Айжана М. Каднова[1], Олег Ю. Макаров[2], Сергей А. Мишин[3], Евгений А. Рогозин[4]
[1, 3, 4] Воронежский институт МВД России,
пр-т Патриотов, 53, г. Воронеж, 394065, Россия
[2]Воронежский государственный технический университет,
20 лет Октября, 84, г. Воронеж, 394006, Россия
[1]e-mail: aizhana_kadnova@mail.ru, https://orcid.org/0000-0002-7758-6578
[2]e-mail: moy230@yandex.ru, https://orcid.org/0000-0003-2795-419X
[3]e-mail: samishin@bk.ru, https://orcid.org/0000-0002-8321-2759
[4]e-mail: evgenirogozin@yandex.ru, https://orcid.org/0000-0002-4455-7535

АЛГОРИТМ СОЗДАНИЯ АВТОМАТИЗИРОВАННЫХ СИСТЕМ В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ

DOI: http://dx.doi.org/10.26583/bit.2019.4.07

Аннотация. В статье проведен анализ нормативной документации, регламентирующей вопросы создания автоматизированных систем в защищенном исполнении, а также открытых литературных источников, посвященных проблемам проектирования автоматизированных систем в защищенном исполнении, их оптимизации и разработки математических моделей этих систем. По результатам анализа указанных источников разработан алгоритм, представляющий процесс создания автоматизированных систем в защищенном исполнении в виде совокупности взаимосвязанных и упорядоченных во времени этапов, включающих в себя необходимые работы для создания автоматизированных систем указанного типа. Создание автоматизированных систем в защищенном исполнении в соответствии с разработанным в статье алгоритмом позволит исследовать создаваемую автоматизированную систему в защищенном исполнении во временном диапазоне, снизить вероятность совершения ошибок разработчиками, следствием чего является сокращение временных и финансовых затрат, а также высокоустойчивость к угрозам безопасности информации созданной в результате системы.

Ключевые слова: система защиты информации, автоматизированная система, защита информации, информационный ресурс, несанкционированный доступ.
Для цитирования: КАДНОВА, Айжана М. et al. АЛГОРИТМ СОЗДАНИЯ АВТОМАТИЗИРОВАННЫХ СИСТЕМ В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ. Безопасность информационных технологий, [S.l.], v. 26, n. 4, p. 93–100, 2019. ISSN 2074-7136. Доступно на: <https://bit.mephi.ru/index.php/bit/article/view/1235>. Дата доступа: 01 dec. 2019. doi:http://dx.doi.org/10.26583/bit.2019.4.07.

Aizhana M. Kadnova[1], Oleg Yu. Makarov[2], Sergey A. Mishin[3], Evgeniy A. Rogozin[4]
[1, 3, 4] Voronezh Institute of the Ministry of Internal Affairs of Russia,
Revolution Avenue, 53, Voronezh, 394065, Russia
[2]Voronezh State Technical University,
20 years of October, 84, Voronezh, 394006, Russia
[1]e-mail: aizhana_kadnova@mail.ru, https://orcid.org/0000-0002-7758-6578
[2]e-mail: moy230@yandex.ru, https://orcid.org/0000-0003-2795-419X
[3]e-mail: samishin@bk.ru, https://orcid.org/0000-0002-8321-2759
[4]e-mail: evgenirogozin@yandex.ru, https://orcid.org/0000-0002-4455-7535

Algorithm for creation of automated systems in protected performance

DOI: http://dx.doi.org/10.26583/bit.2019.4.07

Abstract. The article analyzes the regulatory documentation governing the creation of automated systems in secure execution, as well as open literature on the problems of designing automated systems in secure execution, their optimization and the development of mathematical models of these systems. Based on the analysis of these sources, an algorithm has been developed that represents the process of creating automated systems in a secure execution in the form of a set of interconnected and time-ordered stages that include

the necessary work to create automated systems of the specified type. The creation of automated systems in secure execution in accordance with the algorithm developed in the article will allow us to investigate the automated system being created in secure execution in the time range, reduce the likelihood of errors by developers, resulting in a reduction in time and financial costs, as well as high resistance to security threats to information created as a result system.
Keywords: information security system, automated system, information security, information resource, unauthorized access.
For citation: KADNOVA, Aizhana M. et al. Algorithm for creation of automated systems in protected performance. IT Security (Russia), [S.l.], v. 26, n. 4, p. 93–100, 2019. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/1235>. Date accessed: 01 dec. 2019. doi:http://dx.doi.org/10.26583/bit.2019.4.07.

Введение

В современных условиях развития различных сфер человеческой деятельности и внедрения в них новых информационных технологий потребности организаций, занимающихся обработкой информации ограниченного доступа, в автоматизированных системах (АС) в защищенном исполнении неуклонно возрастают. В соответствии с [1] АС в защищенном исполнении – это АС, реализующая информационную технологию выполнения установленных функций в соответствии с требованиями стандартов и/или нормативных документов по защите информации. Неотъемлемой составной частью такой АС является система защиты информации (СЗИ), которая реализует программно-технические меры защиты информации, обрабатываемой в АС в защищенном исполнении [2]. При этом СЗИ в процессе выполнения своих функций не должна препятствовать достижению целей функционирования АС в защищенном исполнении или потреблять чрезмерное количество ресурсов этой системы. Целью создания АС в защищенном исполнении является предотвращение или снижение величины ущерба (финансового, морального, экологического, социального и т.д. и их сочетаний), наносимого владельцу или пользователю(-ям) этой системы и/или владельцу информации, обрабатываемой данной системой, вследствие реализации угроз информационной безопасности. Степень защищенности информации зависит от качества функционирования АС [3] в защищенном исполнении, которое определяется точностью и полнотой выполнения всех этапов процесса создания данной АС.

Этапы создания АС в защищенном исполнении

Анализ существующих подходов (методик, способов и схем) к созданию АС в защищенном исполнении показал, что в них есть ряд недостатков, в частности в [4–11] схемы создания АС в защищенном исполнении основаны на ГОСТ Р 51583-2014 [12] и ГОСТ 34.601-90 [13], но используемые в них терминологии не соответствуют указанным стандартам, что может привести к ошибкам разработчиков при создании АС в защищенном исполнении в связи с непрозрачностью и некорректностью используемых понятий и терминов. С учетом разработанных в [4–11] методик создания АС в защищенном исполнении и предпринятой попытке в [14] разработать алгоритм создания АС в защищенном исполнении был построен новый преобразованный и доработанный поэтапный алгоритм создания АС в защищенном исполнении с входящей в нее системой защиты информации. Разработанный алгоритм приведен на рис. 1.

Процесс создания АС в защищенном исполнении представлен следующими этапами:

1. Обследование АС и анализ циркулирующей в ней информации [15]. На данном этапе проводится анализ целей создания АС в защищенном исполнении, назначения,

функций, условий функционирования и характера обрабатываемой информации. Определяется перечень информации, подлежащий защите. Проводится оценка целесообразности создания АС в защищенном исполнении.

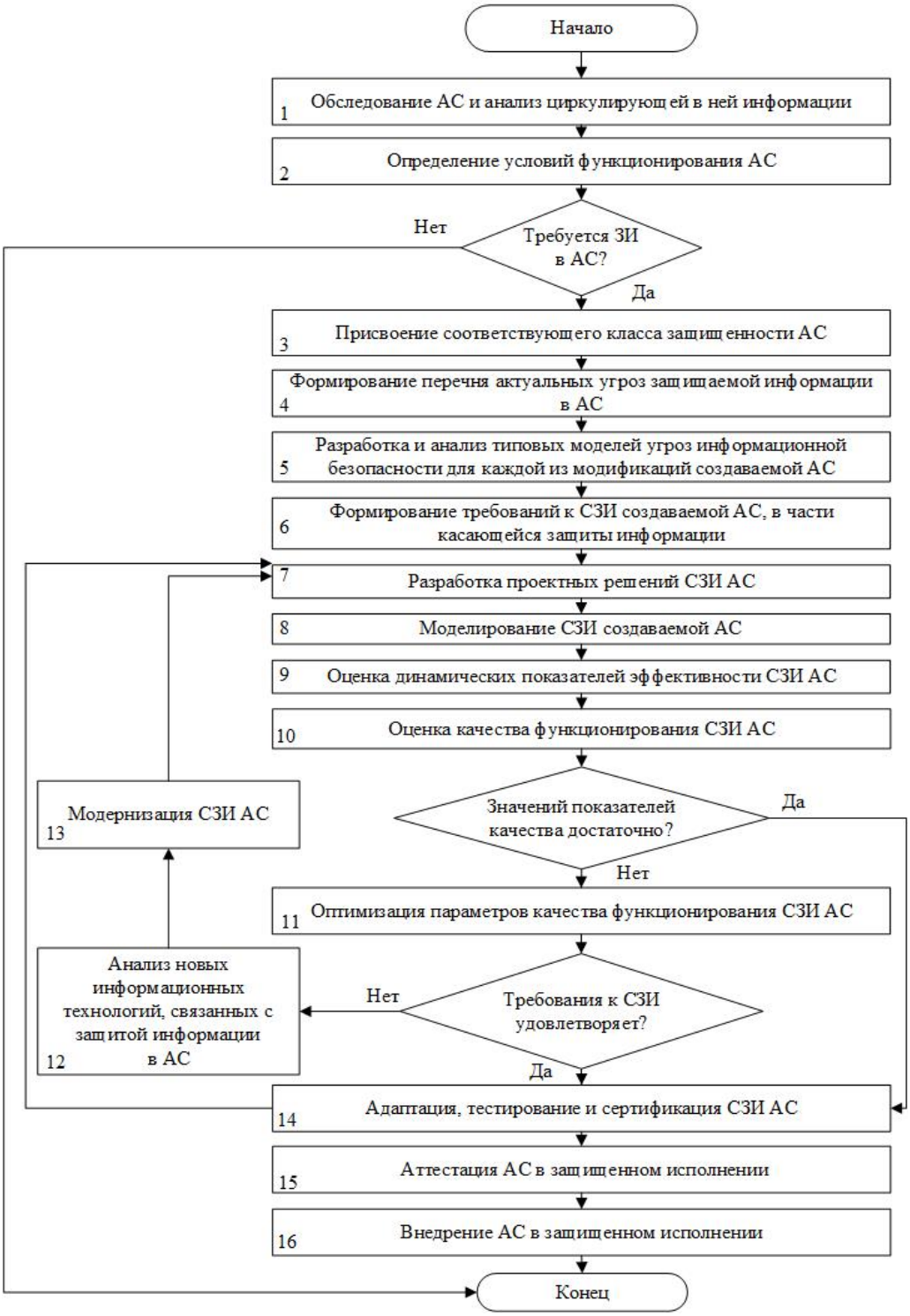

Рис. 1. Основные стадии (этапы) создания АС в защищенном исполнении
(Fig. 1. Main stages (stages) of creation of the automated systems in the protected execution)

2. Определение условий функционирования АС. После определения характера информации, циркулирующей в создаваемой АС, устанавливается порядок ее обработки в АС в целом и в отдельных составляющих, степень участия пользователей различной категории в обработке защищаемой информации и утверждается поименный список лиц, допущенных к АС в соответствии со своими служебными обязанностями. Устанавливаются полномочия доступа пользователей к защищаемым ресурсам АС. Изучаются возможности по взаимодействию с другими АС и подключение к информационно-телекоммуникационным сетям. По завершении данного этапа принимается решение о необходимости разработки дополнительных средств ЗИ в АС.

3. Присвоение соответствующего класса защищенности АС. На основе анализа условий обработки конфиденциальной информации выявляются признаки создаваемой АС, которые сравниваются с классифицируемыми, в целях присвоения АС правильного класса защиты обрабатываемой в ней информации [15]. Данный этап основан на структурном анализе АС в связи с тем, что класс защищенности АС является основой выбора организационных и технических мероприятий, позволяющих достичь необходимого уровня защиты информации. В зависимости от задач системы защиты информации структурный анализ позволяет оптимизировать использование различных ресурсов разрабатываемой АС. Если выявленные признаки АС не соответствуют ни одному классу защищенности, в частности обрабатываемая АС информация потеряла свойство конфиденциальности, то мероприятия по защите данной информации не требуются и создание АС в защищенном исполнении прекращается.

4. Формирование перечня актуальных угроз защищаемой информации в АС. Проводится анализ потенциальных угроз безопасности информации, циркулирующей в АС, связанных с несанкционированным к ней доступом, несанкционированным воздействием, а также с ее утечкой по техническим каналам, и уязвимых мест АС. Проводится оценка возможностей нарушителя по реализации вышеперечисленных угроз.

5. Разработка и анализ типовых моделей угроз информационной безопасности для каждой из модификаций создаваемой АС. Модель угроз информационной безопасности должна содержать описание АС, в том числе ее структурно-функциональных характеристик, перечень возможных угроз информационной безопасности, способов и последствий (нарушение конфиденциальности, целостности, доступности информации) их реализации, модель нарушителя и описание возможных уязвимостей АС.

6. Формирование требований к СЗИ создаваемой АС, в части касающейся защиты информации. Требования к системе защиты определяются классом защищенности разрабатываемой АС с учетом принятой «Модели угроз...». Требования включают в себя цели и задачи защиты информации, перечень защищаемых информационных ресурсов, функции СЗИ и меры доверия к ним, нормативные акты, регламентирующие требования. В зависимости от тактико-технических характеристик создаваемой АС в защищенном исполнении формируются требования к параметру эффективность функционирования СЗИ.

7. Разработка проектных решений СЗИ АС. На данном этапе обеспечивается разработка общих решений по системе защиты, ее функциональному составу, программно-техническим средствам, обеспечивающим функциональные возможности системы защиты, по алгоритмам функционирования, а также функциям персонала. Утверждается техническое задание на создание СЗИ [16].

8. Моделирование СЗИ создаваемой АС. На данном этапе создается модель функционирования СЗИ с целью анализа ее характеристик, показателей качества и эффективности функционирования системы защиты.

9. Оценка динамических параметров эффективности СЗИ создаваемой АС. На

данном этапе анализируется эффективность функционирования системы защиты в динамике [17].

10. Оценка качества функционирования СЗИ АС. На данном этапе анализируется качество функционирования системы защиты в целом [17]. В случае удовлетворения показателей качества функционирования СЗИ предъявляемым требованиям выполняется переход на этап 13, в противном случае – на этап 11.

11. Оптимизация параметров качества функционирования СЗИ АС. На данном этапе осуществляется поиск наиболее выгодного и эффективного соотношения между параметрами, характеризующими разрабатываемую СЗИ, к которым относятся финансовые и трудовые затраты, условия функционирования, сроки создания, реализация целей заказчика и т.д. Если разрабатываемая СЗИ не соответствует требованиям заказчика, то осуществляется переход на этап 12, если соответствует – переход на этап 13.

12. Анализ новых информационных технологий, связанных с защитой информации в АС. Постоянный рост числа угроз безопасности информации влечет за собой рост защитных технологий. Учитывая данный факт, на данном этапе при построении АС в защищенном исполнении необходимо использовать новые защитные технологии, например, биометрические средства предоставления доступа в систему (идентификация по рисунку папиллярных линий, радужной оболочке глаз, геометрии и тепловому изображению лица и т.д.)

13. Модернизация СЗИ АС. Выявленные недостатки на предыдущих этапах создания АС в защищенном исполнении устраняются, вносятся изменения в документацию на СЗИ, после чего уточняются требования к СЗИ и осуществляется переход на этап 7.

14. Адаптация, тестирование и сертификация СЗИ АС. На данном этапе разрабатывается полный комплект документов, содержащий информацию по внедрению и эксплуатации СЗИ, осуществляется адаптация (настройка) СЗИ к условиям использования, проводятся ее испытания и тестирование. В процессе тестирования СЗИ проверяется ее работоспособность и совместимость с программным и техническим оборудованием АС. В случае успешного прохождения тестирования СЗИ проводится сертификация разрабатываемой СЗИ АС в защищенном исполнении по требованиям безопасности информации и осуществляется переход на следующий этап, в противном случае – на этап 7.

15. Аттестация АС в защищенном исполнении. До ввода АС в защищенном исполнении в постоянную эксплуатацию проводится ее аттестация на соответствие требованиям по защите информации. Аттестация содержит подтверждение соответствия СЗИ разрабатываемой АС в защищенном исполнении требованиям по защите информации в реальных условиях эксплуатации, регламентируемое нормативно-правовыми документами в области обеспечения безопасности информации.

16. Внедрение АС в защищенном исполнении. Внедрение и сопровождение АС в защищённом исполнении осуществляется на основе организационно-распорядительной, эксплуатационной и нормативной документации по защите информации. На данном этапе осуществляется настройка СЗИ, обучение персонала в целом и администраторов, ответственных за защиту информации, проверка непосредственного функционирования, доработка, наладка СЗИ и ее сопровождение (техническая поддержка), проводимое высококвалифицированными специалистами. Техническая поддержка СЗИ включает в себя исправление ошибок, ее адаптацию к условиям использования, модернизацию, а также периодический контроль функционирования СЗИ, в процессе которого администратор, служба безопасности подразделения, отраслевые и федеральные органы контроля, проверяют соблюдение нормативной документации по защите информации, работоспособность СЗИ в соответствии с эксплуатационной документацией и выполнение

обычными пользователями своих функциональных обязанностей в части, касающейся защиты информации.

Заключение

В работе по результатам анализа нормативной документации и открытых литературных источников, посвященных проблемам создания АС в защищенном исполнении, разработан алгоритм, представляющий процесс создания автоматизированных систем в защищенном исполнении в виде совокупности взаимосвязанных и упорядоченных во времени этапов, включающих в себя необходимые работы для создания автоматизированных систем указанного типа. От соблюдения последовательности, четкости и полноты выполнения каждого этапа зависит качество создаваемой АС в защищенном исполнении. Отсутствие ошибок на каждом из этапов обеспечит создание высокоустойчивой к угрозам безопасности информации АС.

СПИСОК ЛИТЕРАТУРЫ:

1. ГОСТ Р 53114-2008 Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения. URL: http://docs.cntd.ru/document/1200075565 (дата обращения: 23.11.2019).
2. ГОСТ Р 50922-2006. Защита информации. Основные термины и определения. URL: http://docs.cntd.ru/document/gost-r-50922-2006 (дата обращения: 23.11.2019).
3. Каднова А.М. Система показателей качества функционирования при создании системы информационной безопасности на объекте информатизации ОВД / О.И. Бокова, А.М. Каднова, Е.А. Рогозин, А.С. Серпилин // Приборы и системы, управление, контроль, диагностика. 2019. № 1. С. 26–33.
4. Гаскаров В.Д. Концептуальное проектирование защищенных автоматизированных информационных систем / В.Д. Гаскаров // Водные пути и гидротехнические сооружения, информационные технологии, портовая техника и электромеханика, судостроение и судоремонт, гуманитарные вопросы, экономика и финансы, юриспруденция : сб. науч. тр. – Санкт-Петербург, 2008. С. 91–96.
5. Лойко В.И. Проектирование автоматизированных систем в защищенном исполнении военного назначения / В.И. Лойко, Ф.Г. Хисамов, Р.С. Шерстобитов // Политематический сетевой электронный научный журнал Кубанского государственного аграрного университета. 2017. № 126. С. 519–532.
6. Хисамов Ф.Г. Математическая модель оценки защищенности информации от несанкционированного доступа при проектировании автоматизированных систем в защищенном исполнении / Ф.Г. Хисамов, А.С. Жук, Р.С. Шерстобитов // Известия ЮФУ. Технические науки. 2017. № 9 (194). С. 91–102.
7. Гудков С.Н. Основные этапы и задачи проектирования программных систем защиты информации в автоматизированных системах /С.Н. Гудков, Д.И. Коробкин, Е.А. Рогозин // Вестник Воронежского государственного технического университета. 2009. Т. 5. № 10. С. 139–142.
8. Львович Я.Е. Оптимизация проектирования систем защиты информации в автоматизированных информационных систем промышленных предприятий / Я.Е. Львович, Д.С. Яковлев // Вестник ВГУИТ. 2014. №2. С. 90–94.
9. Каднова А.М. Имитационная модель функционирования системы защиты информации от несанкционированного доступа «Страж NT» в программной среде «CPN Tools» с целью исследования ее временных характеристик / А.М. Каднова, Е.А. Рогозин, Ю.С. Лунёв, А.Д. Попов // Охрана, безопасность, связь – 2018 : материалы международной научно-практической конференции. Т 3. № 4(4). Воронеж: ВИ МВД России, 2019. С. 78–81
10. Дровникова И.Г. Методика проектирования систем информационной безопасности в автоматизированных системах / И.Г. Дровникова, Е.А. Рогозин, А.А. Никитин // Интернет-журнал «Технологии техносферной безопасности». 2016. №4 (68). С. 17–25.
11. Методы и средства оценки эффективности подсистемы защиты конфиденциального информационного ресурса при её проектировании в системах электронного документооборота : монография / И.Г. Дровникова [и др.]. Воронеж: Воронеж. гос. техн. ун-т, 2015. – 106 с.
12. ГОСТ Р 51583-2014 Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения. URL: http://docs.cntd.ru/document/1200108858 (дата обращения: 23.11.2019).

13. ГОСТ 34.601-90 Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания. URL: http://docs.cntd.ru/document/1200006921. (дата обращения: 23.11.2019).
14. Рогозин Е.А. Проектирование систем защиты информации от несанкционированного доступа в автоматизированных системах органов внутренних дел / Е.А. Рогозин, А.Д. Попов, Т.В. Шагиров // Вестник Воронежского института МВД России. 2016. № 2. С. 174–183.
15. ФСТЭК РФ. Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. – Москва: Воениздат, 1992.
16. ГОСТ 34.602-89 Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы. URL: http://docs.cntd.ru/document/1200006924 (дата обращения: 23.11.2019).
17. ФСТЭК РФ. Руководящий документ. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации. Москва: Воениздат, 1992.

REFERENCES:

[1] GOST R 53114-2008 Zashchita informatsii. Obespechenie informatsionnoy bezopasnosti v organizatsii. Osnovnye terminy i opredeleniya. URL: http://docs.cntd.ru/document/1200075565 (accessed: 23.11.2019) (in Russian).
[2] GOST R 50922-2006. Zashchita informatsii. Osnovnye terminy i opredeleniya. URL: http://docs.cntd.ru/document/gost-r-50922-2006 (accessed: 23.11.2019) (in Russian).
[3] Kadnova A.M. Sistema pokazateley kachestva funktsionirovaniya pri sozdanii sistemy informatsionnoy bezopasnosti na obekte informatizatsii OVD O.I. Bokova, A.M. Kadnova, Ye.A. Rogozin, A.S. Serpilin. Pribory i sistemy, upravlenie, kontrol, diagnostika. 2019. № 1. S. 26–33 (in Russian).
[4] Gaskarov V.D. Kontseptualnoe proektirovanie zashchishchennykh avtomatizirovannykh informatsionnykh system V.D. Gaskarov. Vodnye puti i gidrotekhnicheskie sooruzheniya, informatsionnye tekhnologii, portovaya tekhnika i elektromekhanika, sudostroenie i sudoremont, gumanitarnye voprosy, ekonomika i finansy, yurisprudentsiya : sb. nauch. tr. – Sankt-Peterburg, 2008. S. 91–96 (in Russian).
[5] Loyko V.I. Proektirovanie avtomatizirovannykh sistem v zashchishchennom ispolnenii voennogo naznacheniya V.I. Loyko, F.G. Khisamov, R.S. Sherstobitov. Politematicheskiy setevoy elektronnyy nauchnyy zhurnal Kubanskogo gosudarstvennogo agrarnogo universiteta. 2017. № 126. S. 519–532 (in Russian).
[6] Khisamov F.G. Matematicheskaya model otsenki zashchishchennosti informatsii ot nesanktsionirovannogo dostupa pri proektirovanii avtomatizirovannykh sistem v zashchishchennom ispolnenii F.G. Khisamov, A.S. Zhuk, R.S. Sherstobitov. Izvestiya YuFU. Tekhnicheskie nauki. 2017. № 9 (194). S. 91–102 (in Russian).
[7] Gudkov S.N. Osnovnye etapy i zadachi proektirovaniya programmnykh sistem zashchity informatsii v avtomatizirovannykh sistemakh S.N. Gudkov, D.I. Korobkin, Ye.A. Rogozin. Vestnik Voronezhskogo gosudarstvennogo tekhnicheskogo universiteta. 2009. T. 5. № 10. S. 139–142 (in Russian).
[8] Lvovich Ya.Ye. Optimizatsiya proektirovaniya sistem zashchity informatsii v avtomatizirovannykh informatsionnykh sistem promyshlennykh predpriyatiy Ya.Ye. Lvovich, D.S. Yakovlev. Vestnik VGUIT. 2014. №2. S. 90–94 (in Russian).
[9] Kadnova A.M. Imitatsionnaya model funktsionirovaniya sistemy zashchity informatsii ot nesanktsionirovannogo dostupa «Strazh NT» v programmnoy srede «CPN Tools» s tselyu issledovaniya ee vremennykh kharakteristik A.M. Kadnova, Ye.A. Rogozin, Yu.S. Lunev, A.D. Popov. Okhrana, bezopasnost, svyaz 2018: materialy mezhdunarodnoy nauchno-prakticheskoy konferentsii. T 3. № 4(4). Voronezh: VI MVD Rossii, 2019. S. 78–81(in Russian).
[10] Drovnikova I.G. Metodika proektirovaniya sistem informatsionnoy bezopasnosti v avtomatizirovannykh sistemakh I.G. Drovnikova, Ye.A. Rogozin, A.A. Nikitin. Internet-zhurnal «Tekhnologii tekhnosfernoy bezopasnosti». 2016. №4 (68). S. 17–25 (in Russian).
[11] Metody i sredstva otsenki effektivnosti podsistemy zashchity konfidentsialnogo informatsionnogo resursa pri ee proektirovanii v sistemakh elektronnogo dokumentooborota: monografiya / I.G. Drovnikova [i dr.]. Voronezh: Voronezh. gos. tekhn. un-t, 2015. – 106 s.
[12] GOST R 51583-2014 Zashchita informatsii. Poryadok sozdaniya avtomatizirovannykh sistem v zashchishchennom ispolnenii. Obshchie polozheniya. URL: http://docs.cntd.ru/document/1200108858 (accessed: 23.11.2019) (in Russian).
[13] GOST 34.601-90 Informatsionnaya tekhnologiya. Kompleks standartov na avtomatizirovannye sistemy. Avtomatizirovannye sistemy. Stadii sozdaniya. URL: http://docs.cntd.ru/document/1200006921 (accessed: 23.11.2019) (in Russian).

[14] Rogozin Ye.A. Proektirovanie sistem zashchity informatsii ot nesanktsionirovannogo dostupa v avtomatizirovannykh sistemakh organov vnutrennikh del Ye.A. Rogozin, A.D. Popov, T.V. Shagirov. Vestnik Voronezhskogo instituta MVD Rossii. 2016. № 2. S. 174–183 (in Russian).
[15] FSTEK RF. Rukovodyashchiy dokument. Avtomatizirovannye sistemy. Zashchita ot nesanktsionirovannogo dostupa k informatsii. Klassifikatsiya avtomatizirovannykh sistem i trebovaniya po zashchite informatsii. – Moskva: Voenizdat, 1992 (in Russian).
[16] GOST 34.602-89 Informatsionnaya tekhnologiya (IT). Kompleks standartov na avtomatizirovannye sistemy. Tekhnicheskoe zadanie na sozdanie avtomatizirovannoy sistemy. URL: http://docs.cntd.ru/document/1200006924 (accessed: 23.11.2019) (in Russian).
[17] FSTEK RF. Rukovodyashchiy dokument. Kontseptsiya zashchity sredstv vychislitelnoy tekhniki i avtomatizirovannykh sistem ot nesanktsionirovannogo dostupa k informatsii. Moskva: Voenizdat, 1992 (in Russian).

Поступила в редакцию – 01 ноября 2019 г. Окончательный вариант – 01 декабря 2019 г.
Received – November 01, 2019. The final version – December 01, 2019.