Игнатий А. Грачков, Анатолий А. Малюк
Национальный исследовательский ядерный университет «МИФИ»,
Каширское ш., 31, г. Москва, 115409, Россия
e-mail: ignat958@gmail.com, https://orcid.org/0000-0001-6327-3530,
e-mail: AAMalyuk@mephi.ru, https://orcid.org/0000-0002-5746-1508

ПРОБЛЕМЫ РАЗРАБОТКИ ДОВЕРЕННОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ, ПРИМЕНЯЕМОГО НА ОБЪЕКТАХ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

(организационные и методические аспекты)

DOI: http://dx.doi.org/10.26583/bit.2019.1.06

Аннотация. Вследствие возрастающей сложности информационных систем актуальными становятся угрозы безопасности информации, сопряженные с наличием уязвимостей программного обеспечения, применяемого в составе систем информационной инфраструктуры. В целях защиты от такого типа угроз сегодня, как правило, применяют целый комплекс мер, реализуемый в процессе эксплуатации и сопровождения программного обеспечения. Вместе с тем для обеспечения требуемого уровня защиты данных необходима реализация мер, нацеленных на предотвращение возникновения уязвимостей в процессе жизненного цикла программного обеспечения. Безопасная разработка программного обеспечения является основой доверия к информационно-коммуникационным технологиям в условиях современных киберугроз. Целью статьи является обобщение и анализ проблем создания доверенного программного обеспечения, применяемого на объектах критической информационной инфраструктуры, и поиск возможных путей их решения. В статье рассмотрены организационные и методические аспекты создания доверенного программного обеспечения, применяемого на объектах критической информационной инфраструктуры, описаны основные проблемы, стратегии и технологии обеспечения доверенности различных компонентов программного обеспечения. Вопрос обеспечения доверенности инструментальных средств, общесистемного и специального программного обеспечения пока остается открытым как в методическом, так и в организационном плане. Для решения этих проблем необходима долговременная государственная политика, разработка и уточнение нормативных правовых документов, определяющих общие подходы и конкретные пути обеспечения надежности и безопасности программного обеспечения, применяемого на объектах критической информационной инфраструктуры, с учетом реальных условий их эксплуатации.

Ключевые слова: доверенное программное обеспечение, автоматизированные системы, информационная безопасность, защита информации, сертификация.

Для цитирования: ГРАЧКОВ, Игнатий А.; МАЛЮК, Анатолий А. ПРОБЛЕМЫ РАЗРАБОТКИ ДОВЕРЕННОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ, ПРИМЕНЯЕМОГО НА ОБЪЕКТАХ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ (организационные и методические аспекты). Безопасность информационных технологий, [S.l.], p. 56-63, 2019. ISSN 2074-7136. Доступно на: <https://bit.mephi.ru/index.php/bit/article/view/1180>. Дата доступа: 19 feb. 2019. doi:http://dx.doi.org/10.26583/bit.2019.1.06.

Ignaty A. Grachkov, Anatoly A. Malyuk
National Nuclear Research University MEPhI,
Kashirskoe shosse, 31, Moscow, 115409, Russia
e-mail: ignat958@gmail.com, https://orcid.org/0000-0001-6327-3530,
e-mail: AAMalyuk@mephi.ru, https://orcid.org/0000-0002-5746-1508

Development problems of trusted software applied at critical information infrastructure objects (organizational and methodological aspects)

DOI: http://dx.doi.org/10.26583/bit.2019.1.06

Abstract. Due to the increasing complexity of information systems, information security threats associated with the presence of software vulnerabilities used in the information infrastructure systems become relevant. Today in order to protect against this type of threat one usually applies a range of measures implemented in the operation and maintenance of the software. At the same time, to ensure the required level of data protection, it is necessary to implement measures aimed at preventing

vulnerabilities during the software life cycle. Secure software development is the basis for trust in information and communication technologies in the context of modern cyber threats. The aim of this paper is to summarize and analyze the problems of creating trusted software used in critical information infrastructure, and to find possible ways to solve them. The organizational and methodological aspects of the creation of trusted software used in critical information infrastructure are discussed, and the main problems, strategies and technologies to ensure the trust for various software components are described. The issue of trust for tools, system-wide and special software is still open both in methodological and organizational terms. To solve these problems, it is necessary to have a long-term state policy, development and clarification of legal documents that define common approaches and specific ways to ensure the reliability and security of the software used in critical information infrastructure, taking into account the actual conditions of their operation.

Keywords: trusted software, automated systems, information security, information protection, certification.

For citation: GRACHKOV, Ignaty A.; MALYUK, Anatoly A. Development problems of trusted software applied at critical information infrastructure objects (organizational and methodological aspects). IT Security (Russia), [S.l.], p. 56-63, 2019. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/1180>. Date accessed: 19 feb. 2019. doi:http://dx.doi.org/10.26583/bit.2019.1.06.

Введение

Постоянно возрастающие мощь и функциональные возможности современных информационных технологий создают не только предпосылки, но и фундамент цифровизации всех сфер экономики, включая автоматизированные и управляющие системы критических приложений. Не менее характерной чертой и во многом следствием широкого использования современных информационных технологий в автоматизированных системах стало объективное возрастание сложности проблем обеспечения их информационной безопасности в прогнозируемых условиях применения. С одной стороны, это обусловлено высокой сложностью систем, создаваемых путем объединения десятков и сотен подсистем (комплексов), реализованных, как правило, в разное время и на различных аппаратных и программных платформах. Однако основной причиной является то, что такие критические системы в целом являются приоритетными объектами информационного противоборства, превосходство в котором рассматривается военно-политическим руководством иностранных государств, в качестве необходимого условия достижения успеха в противостоянии с Россией.

Таким образом, в современных условиях резко обостряются проблемы, связанные с созданием так называемого «доверенного» программного обеспечения (ПО) [1 - 4]. Решение этих проблем осложняется тем, что обрабатываемая информация, как правило, относится к различным категориям, а исторически сложившийся весьма широкий спектр используемого в критических системах и прежде всего в органах государственной власти программного и аппаратного обеспечения часто не имеет даже отдаленных отечественных аналогов. Различные подходы к решению этих проблем, равно как и смысл, вкладываемый в термин «доверенное ПО», неоднократно рассматривались специалистами, имеющими дело с разработкой специального ПО [5, 6]. Эти обсуждения показали определенные различия как в подходах к созданию и оценке степени доверия информационной системы, так и в трактовке самого понятия «доверенное ПО». В целом, на наш взгляд, термин «доверенность» обычно употребляется по отношению к степени соответствия ПО требуемым от него функциональным свойствам. При этом понятие доверия подразумевает наличие пары субъект-объект. В зависимости от того, какие целевые функции объекта важны для субъекта, это понятие наполняется конкретным содержанием, что, в свою очередь, и определяет требования к проектированию, разработке, эксплуатации и сопровождению ПО.

Современная автоматизированная система (АС) представляет собой многоуровневый комплекс, в котором каждый уровень оперирует своими понятиями и абстракциями, которые объединяют группы абстракций нижнего уровня. В идеале «доверенность» АС должна формально рассчитываться, другими словами, быть доказуемой средствами формальной логики как на микроуровнях, например, на уровне

функционирования отдельных вентилей микропроцессоров, так и на макроуровнях, вплоть до высокоуровневых протоколов информационного обмена между ее отдельными подсистемами. Такое доказательство возможно лишь при наличии теории, в основе которой будут математические модели функционирования АС, адекватно отражающие все существенные для данной целевой функции особенности и законы функционирования АС на данном уровне абстракции. Поэтому при оценке степени доверия к средствам обеспечения информационной безопасности целесообразнее исходить из того, что АС все же детерминированная система и ПО системы носит детерминированный характер, а затем, при необходимости, вносить неопределенность в модель поведения различных ее компонентов, в том числе неопределенность, связанную с соответствующей моделью нарушителя.

С учетом этого обстоятельства в рамках данной статьи мы ограничимся рассмотрением проблем разработки элементов типовой структуры ПО типовой подсистемы критической системы, в результате функционального взаимодействия и объединения которых, собственно, и образуется система в целом.

1. Доверенное программное обеспечение

Как показывает анализ различных работ [7 - 11], содержание термина «доверенное ПО» в основном связывается со следующими свойствами последнего:

- степенью доверия со стороны пользователя к устойчивости функционирования, защищенности и безопасности ПО, гарантиям возможности его сопровождения и поддержки в процессе разработки в течение требуемого периода времени;
- безопасностью и защищенностью ПО;
- надежностью, безопасностью и защищенностью ПО в процессе эксплуатации в пределах расчетного срока службы.

При всех различиях этих свойств представляется важным то, что все они имеют вероятностную природу и, как следствие, могут изменяться в процессе эксплуатации той или иной критической системы. Эти изменения могут происходить как в результате планового наращивания функциональных возможностей ПО, так и в результате непредсказуемого изменения условий эксплуатации, в том числе связанных с появлением новых угроз безопасности.

Таким образом, этап разработки доверенного ПО играет, безусловно, ключевую роль в формировании требуемых свойств ПО, однако сами по себе эти свойства обуславливают необходимость их контроля в процессе эксплуатации автоматизированных систем. С этим обстоятельством связан, как представляется, ряд организационных, технических и научных проблем создания доверенного программного обеспечения.

Необходимость сохранения свойств доверенности ПО в течение длительного периода времени предполагает, что предприятия-разработчики такого ПО в течение этого периода времени обладают достаточной структурной и экономической устойчивостью. Понятно, что условия, определяющие возможность разработки доверенного ПО, неразрывно связаны с государственной политикой в области информационной безопасности, в частности, с реструктуризацией и целенаправленной поддержкой предприятий и организаций, на которые возлагается задача создания ПО для систем критических приложений. Конкретно в этом направлении, на наш взгляд, должны быть сделаны следующие необходимые шаги.

Первое – это формирование ядра производственно-технологической структуры (минимально достаточной кооперации предприятий-разработчиков), обеспечивающей создание доверенного ПО. Однако такого рода организационные мероприятия сами по себе, очевидно, не устраняют угроз устойчивости (надежности) предприятий-разработчиков доверенного ПО, связанных с экономической сферой. Основной проблемой здесь, по-видимому, является кадровая конкуренция работающих в России филиалов ведущих мировых фирм, специализирующихся в области информационных технологий. При этом перекачка высококвалифицированных кадров из отечественного комплекса

может приобрести необратимый характер и в ближайшем будущем затронет все направления развития информационных технологий, а, следовательно, является одним из глобальных факторов национальной безопасности. Решение этой проблемы возможно лишь на основе целенаправленной и обоснованной государственной политики в области развития отечественных информационных технологий, необходимых для обеспечения безопасности России в информационной сфере.

Следует также отметить, что усилия по разработке доверенного ПО сконцентрированы сегодня в основном на базовых средствах, преимущественно общем программном обеспечении (ОПО). Вопрос о равнопрочном обеспечении доверенности других компонентов ПО, в частности, общесистемного и специального ПО, инструментальных средств пока остается открытым как в методическом, так и в организационном плане. В этой связи одной из ключевых проблем обеспечения доверенности ПО является разработка и внедрение в кратчайшие сроки полной системы стандартов, определяющих единые требования к технологии разработки и подтверждения соответствия заданным требованиям всех без исключения компонентов ПО критических систем.

2. Надежность программного обеспечения

Неотъемлемой частью свойств доверенности является качество или в конечном счете, надежность ПО. Реализация в создаваемом ПО требуемых свойств предполагает согласованное решение трех различных задач:

- формирования в техническом задании обоснованных, соответствующих модели угроз и условиям эксплуатации требований по безопасности и надежности функционирования ПО;
- обеспечения проектно-технологической безопасности и надежности ПО в процессе разработки;
- сертификации ПО.

Процедурные моменты в отношении первой задачи в общем случае хорошо отработаны. Однако применительно к свойству доверенности возникает необходимость создания механизма эффективного контроля соответствия (правильности) сформулированных требований по безопасности и надежности функционирования ПО уточненным моделям угроз и реальным условиям эксплуатации критических систем. Проблемными вопросами при этом являются:

- разработка дифференцированного перечня (моделей) угроз безопасности (с учетом принятой классификации информации по признакам конфиденциальности, используемых технических средств, архитектур систем, технологий обработки, хранения, передачи и защиты информации) и механизма их актуализации (уточнения) в процессе эксплуатации критической системы и ее подсистем;
- методологическое обеспечение процесса оценки и контроля информационной безопасности информационных и телекоммуникационных критических систем в целом;
- обоснование требований к информационной безопасности конкретных подсистем и разработка механизма их уточнения в процессе эксплуатации;
- разработка стандартов, определяющих требования по надежности и безопасности основных компонентов доверенного ПО: операционных сред, систем управления базами данных, инструментальных средств разработки прикладного ПО;
- собственно создание механизма контроля и нормативно-правового обеспечения его функционирования в процессе эксплуатации критических систем.

Обеспечение требуемого качества любой продукции, включая ее надежностные характеристики, неразрывно связано с наличием у производителя (разработчика) соответствующей системы управления качеством. Требования к таким системам наиболее полно сформулированы в международных стандартах ISO 9000, сертификацию на соответствие которым прошли далеко не все российские предприятия. По-видимому, одна

из проблем разработки доверенного ПО заключается в необходимости введения требований по обязательной сертификации предприятия-разработчика доверенного ПО на соответствие требованиям стандартов в области систем качества [12]. При этом с учетом специфики областей применения доверенного ПО в состав требований к системе качества должен войти ряд новых:

- оценка лояльности персонала, участвующего в проектировании, разработке и испытаниях (отработке) доверенного ПО;
- аттестация профессиональной пригодности персонала;
- контроль психофизического состояния;
- независимая оценка (контроль) выполнения требований, определяемых технологией (желательно также сертифицированной) проектирования, разработки и отработки доверенного ПО;
- введение в действие юридических документов, определяющих ответственность персонала за совершение злоумышленных или разрешенных имеющимися полномочиями действий, в результате которых снижается безопасность и/или надежность доверенного ПО.

Самостоятельную проблему представляет обоснование и в конечном счете выбор стратегии и конкретной технологии обеспечения доверенности основных компонентов ПО. Вообще говоря, таких стратегий как минимум две:

- разработка «с нуля»;
- модификация прототипа прежде всего в направлении усиления уже реализованных и добавления новых механизмов обеспечения безопасности информации.

По некоторым мнениям [13, 14], в современных условиях возможности реализации первой стратегии исчезающе малы ввиду чрезвычайно высокой сложности и стоимости данного подхода. Однако в мировом сообществе происходит осознание неадекватности существующих архитектурных решений современным потребностям. На протяжении ряда лет в различных научных центрах ведутся эксперименты, направленные на создание архитектуры ОС с более развитыми механизмами обеспечения защиты и, в частности, с доказуемой степенью надежности разграничения доступа. Проектов по разработке ОС «с нуля» насчитывается более двух десятков, что свидетельствует о серьезном внимании в мире к «нулевому» варианту создания защищенной доверенной ОС. Намечается и определенная тенденция к учету проблем обеспечения информационной безопасности и среди производителей процессоров.

В рамках второй стратегии в России на сегодня получен известный нам ряд практически значимых результатов. Однако при реализации и этой стратегии сохраняется ряд пока не решенных проблемных вопросов. Среди них:

- обоснование приоритетов, рационального соотношения требований к степени программной совместимости и мобильности доверенного ПО по отношению к коммерческому ПО;
- обоснование требований по программной совместимости и мобильности доверенного ПО с учетом тенденций развития перспективных аппаратных платформ.

Практическая реализация второй стратегии стала возможной только благодаря массовому использованию свободно распространяемого ПО и, в частности, ОС LINUX, которая подвергается интенсивным испытаниям по существу на всемирном полигоне. Это обстоятельство, возможность мониторинга процесса испытаний, доступ к исходным текстам создают достаточно высокий уровень доверия к подобному или создаваемому на его основе ПО. Очевидно и то, что процесс развития ОС LINUX, как и прикладных коммерческих приложений для нее, носит исключительно динамичный характер.

Заключение

Наиболее радикальным и последовательным подходом к обеспечению мобильности прикладного (в том числе специального) ПО является разработка доверенной ОС, что, однако, невозможно без введения ограничений на функции прикладного программного интерфейса и, как следствие, введения ограничений на степень программной совместимости. Таким образом, для доверенного ПО должна быть четко очерчена область применения. Одновременно представляется принципиально важным создание механизма поддержания программной совместимости за пределами этой области с целью сохранения актуальности доверенного ПО.

При этом возникает проблема оценки степени зависимости процесса разработки доверенного ПО от точного знания особенностей перспективных аппаратных платформ, информация о которых, возможно, будет распространяться на лицензионной основе. Возможность получения точной информации об особенностях аппаратной платформы, в частности, обо всех ошибках, влияющих на программную совместимость, будет непосредственно влиять на степень ее достижения в перспективном доверенном ПО.

Как представляется, для решения проблемы программной совместимости и мобильности доверенного ПО не только целесообразна, но и необходима разработка концепции создания и развития доверенного ПО для объектов критической информационной инфраструктуры, в которой должны быть сформулированы и обоснованы цели, приоритеты, основные подходы и технологии достижения и поддержания требуемой степени доверенности ПО. Для успешного решения обсуждаемой проблемы приоритетное значение имеет принятие системообразующих планирующих документов, которые опирались бы на ясное понимание задач, ведущих к решению проблемы, учитывали бы обстоятельства, способствующие как выполнению этих задач, так и осложняющие их выполнение.

Как известно, в России в настоящее время действую четыре системы обязательной сертификации на соответствие требованиям по безопасности информации. При этом в пределах компетенции каждой из систем сертификации ее внимание акцентируется на отдельных компонентах ПО (НСД, СЗИ, криптография и т.д.). Программное же обеспечение в целом в качестве объекта сертификации на соответствие требованиям, в совокупности определяющим свойства доверенности ПО, ни в одной из существующих систем сертификации не рассматривается. Кроме того, процедура сертификации носит статический (одномоментный) характер, в то время как свойства доверенности проявляются, а главное – изменяются в процессе эксплуатации ПО [15, 16].

Одним из шагов на пути к обеспечению доверенности программного обеспечения является утверждение ФСТЭК России Требований по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий. Данные Требования устанавливают уровни доверия, характеризующие безопасность применения средств обработки и защиты информации, содержащей сведения, составляющие государственную тайну и иной информации ограниченного доступа.

В целом процессы анализа проблем разработки доверенного ПО, применяемого на объектах критической информационной инфраструктуры, и выработка подходов к их решению находятся в начальной стадии. Однако уже сейчас ясно, что для решения этих проблем необходима долговременная государственная политика, разработка (уточнение) концептуальных и других нормативно-правовых документов, определяющих общие подходы и конкретные пути обеспечения надежности и безопасности ПО, применяемого на объектах критической информационной инфраструктуры, с учетом реальных условий их эксплуатации.

СПИСОК ЛИТЕРАТУРЫ:

1. Хабибуллин, И.В. Основные проблемные вопросы создания доверенной программно-аппаратной среды для АСУ органов военного и государственного управления. Вопросы кибербезопасности, 2014. № 3. URL: http://cyberrus.com/wp-content/uploads/2014/11/vkb_04_03.pdf (дата обращения: 18.09.2018).

2. Барабанов, А.В., Марков, А.С., Цирлов, В.Л. 28 магических мер разработки безопасного программного обеспечения. Вопросы кибербезопасности, 2015. № 5. С. 2 – 10. URL: http://cyberrus.com/wp-content/uploads/2015/12/02-10-513-15_1.-Барабанов.pdf (дата обращения: 18.09.2018).
3. Барабанов, А.В., Марков, А.С., Цирлов, В.Л. Методический аппарат анализа и синтеза комплекса мер разработки безопасного программного обеспечения. Программные продукты и системы, 2015. № 4. С. 166 – 174. URL: http://www.swsys.ru/index.php?page=article&id=4086&lang=; DOI:10.15827/0236-235X.112.166-174. (дата обращения: 18.09.2018).
4. Барабанов, А.В., Марков, А.С., Цирлов, В.Л. Актуальные вопросы выявления уязвимостей и недекларированных возможностей в программном обеспечении. Системы высокой доступности, 2018. №3. С. 12 – 17. DOI: 10.18127/j20729472-201803-03. URL: http://www.radiotec.ru/article/22223
5. Грюнталь, А. И. Информационно безопасное программное обеспечение систем реального времени. Известия ЮФУ. Технические науки. 2007. №1. URL: https://cyberleninka.ru/article/n/informatsionno-bezopasnoe-programmnoe-obespechenie-sistem-realnogo-vremeni (дата обращения: 18.09.2018).
6. Тыкушин, А.В., Калинкин, Е.О., Кузнецов, Е.В., Смирнов, В.Г. Проблемы обеспечения доверенной среды при проектировании программно-аппаратных комплексов. Теория и практика имитационного моделирования и создания тренажёров, 2015. С. 79 – 82. ISBN 978-5-9907043-3-6. URL: http://www.penzgtu.ru/fileadmin/filemounts/science/konf_roganov/modelirovanie/__Сборник_печатный_по_тренажёрам.pdf
7. Старовойтов, А. В. Кибербезопасность как актуальная проблема современности. Информатизация и связь, 2011. №. 6. С. 4 – 7. URL: https://elibrary.ru/item.asp?id=17268244 (дата обращения: 18.09.2018)
8. Dmitry P. Zegzhda, Peter D. Zegzhda, Maxim O. Kalinin Clarifying Integrity Control at the Trusted Information Environment, MMM-ACNS 2010. Lecture Notes in Computer Science, vol 6258. Springer, Berlin, Heidelberg. DOI: 10.1007/978-3-642-14706-7_27
9. Сабанов, А.Г. Доверенные системы как средство противодействия киберугрозам. Защита информации. Инсайд, 2015. № 3 (63). С. 17 – 21. URL: http://www.inside-zi.ru/pages/3_2015/17.html (дата обращения: 18.09.2018)
10. Барабанов, А.В. Задание требований к процессу безопасной разработки программного обеспечения. ИТ-Стандарт, 2015. № 3 (4). С. 1 – 6. URL: https://elibrary.ru/item.asp?id=25727955& (дата обращения: 18.09.2018)
11. Жидков, И.В., Кадушкин, И.В., Шубенин, А.А. Обоснование подхода к созданию доверенной программно- аппаратной среды. ИТ-Стандарт, 2015. № 2 (3). С. 60-67. URL: https://elibrary.ru/item.asp?id=25727952 (дата обращения: 18.09.2018).
12. Antoni Lluís Mesquida, Antonia Mas Implementing information security best practices on software lifecycle processes: The ISO/IEC 15504 Security, Extension Computers & Security, Volume 48, February 2015, Pages 19-34. DOI: 10.1016/j.cose.2014.09.003
13. Кузьмин, А.С., Романов, А.А., Напеденина, Е.Ю. Перенос (перевод) информационных систем в доверенную (отечественную) операционную среду: подводные камни. // Приборы и системы. Управление, контроль, диагностика, 2016. № 4. С. 1 – 9. URL: https://elibrary.ru/item.asp?id=25838794 (дата обращения: 18.09.2018).
14. Кузьмин, А.С., Романов, А.А. Проблемы перевода унаследованных информационных систем в отечественные операционные среды. Прикладная физика и математика, 2016. № 2. С. 39 – 48. URL: https://elibrary.ru/item.asp?id=25864276 (дата обращения: 18.09.2018).
15. Гончаров, А.А. Использование нового стандарта ГОСТ Р 56939-2016 как основной шаг к безрисковой сертификации средств защиты информации. Теоретические исследования и экспериментальные разработки студентов и аспирантов ТвГТУ Материалы научно-практической конференции, приуроченной ко Дню российской науки, 2017. С. 3 – 7. URL: https://elibrary.ru/item.asp?id=32259213 (дата обращения: 18.09.2018).
16. Марков, А.С., Рауткин, Ю.В. Сертификация средств защиты информации по требованиям безопасности информации. Новая парадигма // Информационные и математические технологии в науке и управлении. 2016. № 1. С. 94 – 102. URL: https://elibrary.ru/item.asp?id=27283988 (дата обращения: 18.09.2018).

REFERENCES:

[1] Khabibullin, I.V. The major issues of creating the trusted software and hardware environment for process of acs of military and public administration. Voprosy kiberbezopasnosti, 2014. № 3. URL: http://cyberrus.com/wp-content/uploads/2014/11/vkb_04_03.pdf (in Russian).
[2] Barabanov, A.V., Markov, A.S., Cirlov, V.L. The 28 magic practices for secure software development. Voprosy kiberbezopasnosti, 2015. № 5. P.2 – 10. URL: http://cyberrus.com/wp-content/uploads/2015/12/02-10-513-15_1.-Барабанов.pdf (in Russian).
[3] Barabanov, A.V., Markov, A.S., Cirlov, V.L. A methodical framework of analysis and synthesis of secure software development controls. Programmnye produkty i sistemy (Software & Systems). 2015. № 4. P. 166 – 174 DOI:10.15827/0236-235X.112.166-174.
URL: http://www.swsys.ru/index.php?page=article&id=4086&lang= (in Russian).

[4] Barabanov, A.V., Markov, A.S., Cirlov, V.L., Topical issues of identifying vulnerabilities and undeclared capabilities in software. Highly available systems, 2018. № 3. P. 12 – 17. DOI: 10.18127/j20729472-201803-03. URL: http://www.radiotec.ru/article/22223 (in Russian).

[5] Gryuntal', A. I. Information secure software for real-time systems. Izvestiya YUFU. Tekhnicheskiye nauki. 2007. №1. URL: https://cyberleninka.ru/article/n/informatsionno-bezopasnoe-programmnoe-obespechenie-sistem-realnogo-vremeni (in Russian).

[6] Tykushin A.V., Kalinkin E.O., Kuznetsov E.V., Smirnov V.G Problems of providing a trusted environment for the design of software and hardware complexes. Teoriya i praktika imitatsionnogo modelirovaniya i sozdaniya trenazhorov, 2015. P. 76 – 79. ISBN 978-5-9907043-3-6. URL: http://www.penzgtu.ru/fileadmin/filemounts/science/konf_roganov/modelirovanie/__Сборник_печатный_по_тренажёрам.pdf (in Russian).

[7] Starovoytov, A. V. Cybersecurity as an actual modern problem. Informatizatsiya i svyaz', 2011. №. 6. P. 4 – 7. URL: https://elibrary.ru/item.asp?id=17268244 (in Russian).

[8] Dmitry P. Zegzhda, Peter D. Zegzhda, Maxim O. Kalinin, Clarifying Integrity Control at the Trusted Information Environment, MMM-ACNS 2010. Lecture Notes in Computer Science, vol 6258. Springer, Berlin, Heidelberg. DOI: 10.1007/978-3-642-14706-7_27

[9] Sabanov A.G., Trusted computer systems as a way to counteract the cyber threats. Zaŝita informacii. Inside, 2015. № 3 (63). P. 17 – 2. URL: http://www.inside-zi.ru/pages/about-eng.html (in Russian).

[10] Barabanov, A.V. Job requirements process secure software development. IT-Standart, 2015. № 3 (4). P. 1-6. URL: https://elibrary.ru/item.asp?id=25727955& (in Russian).

[11] Zhidkov, I.V., Kadushkin, I.V., Shubenin, A.A., Rationale for trusted approach to creating software and hardware environment. IT-Standart, 2015. № 2 (3). P. 60 – 67. URL: https://elibrary.ru/item.asp?id=25727952 (in Russian).

[12] Antoni Lluís Mesquida, Antonia Mas, Implementing information security best practices on software lifecycle processes: The ISO/IEC 15504 Security, Extension Computers & Security, Volume 48, February 2015, P. 19 – 34. DOI: 10.1016/j.cose.2014.09.003

[13] Kuzmin, Aleksey S., Romanov Alexander A., Napedenina Ekaterina Y. Shift (translation) the trusted information systems (domestic) operating Wednesday: pitfalls. Instruments and Systems: Monitoring, Control, and Diagnostics 2016. № 4. P. 1 – 9. URL: https://elibrary.ru/item.asp?id=25838794 (in Russian).

[14] Kuzmin, Aleksey S., Romanov, Alexander A. The transfer of legacy information systems in domestic operating environment. Prikladnaya fizika i matematika, 2016. № 2. P. 39 – 48. URL: https://elibrary.ru/item.asp?id=25864276 (in Russian).

[15] Goncharov, A.A., The use of new standard GOST-R 56939–2016 as a major step toward riskless certification of information security. Teoreticheskiye issledovaniya i eksperimental'nyye razrabotki studentov i aspirantov TvGTU Materialy nauchno-prakticheskoy konferentsii, priurochennoy ko Dnyu rossiyskoy nauki, 2017. P. 3 – 7. URL: https://elibrary.ru/item.asp?id=32259213 . (in Russian).

[16] Markov, A.S., Rautkin, Y.V., Sertifikatsiya sredstv zashchity informatsii po trebovaniyam bezopasnosti informatsii. Novaya paradigma // Informatsionnyye i matematicheskiye tekhnologii v nauke i upravlenii. 2016. № 1. P. 94 – 102. URL: https://elibrary.ru/item.asp?id=27283988 (in Russian).

Поступила в редакцию –6 ноября 2018 г. Окончательный вариант – 23 января 2019 г.
Received – November 06, 2018. The final version – January 23, 2019.