах интервальной и экспертной взвешенной оценки. Представленная детализация является лишь возможным иллюстрационным примером для оценки безопасности функционирования СТКС и может быть изменена или доработана.

Количественный анализ любых сложных систем чрезвычайно трудоемок, поскольку надо не только выявить их состав, структуру, морфологию и функциональную среду, но и определиться с параметрами, показателями и количественными характеристиками как всей системы, так и ее существенных компонентов. Поэтому проведение оценки безопасности функционирования СТКС может быть рекомендовано для систем массового обслуживания систем, осуществляющих управление уникальными объектами, процессами – систем, последствия отказа которых могут привести к значительным потерям или нанести существенный урон окружающей среде.

Литература

1. Петров А.Б., Фалин М.Н. Алгоритм оценки безопасности функционирования сложных телекоммуникационных систем // В мире научных открытий. №8.1 (20), 2011. – С. 490-497.
2. Стариковская Н.А. Двухэтапная процедура выбора систем с точки зрения интероперабельности // Наукоемкие технологии. №10, 2010. – С. 36-45.
3. Тхыонг Н.К. Методы и модели надежности, эффективности и безопасности сложных технических систем в конфликтных ситуациях. Дисс. д.т.н. М.: ВЦ РАН, 1999. – 323 с.

QUANTITATIVE CHARACTERISTICS THE SAFE OPERATION OF TELECOMMUNICATION SYSTEMS AND COMPLEX

Falin M.N.

In this paper proposed for the quantitative characteristics of the safe operation of telecommunication systems and complex, according to which the decision can be made about the safety of operation.

Keywords: *telecommunication systems and complex, the operation safety, characteristics of the safe operation.*

Фалин Михаил Николаевич, аспирант Московского государственного технического университета радиотехники, электроники и автоматики. Тел. 8-903-234-76-35. E-mail: mikelbym@gmail.com

УДК 621.391

МОДЕЛИРОВАНИЕ ПАРАЛЛЕЛЬНЫХ АЛГОРИТМОВ ШИФРОВАНИЯ ИНФОРМАЦИИ

Кочеров Ю.Н., Червяков Н.И.

В статье рассмотрены вопросы моделирования параллельных алгоритмов шифрования информации с использованием системы остаточных классов и приведены примеры алгоритмов шифрования RSA, восстановления чисел и моделирования параллельных алгоритмов шифрования в среде Matlab Simulink. Целью статьи является увеличение криптостойкости путем параллельного выполнения различных криптографических алгоритмов или параллельного использования одного алгоритма, но с разными ключами.

Ключевые слова: параллельные алгоритмы, шифрование информации, алгоритм RSA.

Введение

В современном информационном мире информация становится более ценным ресурсом, чем материальные и энергетические ресурсы. Владение точной и достоверной информацией дает преимущество той стороне, которая ею владеет, – особенно если эта информация касается конкурентов. Обладание такой информацией позволяет ее владельцу получить выигрыш: материальный, политический или военный. В современном мире необходимо защищать огромное количество информации, хранимой в базах данных и предаваемой по информационным сетям.

Постановка задачи и моделирование алгоритма шифрования RSA в среде Matlab Simulink

В настоящее время наиболее важную роль играет защита электронной информации от несанкционированного доступа. Для защиты информации используют различные криптографические алгоритмы, такие как RSA, DSA, ГОСТ 28147-89, Шифросистема Эль-Гамаля и многие другие. Надежность криптографических алгоритмов во многом зависит от сложности реализации и от длины ключа шифрования данных. При моделировании в системе Matlab Simulink был использован алгоритм шифрования RSA – криптографический алгоритм с открытым ключом (RSA стал первым алгоритмом такого типа, пригодным и для шифрования и цифровой подписи, сегодня он используется в большом числе криптографических приложений [1]).

Возьмем два больших простых числа p и q. Определим n как результат умножения p на $q: n = p \cdot q$. Выберем случайное число, которое назовем d: это число должно быть взаимно простым (не иметь ни одного общего делителя, кроме единицы, с результатом умножения $(p-1)\cdot(q-1)$).

Определим также число e, для которого является истинным следующее соотношение $(e \cdot d) \bmod (p-1)\cdot(q-1) = 1$. Назовем открытым ключом числа e и n, а секретным – d и n. Задача состоит в том, чтобы зашифровать текст, рассматриваемый как последовательность чисел $M(i)$, по формуле $C(i) = (M(i)^e) \bmod n$. Чтобы расшифровать данные, необходимо выполнить вычисления $M(i) = (C(i)^d) \bmod n$. В результате будет получено множество чисел $M(i)$, которые представляют собой исходный текст.

Следующий пример наглядно демонстрирует алгоритм шифрования RSA.

Зашифруем и расшифруем сообщение «САВ» по алгоритму RSA. Для простоты возьмем небольшие числа, что сократит расчеты.

Выберем $p = 3$ и $q = 11$.

Определим $n = 3 \cdot 11 = 33$.

Найдем $(p-1)\cdot(q-1) = 20$. Пусть d будет равно, например, 3, то есть $d = 3$.