УДК 004.9.621+006

О.А. ИЛЬЯШЕНКО[1], В.С. ХАРЧЕНКО[1], Г. ЕРВАН[2]

[1] *Национальный аэрокосмический университет им. Н.Е. Жуковского «ХАИ», Украина*
[2] *Таллиннский Технический Университет, Эстония*

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ИНДУСТРИАЛЬНЫХ ИУС НА FPGA: НОРМАТИВНАЯ БАЗА И SIS ПОДХОД

В работе рассматривается нормативный аспект регулирования информационной безопасности (ИБ) и кибербезопасности промышленных информационно-управляющих систем (ИУС) на программируемых логических интегральных схемах (ПЛИС) типа field programmable gate arrays (FPGA). Проанализированы стандарты, касающиеся различных аспектов ИБ ИУС на FPGA: общие вопросы обеспечения ИБ, документы по технологии FPGA, документы по регулированию ИБ и кибербезопасности FPGA, документы по регулированию кибербезопасности, а также проведен анализ литературы и научных исследований по данной тематике. В статье проанализированы аспекты security informed safety (SIS) подхода.

Ключевые слова: *ПЛИС, FPGA, информационная безопасность, кибербезопасность, регулирование, индустриальные информационно-управляющие системы, security informed safety.*

Введение

В настоящее время для реализации индустриальных ИУС критического применения широко используются элементная база программируемой логики (ПЛИС). Среди всех ПЛИС большое применение нашел тип FPGA. FPGA представляет собой универсальное полупроводниковое устройство, состоящее из массива взаимосвязанных функциональных блоков, которые можно запрограммировать и перепрограммировать впоследствии для выполнения любых логических функций в рамках ресурсов кристаллов [1]. Цифровые проекты на FPGA представляют сложные решения, которые включают программные и аппаратные компоненты.

Использование FPGA в критических системах (safety-critical, mission-critical, business-critical systems и т.д.) вносит некоторые специфические риски для функциональной [2-5] и информационной безопасности [6-9] таких систем.

Одной из важных задач, появившихся с динамично нарастающим внедрением FPGA в ИУС критического применения, является необходимость разработки методов и техник для оценивания и средств для обеспечения ИБ и кибербезопасности ИУС промышленного и критического применения на ПЛИС. Оценка в любых критических ИУС (ИУС АЭС) базируется на достаточно консервативной и жесткой нормативной базе.

Целью работы является анализ аспектов регулирования ИБ и кибербезопасности индустриальных ИУС на FPGA. В первую очередь статья ориентирована на ИУС АЭС.

1. Нормативное регулирование аспектов информационной безопасности FPGA

Проведем анализ нормативных документов, касающихся регулирования аспектов ИБ и кибербезопасности ИУС на FPGA. Исходя из иерархии «информационная безопасность ИУС-ИУС на FPGA-информационная безопасность ИУС на FPGA» они разделены на группы.

1.1. Документы, относящиеся к информационной безопасности в целом

ИБ и кибербезопасность могут быть достигнуты посредством соблюдения набора активностей, которые определены в международных и национальных стандартах, а также в нормативных документах предприятий.

В рамках международных нормативных документов [10-13] ИБ определяется, как защитный механизм, который обеспечивает:

– конфиденциальность (информация не доступна или закрыта от посторонних лиц, объектов или процессов);

– целостность (защита точности и полноты информации и методов обработки);

– аутентичность (или достоверность - уверенность, что информация получена из правильного источника и/или система доверяет исходному коду);

– доступность (обеспечивается доступ к информации и связанных с ней активов авторизованных пользователей по мере необходимости);

– надежность (сущности, участвующие в обработке информации или связи и не должны иметь возможность отказа в обмене данными).

Для понимания и правильной трактовки сущности ИБ далее приведены базовые определения, которые взяты из стандарта по информационной безопасности международной организации по стандартизации и международной электротехнической комиссии ISO/IEC 27000, Information technology – Security techniques – Information security management systems – Overview and vocabulary [11]: *актив* (asset) определяется, как «все, что имеет ценность для организации». В данном контексте, активом является информация о проекте на FPGA. Под *атакой* понимается «попытка уничтожить, разоблачить, изменить, отключить, украсть или получить несанкционированный доступ или несанкционированно использовать актив». *Угроза* представляет собой «потенциальную причину нежелательных инцидентов, которые могут привести к нанесению вреда системе или организации». *Уязвимость* понимается, как «слабость актива, или контрмеры, которая может быть использована угрозой».

В данной категории можно также выделить стандарт ISO/IEC 15408 [14] Общие критерии оценки защищённости информационных технологий, который известен, как Общие критерии (Common Criteria, CC или ОК). Common Criteria не приводит списка требований по безопасности или списка особенностей, которые должен содержать продукт. В нем описана инфраструктура (framework), в которой пользователи компьютерной системы могут описать требования, разработчики могут заявить о свойствах безопасности продуктов, а эксперты по безопасности определить, удовлетворяет ли продукт заявлениям. Таким образом Common Criteria позволяет обеспечить условия, в которых процесс описания, разработки и проверки продукта будет произведён с необходимой скрупулёзностью.

1.2. Документы, относящиеся к технологии FPGA

На сегодняшний день, фактически, не существует специальных нормативных документов, регулирующих вопросы информационной безопасности FPGA.

Однако к данной категории документов можно отнести отчет NUREG/CR 7006 [15], представляющий собой подборку методов проектирования безопасных FPGA. Данные методы могут быть использованы сотрудниками Комиссии ядерного надзора США (NRC, The Nuclear Regulatory Commission (NRC)) в качестве руководства для аудита систем, важных для безопасности, выполненных на базе FPGA и применяемых на АЭС. Данный документ фокусируется как на перечислении и описании методов проектирования FPGA, которые являются потенциально небезопасными, так и на принятии решения, какие методы могут быть допустимы для проектирования систем, важных для безопасности [16].

В рассматриваемой категории нормативных документов также можно выделить стандарт IEC 62566 [17], который сфокусирован на деятельность, направленную на HDL-основанные интегральные схемы (разработанные с помощью HDL и соответствующих программных средств) в течение проектирования ИУС на базе FPGA.

1.3. Документы, относящиеся к информационной и кибербезопасности FPGA

К этой категории можно отнести несколько технических отчетов, подготовленных Electric Power Research Institute [18-19] в попытке оказать помощь организациям в понимании, оценке и применении FPGA технологии в ИУС АЭС (TR 1019181 "Guidelines on the Use of Field Programmable Gate Arrays (FPGAs) in Nuclear Power Plant I&C Systems" – "Руководства по использованию программируемых логических интегральных схем (ПЛИС) в ИУС АЭС" и TR 1022983 " Recommended Approaches and Design Criteria for Application of Field Programmable Gate Arrays in Nuclear Power Plant Instrumentation and Control Systems" – "Рекомендуемые подходы и критерии проектирования для применения программируемых логических интегральных схем в информационно-управляющих системах атомных электростанций").

В документах также рассматриваются вопросы регулирования использования FPGA при модернизации уже существующих и при проектировании новых ИУС АЭС. В отчетах описаны преимущества и ограничения технологии FPGA на основе практического опыта и уроков, извлеченных из предыдущих приложений. Предоставляется руководство по планированию и проектированию изменений, вносимых в ИУС с использованием FPGA технологии. Также содержится руководство по специфицированию и выбору FPGA-основанных систем с подробным описанием ЖЦ требований, проектирования, верификации и валидации. TR 10229831 [19] основывается на более раннем TR 1019181 [18]. Рекомендуемые подходы и критерии проектирования для применения программируемых логических интегральных схем в информационно-управляющих системах атомных электростанций [19] включают в себя обсуждение воздействия FPGA на общую архитектуру ИУС АЭС и использование FPGA-

основанных решений для поддержки стратегий защиты, таких как диверсность, защита в глубину и защита от угроз кибербезопасности.

1.4. Источники, относящиеся к информационной безопасности FPGA

В современной литературе, относящейся к исследованиям проблем в области ИБ и кибербезопасности FPGA, можно выделить несколько основных источников [6,20]. В [6] проведен базовый анализ и описание проблем кибербезопасности FPGA технологии. Он сочетает в себе теоретические основы и практический подход к управлению безопасностью в проектах FPGA для исследований и применения в области цифрового проектирования с помощью автоматизированных средств проектирования CAD (Computer-Aided Design), и содержит примеры борьбы с реальными угрозами.

В [20] описывается несколько подходов к обеспечению кибербезопасности FPGA на логическом, архитектурном, и системном уровнях для того, чтобы представить общее решение к её обеспечению. Проведено описание атак на каждом уровне представления FPGA с приведением некоторых контрмер. Особое внимание уделяется атакам по сторонним каналам (side-channel attacks), главным образом, фокусируя внимание на таких типах пассивных атак, как разностные атаки по мощности (differential power analysis) и атаки по электромагнитному излучению (electromagnetic analysis attacks). Источник дает хорошее представление о различных практических методах, которые могут быть использованы в реконфигурируемых платформах на базе FPGA.

Анализ проблем ИБ, которые являются уникальными для встроенных систем на основе FPGA (embedded FPGA-based systems), представлен в [21]. Описывается и обосновывается важность и уникальность проблем ИБ во встроенных системах, перечисление требований к ИБ, концепции, и практики проектирования таких систем. Однако работа ограничена требованиями к процессу обеспечения ИБ и архитектуре, иллюстрируя популярный пример с SSL протоколом и обработкой рабочей нагрузки.

Представление концепции проектирования информационно-защищенной аппаратной части во встроенных системах описано в [22]. Приводятся описания основных классов атак и примеры мышления злоумышленников вместе с примерами предыдущих атак на аппаратную реализацию. Описывается типичный цикл разработки продукта и рекомендации относительно объединения ИБ, оценки рисков и политик безопасности.

Исследование различных аспектов ИБ, связанных с физическими неклонируемыми функциями, практические аспекты аппаратно-основанной криптографии, а также проблемы, связанные с применением политик безопасности, вопросы бесконтактных архитектур и применение ИБ-архитектур во встроенных системах рассматриваются в [23].

В [1] подчеркивается важность применения аутентифицированных конфигураций, как дополнительных возможностей FPGA, предлагается протокол ИБ для удаленной реконфигурации FPGA-основанных систем по небезопасным сетям. Обсуждаются некоторые проблемы, относящиеся к воспроизведению и сравнению решений на FPGA. Платежные системы, как повсеместно используемые устройства, исследуются и оцениваются в рамках уязвимостей ИБ, включая атаки «человек посередине» (man-in-the-middle).

1.5. Нормативные документы, относящиеся к обеспечению кибербезопасности индустриальных ИУС

В общем случае, подходы к обеспечению кибербезопасности индустриальных ИУС во многих аспектах совместимы с подходами, которые используются для обеспечения кибербезопасности SCADA систем или систем диспетчерского управления и сбора данных. Требования к кибербезопасности и методологии оценки рисков для промышленных ИУС и SCADA адаптированы из требований для IT систем. [24] В данной категории опубликовано большое количество руководящих документов [12,13, 25-32]. Среди которых NIST SP 800-30 [26], NIST SP 800-37 [27] и NIST 800-39 [28] представляют описание методов оценки рисков, NIST 800-53 [29] и NIST 800-53A [30] адресуют управление ИБ к IT системам. NIST SP 800-82 [32] описывает разницу между IT системами и ИУС и предоставляет руководство для защиты ИУС, включая SCADA системы, распределённые системы управления (англ. Distributed control system, DCS) и другие системы, выполняющие функции управления. Поскольку NIST 800-82 обозначает разницу между IT системами и ИУС, детали методов оценки рисков для ИУС должны быть модифицированы от аналогичных для IT систем.

2. Security informed safety

В настоящее время все более широкое использование находит принцип «security informed safety», SIS (пер. с англ. «информирование функциональной безопасности посредством информационной безопасности») для систем с интенсивным использованием данных (data-intensive systems) по аналогии с риск-ориентированным подходом (risk-informed ap-

proach), который уже активно используется в системах критического применения и не только в ИУС АЭС.

Суть подхода заключается в следующем: для ИУС критического применения, важных для безопасности (safety-critical I&C systems), основным свойством является функциональная безопасность (safety). Остальные свойства ИУС (надежность, подсвойства ИБ - целостность, конфиденциальность, а также готовность и др.) располагаются на следующем уровне иерархии. Таким образом, среди «подчиненных» топ-атрибуту функциональной безопасности свойств располагаются ИБ и кибербезопасность. Указанное отношение иерархии установлено в ряде работ [33,34] и понятие SIS, фактически, формализует данную иерархию посредством детального анализа данных об ИБ и кибербезопасности в интересах обеспечения функциональной безопасности.

Принцип SIS должен быть реализован для индустриальных ИУС критического применения на FPGA (например, ИУС АЭС) с учетом особенностей технологии и процессно-продуктных аспектов ИУС, например:

– для обеспечения защиты в глубину (defence in depth) как архитектурного принципа построения ИУС;

– для создания унифицированной методологии оценки угроз и уязвимостей для систем функциональной и информационной безопасности ИУС и т.д.

Управление ИБ и кибербезопасностью в системах критического применения в чем-то похоже на методы и техники, которые описаны в стандартах по направлению функциональной безопасности. Вместе с тем, концепция управления ИБ и кибербезопасностью охватывает широкий спектр различных мероприятий, покрывающих процесс, продукт и организацию. В противоположность этому, стандарты функциональной безопасности, как правило, основываются на модели жизненного цикла. В данном контексте принцип SIS должен соотносить подходы к снижению риска функциональной безопасности с управлением ИБ и кибербезопасностью, но для того, чтобы выполнить такой анализ необходимо определить общий способ классификации средств управления и снижения риска, принимая во внимание специфику технологии FPGA.

Заключение

Для индустриальных ИУС на FPGA (особенно в системах критического применения и важных для безопасности) должно быть обеспечено их функционально и информационно безопасное функционирование. Обеспечение ИБ и кибербезопасности таких систем представляет собой итеративный процесс, а не одноразовое решение.

В статье рассмотрены и проанализированы нормативные документы, касающиеся регулирования ИУС на FPGA в индустриальном секторе. На основании проведенного анализа можно сделать вывод о том, что на данный момент отсутствуют нормативные документы по регулированию вопросов ИБ и кибербезопасности промышленных ИУС на FPGA, а также методы и средства анализа и обеспечения ИБ и кибербезопасности таких систем, которые бы принимали во внимание специфику технологии FPGA.

В работе представлены некоторые аспекты принципа обеспечения функциональной безопасности посредством обеспечения информационной безопасности SIS (security informed safety), определены направления реализации данного принципа применительно для ИУС критического применения на FPGA.

Для обеспечения ИБ и кибербезопасности ИУС на FPGA, кроме мер по обеспечению ИБ и кибербезопасности самого кристала непосредственно, необходимо обеспечивать и ИБ и кибербезопасность всей системы в целом, в которую входит FPGA. Следует обратить внимание на ряд принципиальных различий в нормировании и оценивании ИБ для индустриальных ИУС и обычных ИТ-систем. В первом случае должен быть реализован жесткий процессно-продуктный подход, исходя из жизненного цикла функциональной безопасности, описанного в стандарте IEC61508.

Дальнейшие исследования будут направлены на разработку методов и средств оценки и обеспечения ИБ и кибербезопасности промышленных ИУС на FPGA.

Литература

1. Drimer, S. Security for volatile FPGAs [Text] / S. Drimer // UCAM CL-TR-763, University of Cambridge.– Cambridge, 2009. – 169 p.

2. NPP I&Cs: Problems of Safety [Text] / M.A. Yastrebenetsky (edit.) – Ukraine, Kyiv, Technics, 2004. – 427 p. (translated in USA by NPC, 2007).

3. FPGA-based NPP I&C Systems: Development and Safety assessment [Text] / E.S. Bakhmach, A.D. Herasimenko, V.A. Golovyr, V.S. Kharchenko, Yu.V. Rozen, A.A. Siora, V.V. Sklyar, V.I. Tokarev, S.V. Vinogradskaya, M.A. Yastrebenetsky. – RPC Radiy, National Aerospace University "KhAI", SSTC on Nuclear and Radiation Safety, 2008. – 188 p.

4. Kharchenko, V.S. Diversity-scalable decisions for FPGA-based safety-critical I&CS: From Theory to Implementation [Text] / V.S. Kharchenko, A.A. Siora, E.S. Bakhmach // NPIC&HMIT 2009, Knoxville, USA, April 5-9, 2009, unpublished.

5. Sklyar, V. Cyber Security of Safety-Critical Infra-

structures: a Case Study for Nuclear Facilities [Text] / V. Sklyar // Information & Security An international Journal. – 2012. – Vol. 28, No.1. – P. 98-117.

6. Handbook of FPGA Design Security [Text] / T. Huffmire, C. Irvine, T.D. Nguyen, T. Levin, R. Kastner, T. Sherwood. – Springer Dordrecht Heidelberg London New York, 2010. – 177 p.

7. Wollinger, T. How Secure are FPGAs in Cryptographic applications [Text] / T. Wollinger, C. Paar // Field Programmable Logic and Application, Lecture Notes in Computer Science Volume 2778, Springer Berlin Heidelberg. – 2003. – P. 91-100.

8. Skorobogatov, S. Breakthrough silicon scanning discovers backdoor in military chip (DRAFT of 05 March 2012) [Электронный ресурс] / S. Skorobogatov, C. Woods. – Режим доступа: http://www.cl.cam.ac.uk/~sps32/Silicon_scan_draft.pdf. - 21.8.2013.

9. Skorobogatov, S. Semi-invasive attacks A new approach to hardware security analysis [Text] / S. Skorobogatov / University of Cambridge: UCAM-CL-TR-630; ISSN 1476-2986, 2005. – 144 p.

10. ISO/IEC 13335-1. Information technology - Security techniques - Management of information and communications technology security - Part 1: Concepts and models for information and communications technology security management [Text]. – International Organization for Standardization and International Electrotechnical Commission, 2004. – 180 p.

11. ISO/IEC 27000. Information technology – Security techniques – Information security management systems – Overview and vocabulary [Text]. – International Organization for Standardization and International Electrotechnical Commission, 2009. – 20 p.

12. ISO/IEC 27001. Information technology - Security techniques - Information security management systems - Requirements [Text]. – International Organization for Standardization and International Electrotechnical Commission, 2005. – 35 p.

13. ISO/IEC 27002. Information technology - Security techniques - Code of practice for information security management [Text]. – International Organization for Standardization and International Electrotechnical Commission, 2005 – 108 p.

14. ISO/IEC 15408. Information technology – Security techniques – Evaluation criteria for IT security – Part 1: Introduction and general model [Text]. – International Organization for Standardization and International Electrotechnical Commission, 2009. – 76 p.

15. NUREG/CR-7006. Review Guidelines for Field-Programmable Gate Arrays in Nuclear Power Plant Safety Systems [Text]. – Nuclear Regulatory Commission, Washington, 2010. – 94 p.

16. Брежнев, Е.В. Основы ИТ-инженерии безопасности критических инфраструктур. Практикум. [Text] / Е.В. Брежнев, О.А. Ильяшенко, А.А. Орехова / под ред. Харченко В.С. – Харьков: Национальный аэрокосмический университет "Харьковский авиационный институт", 2012. – 185 с.

17. IEC 62566. Nuclear Power Plants – Instrumentation and control important to safety – Hardware language aspects for systems performing category A functions [Text]. – International Electrotechnical Commission, 2010. – 47 p.

18. EPRI TR 1019181, Guidelines on the Use of Field Programmable Gate Arrays (FPGAs) in Nuclear Power Plant I&C Systems [Text]. – Electric Power Research Institute, 2009. – 216 p.

19. EPRI TR 1022983. Recommended Approaches and Design Criteria for Application of Field Programmable Gate Arrays in Nuclear Power Plant I&C Systems [Text]. - Electric Power Research Institute, 2011. – 140 p.

20. Security Trends for FPGAs: From Secured to Secure Reconfigurable Systems [Text] / B. Badrignans, J.L. Danger, V. Fischer, G. Gogniat, L. Torres. – Berlin: Springer, 2011. – 196 p.

21. Security in Embedded Systems: Design Challenges [Text] / S. Ravi, C. Irvine, T. Nguyen, T. Levin, R. Kastner // ACM Transactions on Embedded Computing Systems. – 2004. – Vol. 3, No. 3. – P. 461–491.

22. Practical Secure Hardware Design for Embedded Systems [Электронный ресурс] / Proc. of the 2004 Embedded Systems Conference, San Francisco, California, March 29 – April 1. – Режим доступа http://grandideastudio.com/wp-content/uploads/secure_embed_paper.pdf. – 17.06.2013.

23. Towards Hardware-Intrinsic Security: Foundations and Practice [Text] / A.-R. Sadeghi, D. Naccache (Eds.). – Berlin: Springer, 2010. - ISBN 978-3-642-14451-62010. - 407 p.

24. A cyber security risk assessment for the design of I&C systems in nuclear power plants [Text] / J.-G. Song, J.-W. Lee, C.-K. Lee, K.-C. Kwon, D.-Y. Lee // Nuclear Engineering and Technology. – 2012. – Vol. 44, No. 8. – P. 919-928.

25. ISO/IEC TR 19791:2010(E). Information technology - Security techniques - Security assessment of operational systems [Text]. – International Organization for Standardization and International Electrotechnical Commission, 2010 – 235 p.

26. NIST Special Publication 800-30, Risk Management Guide for Information Technology Systems [Text]. – National Institute of Standards and Technology, 2002 – 95 p.

27. NIST Special Publication 800-37 Revision 1, Guide for Applying the Risk Management Framework to Federal Information Systems [Text]. – National Institute of Standards and Technology, 2010. – 93 p.

28. NIST Special Publication 800-39, Managing Information Security Risk [Text]. – National Institute of Standards and Technology, 2011. – 88 p.

29. NIST Special Publication 800-53 Revision 4, Recommended Security Controls for Federal Information Systems [Text]. – National Institute of Standards and Technology, 2013. – 457 p.

30. NIST Special Publication 800-53A Revision 1, Guide for Assessing the Security Controls in Federal Information Systems [Text]. – National Institute of Standards and Technology, 2010. – 399 p.

31. NIST Special Publication 800-64 Revision 2, Se-

curity Considerations in the System Development Life Cycle [Text]. – National Institute of Standards and Technology, 2008. – 67 p.

32. NIST Special Publication 800-82 Revision 1, Guide to Industrial Control Systems (ICS) Security [Text]. – National Institute of Standards and Technology, 2013. – 170 p.

33. Харченко, В. Безопасность информационно-управляющих систем и инфраструктур Модели, методы и технологии [Текст] / В. Харченко, В. Скляр, Е. Брежнев. – Palmarium Academic Publishing, 2013. – 528 p.

34. Bloomfield, R. Security-Informed Safety: If It's Not Secure, It's Not Safe [Text] / R. Bloomfield, K. Netkachova, R. Stroud // Software Engineering for Resilient Systems Lecture Notes in Computer Science Volume 8166, Springer Berlin Heidelberg, 2013. – P. 17-32.

Поступила в редакцию 1.09.2013, рассмотрена на редколлегии 10.09.2013

Рецензент: д-р техн. наук, профессор Александр Владимирович Потий, АО «Институт информационных технологий», начальник кафедры «Радиоэлектронных систем пунктов управления Воздушных Сил», Харьковский университет Воздушных Сил им. И. Кожедуба, Харьков.

ІНФОРМАЦІЙНА БЕЗПЕКА ІНДУСТРІАЛЬНИХ ІУС НА FPGA: НОРМАТИВНА БАЗА І SIS ПІДХІД

О.О. Ілляшенко, В.С. Харченко, Г. Єрван

У роботі розглядається нормативний аспект регулювання інформаційної безпеки (ІБ) і кібербезпеки промислових інформаційно-керуючих систем (ІКС) на програмованих логічних інтегральних схемах (ПЛІС) типу field programmable gate arrays (FPGA). Проаналізовано стандарти, що стосуються різних аспектів ІБ ІКС на FPGA: загальні питання забезпечення ІБ, документи за технологією FPGA, документи з регулювання ІБ і кібербезпеки FPGA, документи з регулювання кібербезпеки, а також проведено аналіз літератури та наукових досліджень з даної тематики. Проаналізовано аспекти security informed safety (SIS) підходу.

Ключові слова: ПЛІС, FPGA, інформаційна безпека, кібербезпека, регулювання, промислові інформаційно-керуючі системи, security informed safety.

SECURITY OF INDUSTRIAL FPGA-BASED I&C SYSTEMS: NORMATIVE BASE AND SIS APPROACH

O.A. Illiashenko, V.S. Kharchenko, G. Jervan

The work is dedicated to the security and cyber security normative regulation aspect of industrial instrumentation and control systems (I&Cs) based on programmable logic devices (PLD) of field programmable gate arrays (FPGA) type. Standards that cover different aspects of FPGA-based I&Cs security and cyber security were analyzed: general questions of security assurance, FPGA technology documents, regulation of FPGA security and cyber security. The analysis of references and scientific state-of-the-art problems is shown. The security informed safety (SIS) approach is analysed.

Key words: PLD, FPGA, security, cyber security, regulation, industrial instrumentation and control systems, security informed safety.

Ильяшенко Олег Александрович – аспирант, ассистент каф. компьютерных систем и сетей, Национальный аэрокосмический университет им. Н.Е. Жуковского «Харьковский авиационный институт», Харьков, Украина, e-mail: o.illiashenko@csn.khai.edu

Харченко Вячеслав Сергеевич – д-р техн. наук, проф., заслуженный изобретатель Украины, зав. каф. компьютерных систем и сетей, Национальный аэрокосмический университет им. Н.Е. Жуковского «Харьковский авиационный институт», Харьков, Украина, e-mail: v.kharchenko@khai.edu

Герт Ерван (Gert Jervan) – доктор философии, профессор, декан ф-та информационных технологий, Таллиннский технический университет, Таллинн, Эстония, e-mail: gert.jervan@ttu.ee.