УДК 004.728 : 519.87

Е. В. БРЕЖНЕВ[1], А. А. КОВАЛЕНКО[2], О. А. ИЛЬЯШЕНКО[1]

[1] *Национальный аэрокосмический университет им. Н. Е. Жуковского «ХАИ», Украина*
[2] *ПАО «НПП «Радий», Украина*

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ИУС, ВАЖНЫХ ДЛЯ БЕЗОПАСНОСТИ: ПРОЦЕССНЫЙ ПОДХОД НА ОСНОВЕ СИСТЕМЫ МЕНЕДЖМЕНТА КАЧЕСТВА

Кибербезопасность любого продукта непосредственно связана с безопасностью среды, используемой для его создания, а также обеспечивается его свойствами и процессами разработки. В статье описан предлагаемый подход к разработке кибербезопасных приложений путем создания и имплементации процесса обеспечения информационной безопасности (ИБ) в компании-разработчике. Процесс обеспечения ИБ рассматривается как важный бизнес-процесс, входами которого являются ресурсы компании, а выходом – безопасный продукт, удовлетворяющий требованиям заказчика. Этот процесс должен разрабатываться с учетом других бизнес процессов компании, в рамках системы менеджмента качеством (СМК). Процесс обеспечения ИБ осуществляется с учетом множества внешних и внутренних факторов. Безопасная среда разработки является важным фактором разработки приложения. В статье рассмотрен пример создания среды в рамках специальной СМК Nuclear Quality Assurance (NQA).

Ключевые слова: *безопасность, продукт, процесс, СМК, активность, подход, аудит, дизайн, ИУС, доступ, мера.*

Введение

Аспект кибербезопасности при разработке индустриальных систем, применяемых для управления производством или сложными технологическими процессами, становится актуальным. Это обусловлено возрастающим количеством киберинцидентов, связанных с атаками на системы типы SCADA.

Анализ тенденций указывает на устойчивый рост числа атак на индустриальные системы, начиная с 2010 г. (после Stuxnet). Так, в феврале 2011 г. была проведена массивная атака «Night Dragon» на пять компаний по переработке нефти. В 2012 г. в ряде крупных компаний, работающих в банковской сфере Сирии, Ливана, Судана было обнаружено вредоносное ПО (червь Flame), предназначено для выполнения шпионских действий, записи переговоров, и проч. Таким образом, очевидна тенденция роста числа атак на индустриальные системы, которая в будущем будет стремительно увеличиваться.

Разработчики индустриальных систем стремятся повысить их защищенность от внешних атак, снизить риски для кибербезопасности и потенциальных уязвимостей. Имплементируя требования ИБ к системам, разработчики стремятся разработать безопасный продукт. Множество требований к ИБ можно разделить на: требования регулятора, нормативной базы, заказчика, пр. Довольно часто общая группа требований является несогласованной и не гармонизированной. Для компаний-разработчиков приложений одной из первоначальных задач является анализ требований, их систематизация и определение их приоритетов [1]. С учетом результатов этого анализа, компания-разработчик стремится разработать практические подходы, направленные на выполнение всего множества требований.

Следует отметить, что анализ требований и разработка подходов не являются единичными (отдельными) задачами. Очень часто приходится иметь дело со множеством согласованных задач, выходы и входы которых взаимосвязаны между собой. При этом, на основании статистических данных, около 74% организаций основывают свои механизмы проверки соответствия продукта / процесса требованиям по ИБ, выдвигаемым к нему, в основном с использованием мануальных методов и средств (текстовых редакторов, электронных таблиц, и т.д.), указывая на отсутствие существования удовлетворительных решений в 37% случаев [2, 3].

Таким образом, можно говорить о необходимости дизайна (разработки) процесса обеспечения ИБ продукта в компании и обеспечения его последующей автоматизации и поддержки программными средствами. Такой процесс является, по сути, одним из важных бизнес процессов компании, направленных на достижение удовлетворенности заказчика свойствами конечного продукта и на его кибербезопасность. Дизайн эффективного процесса обеспечения ИБ продукта может быть основан на использовании подходов к инжинирингу бизнес процес-

сов [4].

При разработке процессов ИБ в компании необходимо учитывать ее ресурсы, уровень подготовки персонала, требования к продукту, зрелость используемых технологий, пр. Важной основой для дизайна процесса является СМК, которая является важнейшей составляющей системы управления бизнесом. Она содержит описание всех бизнес процессов компании, направленных на получение качественной продукции.

Поскольку обеспечение ИБ также является важным бизнес процессом компании, то его дизайн необходимо проводить с учетом других процессов компании в рамках системы менеджмента качеством.

Целью данной работы является освещение разработки подхода к дизайну и имплементации процесса обеспечения ИБ продуктов в рамках СМК компании.

1. Описание процессного подхода к обеспечению ИБ

Представленный ниже процессный подход к обеспечению ИБ продукта применим для разработки ИУС АЭС.

1.1. Анализ требований к ИБ ИУС

ИУС АЭС являются примером индустриальных систем управления, к которым выдвигаются высокие требования к функциональной безопасности и ИБ. В частности, в США, Комиссия по ядерному регулированию (United States Nuclear Regulatory Commission, US NRC) в своей практике активно использует ряд документов, к наиболее важным из которых, с точки зрения ИБ, можно отнести следующие:

– 10 CFR Part 50, Appendix B, “Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants”;

– NQA-1a-2009 Quality Assurance Requirements for Nuclear Facility Applications;

– Regulatory Guide (RG) 1.152-2011, Revision 3, “Criteria for Use of Computers in Safety Systems of Nuclear Power Plants”;

– IEEE Std 7-4.3.2-2003, “IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations”;

– IEEE Std 603-1991 “Standard Criteria for Safety Systems for Nuclear Power Generating Stations”;

– DI&C-ISG-01, Revision 0, “Cyber Security Associated with Digital Instrumentation and Controls”;

– DI&C-ISG-06, Revision 1, “Licensing Process”;

– Regulatory Guide 5.71, “Cyber Security Programs for Nuclear Facilities”;

– IEEE Std 1074-2006, “IEEE Standard for Developing a Software Project Life Cycle Process”;

– NUREG/CR-7117, “Secure Network Design”;

– NIRMA TG-16;

– BTP 7-14, NUREG 6101.

Такие документы регламентируют множество аспектов, покрывая этапы, начиная с безопасной среды разработки и эксплуатации и заканчивая свойствами безопасности критических систем, включая ИБ. Однако, вопросы интеграции активностей, связанных с ИБ в модель жизненного цикла ИУС, остаются актуальными и нерешенными.

ИБ, в первую очередь, имеет непосредственное отношение к защитным мерам критических активов компании-разработчика, включая критические ИУС, от злоумышленных действий.

Стандарт IEEE Std 603-1991 акцентирует внимание на важности административных мер доступа к оборудованию ИУС, а также необходимости совместного использования средств ограничения физического и электронного доступа к критическим системам и данным с целью предотвращения несанкционированных изменений.

Отмечено, что безопасность программного обеспечения (ПО) компьютеризированных систем относится к возможности уцелеть вследствие несанкционированных, нежелательных, и небезопасных вмешательств на протяжении всего жизненного цикла таких систем.

Документы 10 CFR Part 50, Appendix B и 10 CFR 73.54, разработанные US NRC, представляют собой универсальные правила для лицензирования продукции и соответствующих предприятий на рынке США [5, 6].

Аспекты, относящиеся к кибербезопасности, покрываются документами RG 1.152-2011 [7] и RG 5.71-2010 [8]. Первый из них описывает приемлемый с точки зрения US NRC метод, позволяющий реализовать процесс лицензирования использования компьютеров в системах безопасности атомных электростанций (АЭС). В частности, он содержит критерии установления безопасных сред разработки и эксплуатации (SDOE) цифровых ИУС посредством соответствующих физических, логических, программных и административных мер. Второй документ содержит непосредственное руководство по реализации активностей по защите компьютеров и коммуникационных систем и сетей. Он основывается на международных и федеральных стандартах и относится к этапам функционирования и обслуживания АЭС.

Документ BTP 7-14 представляет собой руководство по обзорам ПО для цифровых ИУС и содержит основные определения, касающиеся понятий

безопасности и безопасности как функционального свойства. Вместе с тем он множество требований к документам планирования, каждый из которых содержит множество требований к ИБ.

Таким образом, существует множество требований к ИБ продукта. Их выполнение может быть достигнуто в рамках реализации одного из важных бизнес процессов компании – обеспечения ИБ. Дизайн процесса обеспечения ИБ должен проводиться с учетом взаимосвязи с другими процессами в компании. Процесс обеспечения ИБ должен стать интегральной частью СМК компании.

1.2. Сравнительный анализ СМК с учетом требований к процессу обеспечения ИБ

В общем случае, процесс обеспечения ИБ ИУС может быть реализован в рамках двух типов СМК: коммерческих и специальных (ядерных).

Коммерческие СМК. Традиционно, компании, работающие в отрасли информационных технологий, и не имеющие сертифицированный разрабатываемый продукт, к которому существуют требования ИБ, не используют все возможности СМК в обеспечении ИБ конечного продукта. Как правило, рассматривается продуктовая составляющая ИБ (соответствие требованиям к ИБ продукта). При таком подходе главный фокус делается на процесс тестирования безопасности для обеспечения удобоваримого качества продукта. Представители групп верификации являются представителями контроля качества в компании.

Стандарты ISO серии 9001, описывающие модель СМК, разработаны для того, чтобы помочь организациям удовлетворять требования и ожидания клиентов и иных заинтересованных сторон. В рамках ISO существует ряд требований, которые косвенно можно отнести к требованиям ИБ. Так, требования по управлению документированной информацией включают необходимость обеспечения мер для следующих пунктов:

– надлежащей защиты информации (например, от потери конфиденциальности, неправильного применения или потери целостности);

– управления документированной информацией (обеспечение доступа, хранение в надлежащем состоянии, контроль изменений, контроль версий);

– определения срока хранения и методов уничтожения. Документированная информация, сохраненная как свидетельство соответствия, должна быть защищена от непреднамеренных изменений.

Таким образом, в рамках ISO существует ряд требований к защите документированной информации от преднамеренных воздействий. Это единственное требование ИБ в рамках СМК ISO 9001.

Специфические СМК. Коммерческие СМК не выдвигают существенных требований к ИБ продукта. Более строгими в этом смысле являются специфические СМК, в которых главным фокусом является не удовлетворенность заказчика, а безопасность конечного продукта. В таких системах, важность уделяется бизнес процессам, важным с точки зрения выполнения продуктом функций безопасности.

Так, например, в США, компании, желающие продавать свой продукт на ядерном рынке, или стать поставщиком оборудования на АЭС должны иметь специфическую систему качества 10CFR50 Appendix B.

Стандарт по обеспечению качества в ядерной индустрии (NQA) является общим индустриальным стандартом, содержащим 18 критериев, соответствующих критериям 10 CFR 50 Appendix B. NQA содержит требования к построению всех процессов, важных для безопасности для соответствия требованиям 10 CFR 50 Appendix B.

Ядерная СМК уделяет больше внимания аспектам ИБ систем, важных для безопасности. Так, например, указывается, что требования к ПО должны содержать специфические требования (защиту от уязвимостей, кибербезопасность, защиту от несанкционированного доступа, пр.). Аспект ИБ конечного продукта учитывается на всем ЖЦ ПО. Стандарт также выделяет ряд отдельных требований к контролю доступа. Уделяется внимание безопасности сети и данных, требуется парольная защита. Следует отметить, что, поскольку ответственными за выполнение процедур и требований СМК являются менеджеры по качеству, то целесообразно усилить их вовлеченность в контроль процесса обеспечения ИБ.

Требования СМК в части ИБ усиливаются требованиями ряда документов типа Technical Guideline 16. Этот документ был разработан Nuclear Information and Records Management Association (NIRMA) с целью обзора лучших практик управления записями.

Документ содержит требования по:

– разработке программы ИБ записей;

– управлению правами доступа;

– безопасности сети;

– правлению правами изменения содержания.

2. Дизайн процесса обеспечения ИБ приложений на основе СМК

2.1. Основные элементы дизайна процесса обеспечения ИБ

В рамках разработки процесса обеспечения ИБ на основе СМК целесообразно создать:

– *процедуры и рабочие инструкции* по обеспе-

чению безопасности;

– *политику компании*, направленную на разработку безопасных приложений;

– *программу тренингов* с персоналом.

Процедура описывает процесс создания безопасных приложений. Целью процедуры является предоставление руководства для проектирования безопасных приложений с целью минимизации всех возможных уязвимостей, которые могут привести к невыполнению функций безопасности. Этот документ качества описывает методологию, направленную на выполнение требований по надежности, функциональной безопасности, качеству ПО, на создание безопасной среды разработки и эксплуатации. Документ описывает мероприятия, направленные на создание безопасной среды разработки приложения, ее защиты от недокументированных, нежелательных модификаций, защитных мер против любых действий, направленных на снижение рисков для надёжности и безопасности при эксплуатации.

Важной частью процесса обеспечения ИБ является создание среды для безопасной разработки и ее последующего применения. В рамках проекта разрабатываются план и отчет по обеспечению SDOE.

2.2. Подход к реализации безопасных сред разработки и эксплуатации для процесса обеспечения ИБ

Безопасная среда разработки определена как условие наличия соответствующих физических, логических и программных мер во время этапов разработки системы (рис. 1) для отсутствия возможности внесения нежелательной, излишней и недокументированной функциональности (например, избыточного кода) в цифровые системы, критические с точки зрения безопасности.

Безопасная среда функционирования определена как условие наличия соответствующих физических, логических и административных мер на предприятии для обеспечения надежного функционирования ИУС посредством отсутствия их деградации вследствие некорректного поведения подключенных систем, а также событий, порожденных непреднамеренным доступом к таким ИУС [8].

Для обеих сред, в общем случае, основными типами компонент являются следующие:

– *аппаратное обеспечение* (включая технические средства функционирования и обеспечения безопасности инфраструктур сред разработки и эксплуатации, оборудование разработки и эксплуатации);

– *программное обеспе*чение (включая то, которое относится к процессам разработки и эксплуатации, а также непосредственно к рассматриваемым инфраструктурам);

– *сеть передачи данных* (относящаяся как к среде разработки, так и эксплуатации);

– *персонал*;

– *продукт* (ИУС, которая разрабатывается и, затем, эксплуатируется).

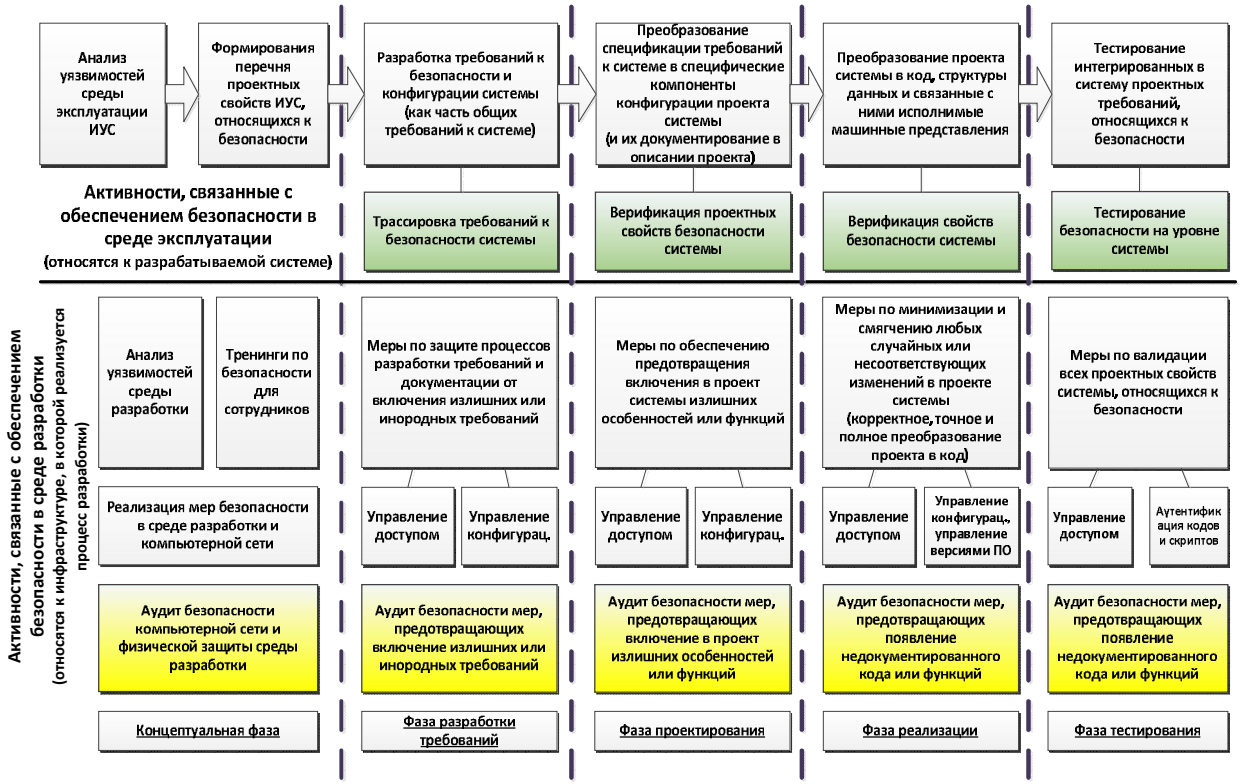

Рис. 1. Детализация активностей по обеспечению безопасных сред разработки и эксплуатации

Кроме вышеперечисленных типов компонент, немаловажным аспектом, подлежащим отдельному детальному анализу, является их конфигурация, которая включает множество факторов, охватывающих физические, логические и поведенческие взаимосвязи. Конфигурация в значительной степени зависит от качества и полноты внедрения СМК в средах разработки и эксплуатации, квалификации персонала, качества используемых программных и аппаратных компонент.

Реализация SDOE, в контексте документа RG 1.152-2011, относится к следующим аспектам:

– предпринятым мерам и средствам по реализации безопасной среды для разработки ИУС, критических с точки зрения безопасности, предотвращающим недокументированные, избыточные и нежелательные изменения;

– защитным мерам, предотвращающим предсказуемый набор нежелательных действий, которые могут повлиять на целостность, надежность или функциональность ИУС во время ее функционирования.

Фазы каскадной модели жизненного цикла позволяют сформировать структуру специальных руководств по защите цифровых систем, критических с точки зрения безопасности, а также по реализации SDOE посредством идентификации и смягчения потенциальных недостатков либо уязвимостей в каждой из фаз, которые могут привести к деградации SDOE или надежности таких систем.

Аудиты безопасности являются неотъемлемой частью процесса обеспечения безопасности во время разработки, реализации и поддержания SDOE. Такие аудиты включают в себя:

– *аудит среды разработки:* после учреждения инфраструктуры, в которой будет производиться разработка, и до начала проекта разработки ИУС;

– *периодические аудиты:* до начала каждой из фаз разработки.

Аудит среды разработки предназначен для оценки «базового» уровня безопасности среды разработки. Преимущественно, соответствующие меры реализуются техническими средствами и относятся к сетям такой инфраструктуры, задействованным в процессе разработки, физическим средствам защиты и т.д. В свою очередь, периодические аудиты предназначены для оценки дополнительных специфических мер, требуемых при реализации каждой из фаз разработки в жизненном цикле. Каждый из таких аудитов включает следующие этапы:

– проверка реализации дополнительных мер для фазы разработки (т.е. что реализовано и как);

– проверка соблюдения руководств и инструкций организации, относящихся к безопасной среде разработки, персоналом (т.е. практическая оценка того, следуют ли сотрудники соответствующим требованиям СМК).

Входом для каждого из аудитов является соответствующий план (и, возможно, документы, относящиеся к определенным аспектам организации среды разработки либо реализации процессов), а выходом – отчет по аудиту SDOE, в котором задокументированы полученные результаты.

Заключение

Обеспечение ИБ является важным бизнес-процессом компании. Его дизайн (разработку) необходимо проводить с учетом специфики компании, ее ресурсов и используемых технологий. Выходом этого процесса является продукт, удовлетворяющий заказчика с точки зрения качества. Процесс обеспечения ИБ должен быть реализован в рамках СМК компании. При дизайне процесса обеспечения ИБ необходимо создать безопасную среду разработки приложений. Основой для разработки безопасного приложения может стать создание безопасной среды разработки, основой которой может быть ядерная СМК и ее принципы.

Специалисты по ИБ компании должны работать вместе со специалистами по качеству, уделяя внимание проблемам безопасности приложений, управлению доступом, управлению записями и документами. В компании должны быть специалисты по качеству, понимающие важность рисков ИБ. СМК ориентирована на ИБ, группа ИБ – на качество.

Важным аспектом является внесение процесса создания и контроля безопасной среды разработки непосредственно в СМК. Таким образом, контроль разработки безопасной системы является совместной ответственностью менеджеров по качеству и специалистов по ИБ в компании. Для оценивания уровня гарантий ИБ среды разработки финального продукта предлагается использовать Advanced Security Assurance Case (ASAC) – подход, описанный [2]. Визуализация алгоритма оценивания позволит однозначно установить уровень гарантий ИБ процесса разработки (и финального продукта) как проектной командой разработчиков, так и провести внешний аудит безопасности третьей стороной.

Литература

1. Kharchenko, V. Security Assessment of FPGA-based Safety-Critical Systems: US NRC Requirements Context [Текст] / V. Kharchenko, A. Kovalenko, V. Sklyar, O. Siora // Proceedings of the International Conference on Information and Digital Technologies (IDT 2015) July 7-9 2015, Žilina, Slovakia. – IEEE, 2015. – P. 117-123.

2. Illiashenko, O. Advanced Security Assurance Case Based on ISO/IEC 15408 [Текст] / O. Illiashenko, O. Potii, D. Komin // Theory and Engineering of Complex Systems and Dependability : Proceedings of the Tenth International Conference on Dependability and Complex Systems DepCoS-RELCOMEX, Brunów, Poland, June 29 – July 3 2015. - Advances in Intelligent Systems and Computing, Vol. 365, Springer International Publishing, 2015. – P. 391 – 401, doi: 10.1007/978-3-319-19216-1_37.

3. Cyra, L. SCF - A Framework Supporting Achieving and Assessing Conformity with Standards [Текст] / L. Cyra, J. Gorski // Special Issue: Secure Semantic Web. – 2011. – № 33(1). – P. 80-95. doi:10.1016/j.csi.2010.03.007.

4. Yastrebenetsky, M. Nuclear Power Plant Instrumentation and Control Systems for Safety and Security [Текст] / V. Kharchenko, M. Yastrebenetsky // Advances in Environmental Engineering and Green Technologies (AEEGT) Book Series: Hershey. – Pennsylvania, United States of America, IGI Global, 2014. – 470 p.

5. 10 CFR 50, Appendix B. Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants [Электронный ресурс] ; введен 02.12.2015. – U.S. Nuclear Regulatory Commission, 2015. – Режим доступа: http://www.nrc.gov/reading-rm/doc-collections/cfr/part050/part050-appb.html. – 2.04.2016.

6. 10 CFR 73.54. Protection of digital computer and communication systems and networks [Электронный ресурс] ; введен 27.03.2009. – U.S. Nuclear Regulatory Commission, 2015. – Режим доступа: http://www.nrc.gov/reading-rm/doc-collections/cfr/part073/part073-0054.html. – 2.04.2016.

7. Regulatory Guide 1.152, Revision 3. Criteria for use of computers in safety systems of nuclear power plants; введен 01.07.2009. – Office of nuclear regulatory research. U.S. Nuclear Regulatory Commission, 2009. – 13 p.

8. Regulatory Guide 5.71, Cyber security programs for nuclear facilities ; введен 01.01.2010. – Office of nuclear regulatory research. U.S. Nuclear Regulatory Commission, 2010. – 105 p.

References

1. Kharchenko, V., Kovalenko, A., Sklyar, V., Siora, O. Security Assessment of FPGA-based Safety-Critical Systems: US NRC Requirements Context. *Proceedings of the International Conference on Information and Digital Technologies (IDT 2015),* July 7-9 2015, Žilina, Slovakia, IEEE, 2015, pp. 117-123. doi: 10.1109/DT.2015.7222963.

2. Illiashenko, O., Potii, O., Komin, D. Advanced Security Assurance Case Based on ISO/IEC 15408 *Theory and Engineering of Complex Systems and Dependability. Proceedings of the Tenth International Conference on Dependability and Complex Systems DepCoS-RELCOMEX*, Brunów, Poland, June 29 – July 3 2015. Advances in Intelligent Systems and Computing, vol. 365, Springer International Publishing, 2015, pp. 391-401. doi: 10.1007/978-3-319-19216-1_37.

3. Cyra, L., Gorski, J. SCF - A Framework Supporting Achieving and Assessing Conformity with Standards. *Special Issue: Secure Semantic Web*, 2011, vol. 33(1), pp. 80-95. doi:10.1016/j.csi.2010.03.007

4. Yastrebenetsky, M., Kharchenko, V. Nuclear Power Plant Instrumentation and Control Systems for Safety and Security. *Advances in Environmental Engineering and Green Technologies (AEEGT) Book Series: Hershey*, Pennsylvania, United States of America, IGI Global, 2014. 470 p.

5. *10 CFR 50, Appendix B. Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plant*. U.S. Nuclear Regulatory Commission, 2015. Available at: http://www.nrc.gov/reading-rm/doc-collections/cfr/part050/part050-appb.html (accessed 12.04.2016)

6. *10 CFR 73.54. Protection of digital computer and communication systems and networks*. U.S. Nuclear Regulatory Commission, 2015. Available at: http://www.nrc.gov/reading-rm/doc-collections/cfr/part073/part073-0054.html (accessed 12.04.2016)

7. *Regulatory Guide 1.152, Revision 3. Criteria for use of computers in safety systems of nuclear power plants*. Office of nuclear regulatory research, U.S. Nuclear Regulatory Commission, 2009. 13 p.

8. *Regulatory Guide 5.71, Cyber security programs for nuclear facilities*. Office of nuclear regulatory research, U.S. Nuclear Regulatory Commission, 2010. 105 p.

Поступила в редакцию 12.04.2016, рассмотрена на редколлегии 14.04.2016

ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙННОЇ БЕЗПЕКИ ІУС ВАЖЛИВИХ ДЛЯ БЕЗПЕКИ: ПРОЦЕСНИЙ ПІДХІД НА ОСНОВІ СИСТЕМИ МЕНЕДЖМЕНТУ ЯКОСТІ

Є. В. Брежнєв, А. А. Коваленко, О. О. Ілляшенко

Безпека любого продукту безпосередньо пов'язана з безпекою середовища, що використовується для його створення, а також забезпечується його властивостями і процесами розробки. В статті описано запропонований підхід до розробки кібербезпечних додатків шляхом створення та імплементації в компанії процесу забезпечення інформаційної безпеки (ІБ). Процес забезпечення ІБ розглядається як важливий бізнес-процес у компанії, входами якого є ресурси компанії, а виходом – безпечний продукт, що задовольняє заказ-

ника. Розглянуто приклад створення цього середовища в рамках спеціальної СМЯ NQA. СМЯ NQA являє собою сукупність методів і засобів контролю основних процесів, що впливають на безпеку кінцевого продукту (додатка).

Ключові слова: безпека, продукт, процес, СМЯ, активність, підхід, аудит, дизайн, ІУС, доступ, міра.

ASSURANCE OF CYBER SECURITY FOR I&C SYSTEMS IMPORTANT TO SAFETY: PROCESS APPROACH BASED ON QUALITY MANAGEMENT SYSTEM

E. V. Brezhniev, A. A. Kovalenko, O. A. Illiashenko

Security of any product is directly related to its development environment security, as well as assured by the product inherent properties and development processes. The approach of development of cyber-secured applications via creating and implementation of cyber security (CS) assurance process in a company is described in paper. CS assurance process is considered as an important business process in a company, the inputs are represented by company's resources, and output is a secured product, which satisfies the customer. An example of such environment establishment is considered in the scope of special NQA QMS. NQA QMS is a complex consisting of methods and tools intended for controlling the main processes, which have an impact on security of the final product (application).

Keywords: security, product, process, QMS, activity, approach, audit, design, I&C, access, controls.

Брежнев Евгений Витальевич – канд. техн. наук, доцент кафедры компьютерных систем и сетей, Национальный аэрокосмический университет им. Н. Е. Жуковского «ХАИ», Харьков, Украина, e-mail:e.brezhnev@csis.org.ua.

Коваленко Андрей Анатольевич – канд. техн. наук, доцент, старший научный сотрудник ПАО "НПП "Радий", Кировоград, Украина, e-mail: andriy_kovalenko@yahoo.com.

Ильяшенко Олег Александрович – ассистент, младший научный сотрудник кафедры компьютерных систем и сетей Национального аэрокосмического университета им. Н. Е. Жуковского «ХАИ», Харьков, Украина, e-mail: o.illiashenko@csn.khai.edu.

Brezhnev Eugene Vitalievich – Candidate of Technical Sciences, Assistant Professor of Department of Computer Systems and Networks, National Aerospace University n. a. N. Ye. Zhukovsky "KhAI", Kharkov, Ukraine, e-mail: e.brezhnev@csis.org.ua.

Kovalenko Andriy Anatol'evich – Candidate of Technical Science, Associate Professor, Senior Researcher, RPC Radiy, Kirovograd, Ukraine, e-mail: andriy_kovalenko@yahoo.com.

Illiashenko Oleg Aleksandrovych – Assistant Lecturer, Junior Research Fellow of Department of Computer Systems and Networks, National Aerospace University n. a. N. Ye. Zhukovsky "KhAI", Kharkov, Ukraine, e-mail: o.lliashenko@csn.khai.edu.