SCIENTIFIC JOURNAL

3(70)/2014

INFORMATSIONNO-UPRAVLIAIUSHCHIE SISTEMY (INFORMATION AND CONTROL SYSTEMS)

REFEREED EDITION

Contact information
The Editorial and Publishing Center, SUAI
67, B. Morskaia, 190000, St. Petersburg, Russia
Website: http://i-us.ru/en, E-mail: ius.spb@gmail.com
Tel.: +7 - 812 494 70 02

The Journal was registered in the Ministry of Press, Broadcasting and Mass Media of the Russian Federation. Registration Certificate JD № 77-12412 from April, 19, 2002. Re-registration in the Federal Service for Supervision in the Sphere of Telecom, Information Technologies and Mass Communications (ROSKOMNADZOR) due to change of the founder: «Information and Control Systems», Ltd., JD № FS77-49181 from March, 30, 2012.

The journal is distributed by subscription. Subscription can be made in the Editorial and publishing center, SUAI as well as in any post office based on «Rospechat» catalogue:
№ 48060 — annual subscript, № 15385 — semiannual subscript.

Submitted for publication 07.04.14. Passed for printing 17.06.14. Format 60×841/8.
Offset paper. Phototype SchoolBookC. Offset printing.

Layout original is made at the Editorial and Publishing Center, SUAI.
67, B. Morskaia, 190000, St. Petersburg, Russia
Printed from slides at the Editorial and Publishing Center, SUAI.
67, B. Morskaia, 190000, St. Petersburg, Russia

НАУЧНЫЙ ЖУРНАЛ

3(70)/2014

РЕЦЕНЗИРУЕМОЕ ИЗДАНИЕ

ИНФОРМАЦИОННО-УПРАВЛЯЮЩИЕ СИСТЕМЫ

Учредитель
ООО «Информационно-управляющие системы»

Адрес редакции: 190000, Санкт-Петербург,
Б. Морская ул., д. 67, ГУАП, РИЦ
Тел.: (812) 494-70-02, e-mail: ius.spb@gmail.com, сайт: http://i-us.ru

Журнал зарегистрирован в Министерстве РФ по делам печати, телерадиовещания и средств массовых коммуникаций. Свидетельство о регистрации ПИ № 77-12412 от 19 апреля 2002 г. Перерегистрирован в Роскомнадзоре. Свидетельство о регистрации ПИ № ФС77-49181 от 30 марта 2012 г.

Журнал входит в «Перечень ведущих рецензируемых научных журналов и изданий, в которых должны быть опубликованы основные научные результаты диссертации на соискание ученой степени доктора и кандидата наук».

Журнал распространяется по подписке. Подписку можно оформить через редакцию, а также в любом отделении связи по каталогу «Роспечать»: № 48060 — годовой индекс, № 15385 — полугодовой индекс.

Сдано в набор 07.04.14. Подписано в печать 17.06.14. Формат 60×84 1/8.
Бумага офсетная. Гарнитура SchoolBookC. Печать офсетная.
Усл. печ. л. 16,0. Уч.-изд. л. 20,1. Тираж 1000 экз. Заказ 258.

Оригинал-макет изготовлен в редакционно-издательском центре ГУАП.
190000, Санкт-Петербург, Б. Морская ул., 67.

Отпечатано с готовых диапозитивов в редакционно-издательском центре ГУАП.
190000, Санкт-Петербург, Б. Морская ул., 67.

УДК 004.02

МЕТОДИКА РАСЧЕТА НАДЕЖНОСТИ СЛОЖНЫХ СИСТЕМ, УЧИТЫВАЮЩАЯ УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

С. В. Беззатеев[a], *доктор техн. наук, доцент*
Н. В. Волошина[a], *канд. техн. наук, доцент*
П. С. Санкин[a], *ассистент*
[a]*Санкт-Петербургский государственный университет аэрокосмического приборостроения, Санкт-Петербург, РФ*

Цель: *разработка методики расчета надежности сложных систем, учитывающей влияние угроз информационной безопасности на надежность системы в целом.* ***Результаты:*** *описаны задачи оценки надежности, решаемые на стадии проектирования сложных систем. Одним из наиболее эффективных формальных методов, позволяющих получить численные значения надежности системы, является использование дерева отказов, однако при этом не учитываются проблемы, связанные с информационной безопасностью, и их существенное влияние на работоспособность системы. Для комплексной оценки надежности и безопасности сложных систем на этапе их проектирования предлагается строить дерево отказов с учетом угроз информационной безопасности. В частности, в рассмотрение вводится дополнительный модуль системы, который позволяет учесть влияние угроз безопасности на надежность системы в целом. Таким образом, предложено решение проблемы совместного обеспечения надежности и безопасности систем. Проведена общая оценка надежности и безопасности части системы ETCS, в качестве примера рассмотрена подсистема путевых RFID-меток Eurobalise.* ***Практическая значимость:*** *предложенная методика учета угроз информационной безопасности при расчете надежности систем позволяет получить более адекватные оценки надежности еще на этапе проектирования сложных систем.*

Ключевые слова *— надежность сложных систем, угрозы информационной безопасности, анализ дерева отказов.*

Введение

Роль информационных технологий и степень их интеграции в процессах управления сложными системами постоянно возрастает. Все более актуальной становится задача анализа влияния угроз информационной безопасности на уровень надежности таких систем.

В то же время существующие подходы к оценке надежности не предполагают анализа и учета угроз информационной безопасности. И, как следствие, анализ угроз информационной безопасности производится уже после завершения проектирования и расчета уровня надежности системы [1–3]. Такой подход не позволяет получить адекватное представление об уровне надежности для проектируемой системы в целом и может приводить к значительному завышению оценки уровня надежности системы на этапе ее проектирования, что неприемлемо для критически важных систем.

В данной работе предложена методика учета возможных угроз информационной безопасности при расчете уровня надежности, что позволяет получать адекватные оценки надежности сложной системы еще на этапе ее проектирования.

Метод оценки надежности

В качестве примера сложной, критически важной системы рассмотрена современная европейская система автоматизированного управления движением железнодорожным транспортом ERTMS (European Rail Traffic Management System). Анализ влияния угроз информационной безопасности на оценку уровня надежности систем произведен на примере подсистемы ETCS (European Train Control System) европейской системы управления следованием поездов, активно использующейся на территории Европы.

Подсистема ETCS предназначена для автоматизированного (или автоматического) управления железнодорожным движением, что позволяет значительно повысить эффективность железнодорожных перевозок. В данной системе используются унифицированные протоколы обмена данными между поездом и специализированными устройствами, расположенными на путях, что позволяет принимать оперативные решения по организации и управлению движением.

Система ETCS разделена на две основные части: подсистема на стороне путей и подсистема на стороне поезда. Элементами, обеспечивающими обработку и передачу информации в системе ETCS, являются метки Eurobalise, шлейфы Euroloop, средства радиосвязи Euroradio, локомотивное оборудование Eurocab [4].

Система ETCS может функционировать на нескольких уровнях, которые различаются степенью автоматизации управления поездом. Нулевой уровень характеризует ручной режим управления, однако и на нем, так же как и на всех остальных, при движении состава обрабатывается информация с путевых радиочастотных

меток Eurobalise. Таким образом, подсистема радиочастотных путевых меток является одной из наиболее важных в рассматриваемой системе управления движением поездов. Рассмотрим более подробно эту подсистему, расположенную на стороне путей.

Eurobalise (иногда называемая Balise) — это радиочастотная путевая метка, устанавливаемая на железнодорожных путях. Она является частью системы ETCS и служит для передачи поезду данных, связанных с его текущим местонахождением. Метка хранит такую информацию, как идентификатор, соответствующий точке пути, рекомендуемые параметры движения по участку пути и др. В некоторых случаях путевая метка может предупреждать о ведущихся впереди работах и передавать новое (уменьшенное) значение скорости для участка пути. Метки могут устанавливаться группами из нескольких штук, например, для определения направления движения поезда [5].

Путевая метка представляет собой небольшое устройство, окрашенное в желтый цвет и установленное на шпале между рельсами. По сути, Balise представляет собой пассивную RFID (Radio Frequency Identifier) метку с некоторой предварительно записанной информацией. Особенностью пассивных меток является то, что для работы метки не требуют стационарного питания. Энергия для работы метки получается за счет преобразования энергии излучения RFID-считывателя, расположенного на поезде.

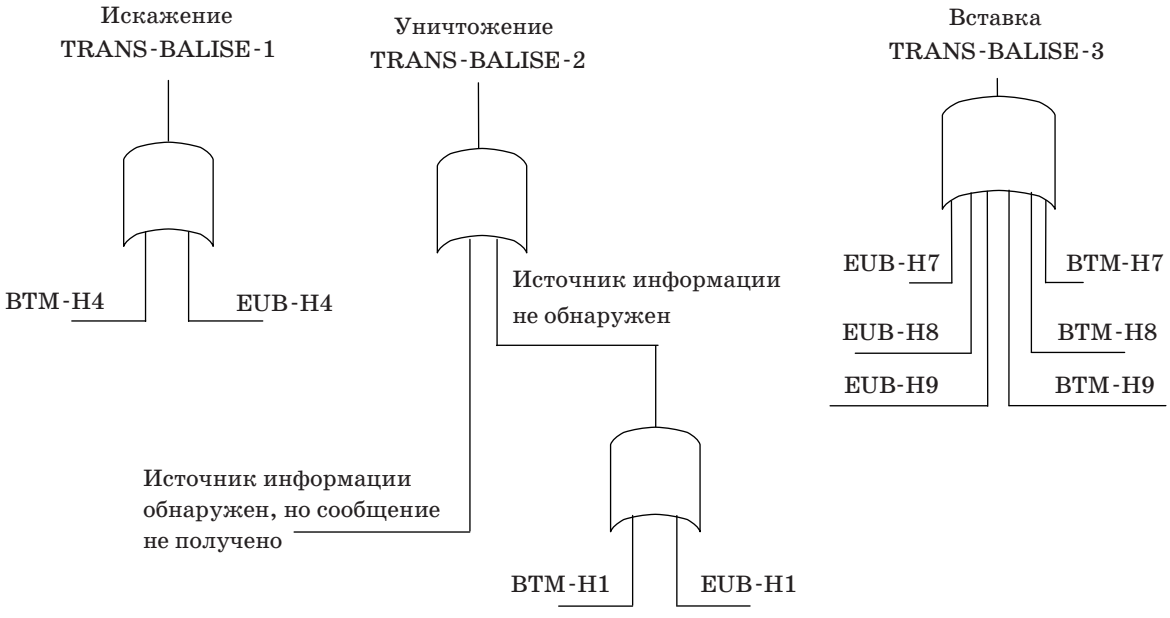
Такая особенность работы системы приводит к появлению угроз со стороны информационной безопасности. Например, при переносе на другое место метка не теряет работоспособности и будет передавать поезду некорректную информацию о его местонахождении. С учетом расположения в относительно легкодоступном месте (на путях следования поездов) она может представлять большой интерес для злоумышленника, целью которого может быть нарушение работы системы управления движением поездов. При более тщательном анализе работы системы могут быть выявлены и другие уязвимости информационной безопасности. При этом уровень надежности столь критически важной системы значительно снижается, а полученные традиционным способом оценки надежности не могут рассматриваться как адекватные.

Для повышения объективности получаемых оценок надежности системы предлагается при использовании стандартных подходов оценки уровня надежности учитывать угрозы информационной безопасности.

В соответствии со стандартом оценки уровня надежности [6] используется метод построения дерева отказов FTA (Fault Tree Analysis). Для подсистемы Eurobalise дерево, построенное в соответствии со стандартом [7], представлено на рис. 1. События, связанные с рисками отказов на стороне бортового оборудования, обозначены как BTM, другие события, связанные с рисками на стороне подсистемы Eurobalise, — EUB. Сами риски отказов интерпретируются следующим образом:

H1 — группа путевых меток (Eurobalise) не определена;

H4 — ошибочное сообщение интерпретировано как верное;



■ ***Рис. 1.*** Деревья отказов для подсистемы Eurobalise

H7 — ошибочная локализация группы путевых меток;

H8 — порядок получения корректных сообщений от путевых меток нарушен;

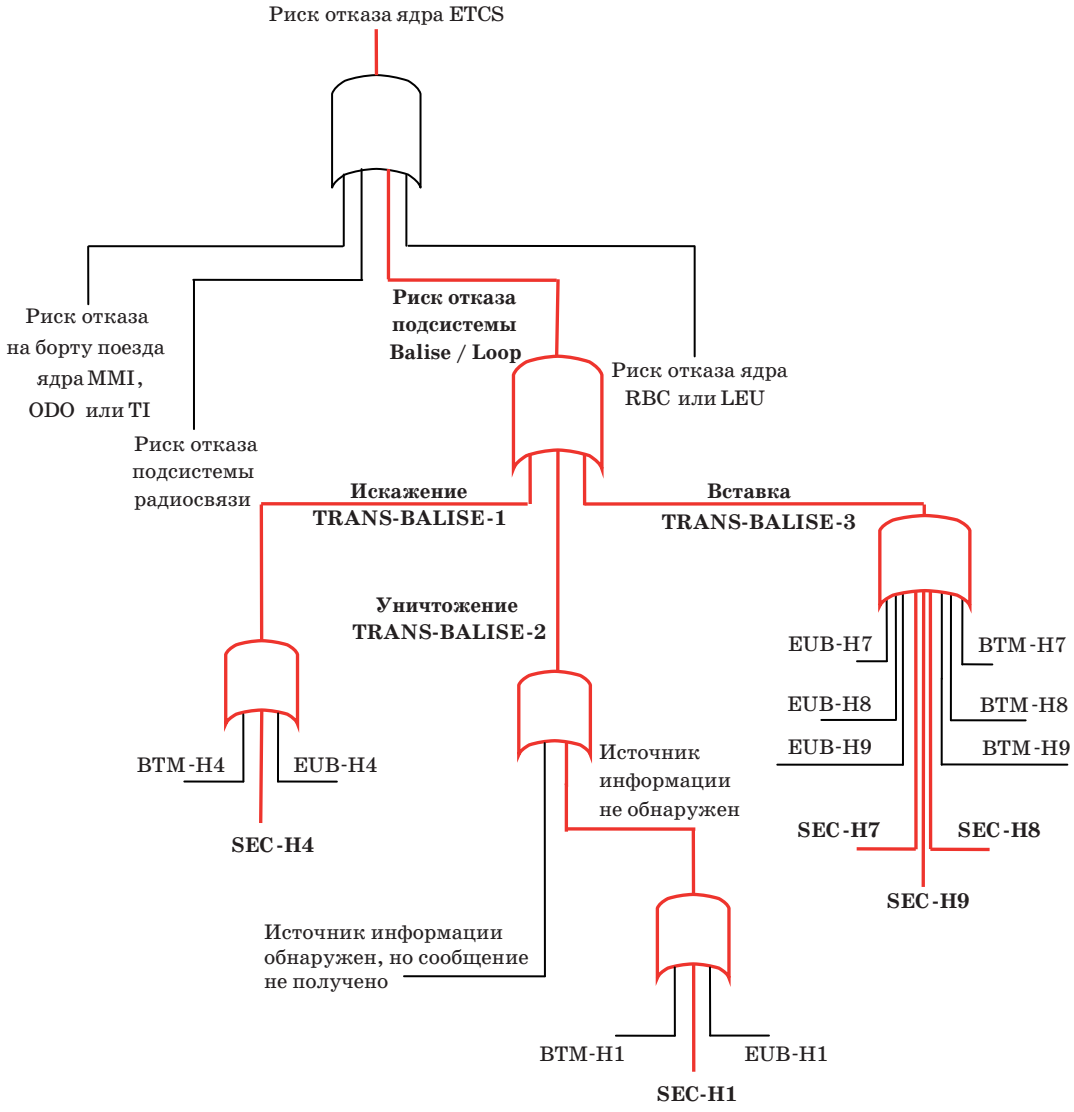
H9 — сообщение путевой метки ошибочно получено с другого пути.

Для учета угроз информационной безопасности добавим в дерево отказов некоторые из обнаруженных уязвимостей информационной безопасности. Так как стандартные риски отказов [7], рассматриваемые при анализе надежности, могут быть вызваны не только сбоем в работе оборудования, но и активными действиями злоумышленников, то дополним ими существующее дерево отказов отдельной ветвью (рис. 2), добавив к стандартному обозначению сокращение SEC (security).

Важно отметить, что в соответствии с теорией информационной безопасности для систем, в которых не предусмотрено никаких мер по обеспечению информационной безопасности, вероятность реализации опасности считается равной единице. В этом случае в соответствии с деревом отказов и вероятность отказа работы системы может быть близкой к единице, что значительно снижает уровень надежности системы.

Для увеличения уровня надежности необходимо применять меры по обеспечению информационной безопасности, а следовательно, использовать специальные методы и средства информационной безопасности.

Для учета влияния используемых средств обеспечения информационной безопасности на общий уровень надежности системы предлагается ввести в рассмотрение при анализе надежности специальный блок «модуль безопасности». В этом случае будем считать, что риски в сфере информационной безопасности учитываются именно



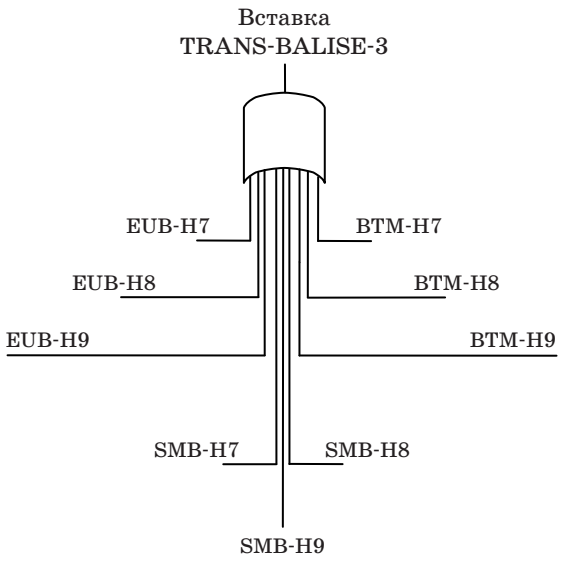
■ ***Рис. 2.*** Связь угроз с ядром системы

в этом блоке. Теперь отказ системы может произойти либо из-за взлома системы безопасности, либо из-за некорректной работы такого блока. В обоих случаях может быть получена оценка вероятности такого критического события. Данная оценка может быть использована в стандартной методике оценки надежности работы сложных систем. Применение данного подхода для ветви рассматриваемого дерева отказов, связанной со вставкой сообщения, показано на рис. 3, где угрозы со стороны модуля безопасности обозначены как SMB-H7, SMB-H8, SMB-H9 (SMB — security module block).

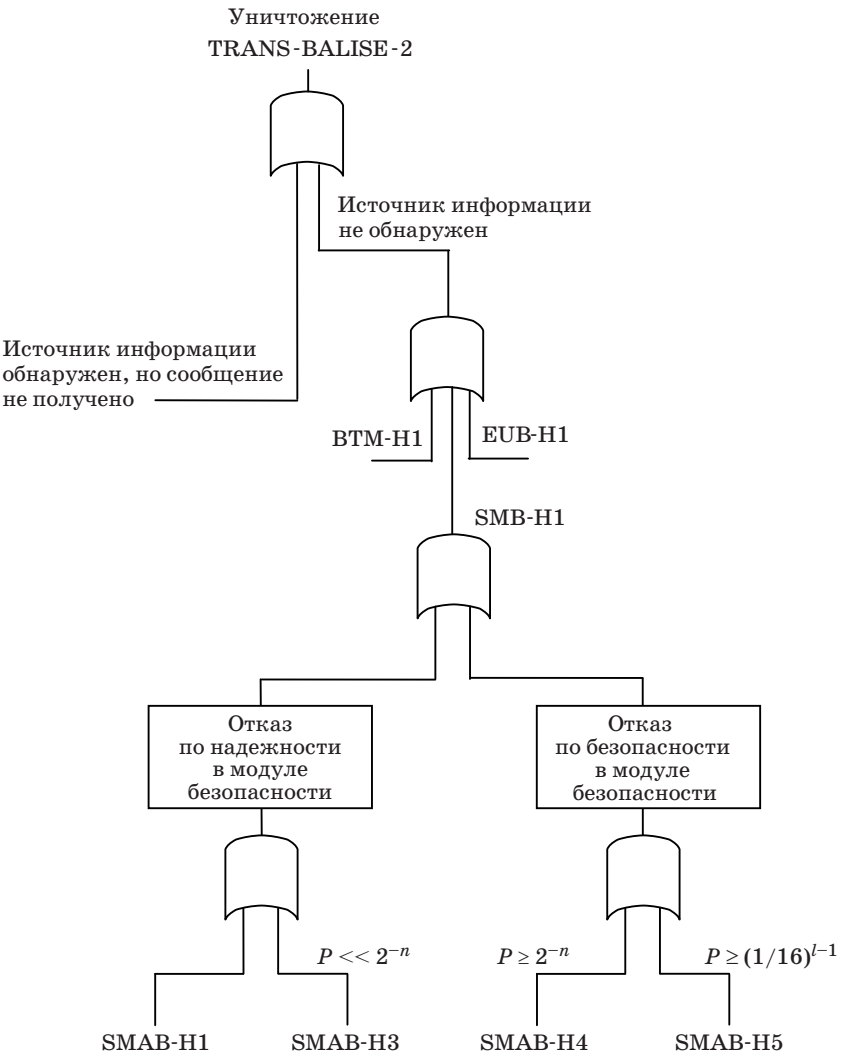
Для случая вставки сообщения (TRANS-BALISE-3) введены дополнительные события:

SMB-H7 — ошибочная локализация группы путевых меток по причине отказа модуля безопасности;

SMB-H8 — порядок получения корректных сообщений от путевых меток нарушен по причине отказа модуля безопасности;



■ ***Рис. 3.*** Дерево угроз с учетом наличия модуля безопасности



■ ***Рис. 4.*** Расчет дерева отказов с учетом надежности модуля безопасности

■ Перечень анализируемых опасностей

Тип угрозы	Обозначение	Описание угрозы	Причина сбоя
Угрозы со стороны сбоев модуля безопасности	SMAB-H1	Метка (Balise) не обнаружена	Сбой модуля безопасности
	SMAB-H2	Сбой аутентификации	То же
	SMAB-H3	Задержка	-"-
Угрозы, обусловленные успешными атаками	SMAB-H4	Успешная атака полным перебором	Реализация атаки
	SMAB-H5	Успешная атака десинхронизации	То же

SMB-H9 — сообщение путевой метки ошибочно получено с другого пути по причине отказа модуля безопасности.

Причины отказов модуля безопасности можно разделить на две группы: отказ по надежности и отказ по безопасности. При этом появляется возможность провести оценку вероятностей возникновения отказов с учетом влияния угроз информационной безопасности.

Для рассмотренного примера системы Eurobalise проведен анализ эффективности предложенного подхода при использовании безопасных протоколов обмена данными на пассивных RFID-метках LMAP++ [8, 9]. Для этого протокола можно оценить вероятность сбоя. Ветвь дерева отказов, связанная с уничтожением (потерей) сообщения, построенная с учетом влияния угроз информационной безопасности, представлена на рис. 4.

В данном случае проведен анализ угроз, связанных с модулем безопасности, реализующим протокол аутентификации: SMAB-H1, SMAB-H3, SMAB-H4, SMAB-H5 (SMAB — security module of authentication block). При этом приняты следующие обозначения: n — число бит, составляющих секретный ключ; l — число путевых меток в группе. Обозначения угроз введены по аналогии с угрозами, представленными в стандарте [7], однако причины возникновения этих угроз связаны с информационной безопасностью рассматриваемой системы. Полный список выявленных угроз приведен в таблице.

Вероятность возникновения угрозы, связанной с информационной безопасностью, можно оценить численно. Так, вероятность атаки перебором ключей (SMAB-H4) будет зависеть от размера ключа и составит величину 2^{-n}. Для одной путевой метки вероятность атаки десинхронизации на LMAP++ составляет 2^{-4}. В системе ETCS предусмотрено использование групп путевых меток, например, для определения направления движения состава. Вероятность десинхронизации для группы можно рассчитать по формуле $P_{\text{SMAB-H5}} = (2^{-4})^{l-1}$. Количество путевых меток в группе может составлять от 3 до 8, таким образом, вероятность успешной атаки десинхронизации будет лежать в диапазоне $2^{-28} \le P_{\text{SMAB-H5}} \le 2^{-8}$.

Проведенный анализ показывает, что результирующая надежность системы с учетом угроз информационной безопасности увеличивается при использовании модуля безопасности, а при отсутствии такого практически равна нулю.

Заключение

Приведенный в статье пример анализа уровня надежности системы управления, использующей элементы автоматизированных или автоматических информационных систем, показал, что при отсутствии учета угроз информационной безопасности получаемые оценки уровня надежности системы могут быть далеки от реальных, поскольку без применения методов и средств информационной безопасности вероятность отказа системы может оказаться близкой к единице. Для данной ситуации это означает, что реальная надежность такой системы в современных условиях может рассматриваться близкой к нулю.

Стоит отметить, что изложенная методика может быть применена для любых критически важных систем управления, в которых могут быть выявлены угрозы информационной безопасности.

Литература

1. **Hedberg K., Elestedt F.** Safety-critical Communication Controllers for Railway Signalling in Public Networks. — Chalmers University of Technology University of Gothenburg, Sweden, 2008. — 91 p.
2. **Novak T., Treytl A., Palensky P.** Common Approach to Functional Safety and System Security in Building Automation and Control Systems, Emerging Technologies and Factory Automation//ETFA. IEEE Conf., 2007. P. 1141–1148. doi:10.1109/EFTA.2007.4416910
3. **Zafar S., Dromey R. G.** Integrating Safety and Security Requirements into Design of an Embedded System// Proc. of 12th Asia-Pacific Software Engineering Conf. (APSEC '05), 2005. P. 629–636. doi:10.1109/APSEC.2005.75
4. **ETCS** Implementation Handbook. — Paris: UIC, 2008. — 91 p.

5. **FFFIS** for Eurobalise. ERTMS/ETCS — Class 1, Subset 036. — UNISIG, 2007. — 170 p.
6. **Unisig** Causal Analysis Process. ERTMS/ETCS — Class 1, Subset 077. — UNISIG, 2003. — 21 p.
7. **Safety** Analysis. ERTMS/ETCS — Class 1, Subset 088. — UNISIG, 2008. — 253 p.
8. **Safkhani M., Bagheri N., Naderi M., Sanadhya S. K.** Security Analysis of LMAP++, an RFID Authentication Protocol// Proc. of 6th Intern. Conf. on Internet Technology and Secured Transactions, 2011. P. 689–694.
9. **Bezzateev S., Voloshina N., Sankin P.** Joint Safety and Security Analysis for Complex Systems//Proc. of 13th Conf. of Open Innovations Association FRUCT and 2nd Regional Seminar on e-Tourism, Petrozavodsk, 2013. P. 3–13.

UDC 004.02

Safety Analysis Methodology of Complex Systems Taking Into Account the Threats to Information Security

Bezzateev S. V.[a], Dr. Sc., Tech., Head of Department, bsv@aanet.ru
Voloshina N. V.[a], PhD, Tech., Associate Professor, natali@vu.spb.ru
Sankin P. S.[a], Assistant, spetros@gmail.com
[a]Saint-Petersburg State University of Aerospace Instrumentation, 67, B. Morskaia St., 190000, Saint-Petersburg, Russian Federation

Purpose: The objective is to develop a methodology of reliability calculation of complex systems which takes into account information security threats. **Results:** There have been stated tasks of reliability calculation solved during the stage of complex systems design. Fault tree analysis is one of the most effective formal methods allowing to get numerical reliability values of a system, however it does not consider the problems associated with information security and their significant influence on operability of a system. To provide comprehensive assessment of reliability and security of complex systems during their design it has been proposed to develop a fault tree with account of information security threats. In particular, there has been introduced an additional system unit taking into account the influence of information security threats on a safety level of the whole system. Therefore, there has been proposed a solution of the problem of joint provision of systems' reliability and security. There has been conducted a joint reliability and security analysis of a subsystem of the complex ETCS system. Eurobalise subsystem based on RFID technology has been taken as an example. **Practical relevance:** The proposed methodology of taking into account information security threats while calculating system reliability provides more adequate assessment of reliability at the design stage of complex systems.

Keywords — Reliability of Complex Systems, Information Security Threats, Fault Tree Analysis.

References

1. Hedberg K., Elestedt F. *Safety-critical Communication Controllers for Railway Signalling in Public Networks*. Chalmers University of Technology University of Gothenburg, Sweden, 2008. 91 p.
2. Novak T., Treytl A., Palensky P. Common Approach to Functional Safety and System Security in Building Automation and Control Systems. *ETFA*. IEEE Conf., 2007, pp. 1141–1148. doi:10.1109/EFTA.2007.4416910
3. Zafar S., Dromey R. G. Integrating Safety and Security Requirements into Design of an Embedded System. *Proc. of 12th Asia-Pacific Software Engineering Conf. (APSEC '05)*, 2005, pp. 629–636. doi:10.1109/APSEC.2005.75
4. *ETCS Implementation Handbook*. Paris, UIC, 2008. 91 p.
5. FFFIS for Eurobalise. ERTMS/ETCS — Class 1, Subset 036. UNISIG, 2007. 170 p.
6. Unisig Causal Analysis Process. ERTMS/ETCS — Class 1, Subset 077. UNISIG, 2003. 21 p.
7. Safety Analysis. ERTMS/ETCS — Class 1, Subset 088. UNISIG, 2008. 253 p.
8. Safkhani M., Bagheri N., Naderi M., Sanadhya S. K. Security Analysis of LMAP++, an RFID Authentication Protocol. *Proc. of 6th Intern. Conf. on Internet Technology and Secured Transactions*, 2011, pp. 689–694.
9. Bezzateev S., Voloshina N., Sankin P. Joint Safety and Security Analysis for Complex Systems. *Proc. of 13th Conf. of Open Innovations Association FRUCT and 2nd Regional Seminar on e-Tourism*. Petrozavodsk, Russia, 2013, pp. 3–13.