Антон А. Конев[1], Татьяна Е. Минеева[1], Михаил Л. Соловьёв[2],
Александр А. Шелупанов[1], Мария П. Силич[1]
[1]Томский государственный университет систем управления и радиоэлектроники,
просп. Ленина, 40, г. Томск, 634050, Россия
e-mail: kaa1@keva.tusur.ru, http://orcid.org/0000-0002-3222-9956
e-mail: tatianamineeva7@gmail.com, http://orcid.org/0000-0003-1702-8731
e-mail: saa@keva.tusur.ru, http://orcid.org/0000-0003-2393-6701
e-mail: mary.silich@yandex.ru, http://orcid.org/0000-0002-5454-1924
[2]Сибирский государственный университет телекоммуникаций и информатики
ул. Кирова, 86, г. Новосибирск, 630102, Россия
e-mail: miksol57@list.ru, http://orcid.org/0000-0002-4242-5571

МОДЕЛЬ ЖИЗНЕННОГО ЦИКЛА СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

DOI: http://dx.doi.org/10.26583/bit.2018.4.03

Аннотация. При построении системы защиты информации одной из ключевых проблем становится создание комплекта нормативной документации. Регуляторы в сфере обеспечения информационной безопасности определяют перечень необходимой документации в основном применительно к механизмам защиты (аутентификация, антивирусная защита и т.п.) и практически не учитывают этапы жизненного цикла средств защиты информации и персонала организации. В статье предлагается подход к формализации составления перечня процессов управления информационной безопасностью, нуждающихся в регламентации. Данный подход позволяет при формировании политики информационной безопасности учитывать процессы управления персоналом и комплексом программно-аппаратных средств защиты информации, что необходимо для обеспечения высокого уровня защищенности объектов критической информационной инфраструктуры.
Ключевые слова: *система защиты информации, жизненный цикл, процессы управления, объект критической информационной инфраструктуры.*
Для цитирования: КОНЕВ, Антон А. et al. МОДЕЛЬ ЖИЗНЕННОГО ЦИКЛА СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ. Безопасность информационных технологий, [S.l.], v. 25, n. 4, p. 34-41, 2018. ISSN 2074-7136. Доступно на: <https://bit.mephi.ru/index.php/bit/article/view/1159>. Дата доступа: 07 nov. 2018. doi:http://dx.doi.org/10.26583/bit.2018.4.03.

Anton A. Konev[1], Tatiana E. Mineeva[1], Mikhail L. Soloviev[2],
Aleksander A. Shelupanov[1], Mariya P. Silich[1]
[1]Tomsk state university of control systems and radioelectronics,
Lenina Av., 40, Tomsk, 634050, Russia
e-mail: kaa1@keva.tusur.ru, http://orcid.org/0000-0002-3222-9956
e-mail: tatianamineeva7@gmail.com, http://orcid.org/0000-0003-1702-8731
e-mail: saa@keva.tusur.ru, http://orcid.org/0000-0003-2393-6701
e-mail: mary.silich@yandex.ru, http://orcid.org/0000-0002-5454-1924
[2]Siberian state university of telecommunications and information sciences
Kirova St, 86, Novosibirsk, 630102, Russia
e-mail: miksol57@list.ru, http://orcid.org/0000-0002-4242-5571

Model of the life cycle of the information security system

DOI: http://dx.doi.org/10.26583/bit.2018.4.03

Abstract. When building an information security system, one of the key problems is the creation of regulatory documents. Regulators in the field of information security determine the list of necessary documentation mainly in relation to protection mechanisms (authentication, anti-virus protection, etc.) and practically do not take into account the stages of the life cycle of information security tools and personnel of the organization. The article proposes an approach to formalization of the list of information security management processes that need regulation. This approach allows the formation of information security policy to take into account the processes of personnel management and the complex of software and hardware information security, which is necessary to ensure a high level of security of critical information infrastructure.
Keywords: information protection system, life cycle, management processes, classification.

For citation: KONEV, Anton A. et al. Model of the life cycle of the information security system. IT Security (Russia), [S.l.], v. 25, n. 4, p. 33-41, 2018. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/1159>. Date accessed: 07 nov. 2018. doi:http://dx.doi.org/10.26583/bit.2018.4.03.

Введение

Вступление в силу Федерального Закона «О безопасности критической информационной инфраструктуры Российской Федерации» [1] с 01.01.2018 г. привело к необходимости разработки практических рекомендаций по обеспечению безопасности соответствующих объектов. В частности, статьей 11 предусматривается «планирование, разработка, совершенствование и осуществление внедрения мероприятий по обеспечению безопасности значимых объектов критической информационной инфраструктуры», а также «принятие организационных и технических мер для обеспечения безопасности значимых объектов критической информационной инфраструктуры». Это означает, что регламентация процессов управления самим объектом критической информационной структуры и комплексом средств защиты информации является крайне актуальной при обеспечении безопасности подобных объектов.

Для конкретизации требований ФЗ «О безопасности критической информационной инфраструктуры РФ» ФСТЭК России были разработаны требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры [2], включающие в том числе и требования по разработке различных нормативных документов, направленных на обеспечение информационной безопасности, на уровне организации. Указанный документ включает требования к обеспечению безопасности в ходе создания, эксплуатации и вывода из эксплуатации значимых объектов.

На сегодняшний день существуют подходы, основанные на разработке эффективных политик безопасности, без которых создание системы защиты информации невозможно [3]. Данные политики безопасности учитывают основные принципы обеспечения информационной безопасности и поддерживаются на протяжении всего жизненного цикла. Но существенным недостатком таких подходов является то, что данной политикой информационной безопасности не учитываются все процессы управления системой защиты информации, следствием чего является низкий уровень защищенности информационной инфраструктуры.

Существует подход к построению системы защиты информации, который основывается на зависимости структуры системы от перечня угроз защищаемой системе. Тем самым модель угроз, на основе которой проектируется структура системы защиты информации, должна включать в себя следующие разделы:

- перечень угроз информации;
- перечень угроз носителям информации;
- перечень угроз элементам информационной системы;
- перечень угроз элементам системы защиты;
- перечень угроз, касающихся управления системой защиты [4].

Модель угроз информации и ее носителям, модель угроз, направленных на информационную систему, представлены в работах [5] и [6]. Необходимо рассмотреть и угрозы, направленные на процессы управления самой системой. Но для получения модели угроз необходимо формализованное описание самих процессов управления защищаемым объектом.

Построение модели жизненного цикла

Под моделью жизненного цикла понимается структурная основа процессов и действий, относящихся к жизненному циклу, которая служит в качестве общей ссылки для установления связей и взаимопонимания сторон [7].

Собственно, жизненный цикл системы — это непрерывный процесс с момента создания системы и до полного завершения ее работы. Процессы управления

предназначены для реализации управляющих действий в отношении системы защиты информации [8].

Для построения модели жизненного цикла была проведена классификация процессов управления системой защиты информации и ее составляющих. Согласно Приказу ФСТЭК России № 235 "Об утверждении Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования, система защиты информации включает силы обеспечения безопасности значимых объектов (персонал) и средства обеспечения безопасности, к таковым относятся программно-аппаратные средства, а также организационную документацию, в соответствии с которой функционирует система безопасности [9].

Классификация процессов управления основывается на определении состояния, которое будет воздействовать на данный процесс на различных этапах жизненного цикла средств защиты информации и персонала организации [10]. Соответственно, были сформированы следующие классы процессов управления:

- процессы, связанные с приобретением/уничтожением;
- процессы, связанные с вводом/выводом из эксплуатации;
- процессы, связанные с эксплуатацией;
- процессы, связанные с проверкой/улучшением;
- процессы, связанные с контролем функционирования/доработкой.

В один класс были объединены противоположные процессы, так как они воздействуют на одни и те же состояния объекта критической информационной инфраструктуры.

На основе данной классификации были построены модели жизненного цикла программно-аппаратных средств защиты, персонала организации, а также нормативной документации.

Стоит пояснить, что процессы, связанные с вводом/выводом из эксплуатации, включают в себя процессы, связанные с правами на работу с конфиденциальной информацией. Например, процесс управления класса ввода/вывода из эксплуатации персонала- это допуск к конфиденциальной информации сотрудника или отбор прав на работу с данной информацией соответственно.

На рис. 1 представлена модель жизненного цикла программных средств защиты информации. Данная модель также подходит и для аппаратных средств защиты, так как состояния на различных этапах жизненного цикла, а также процессы управления данными средствами будут аналогичными.

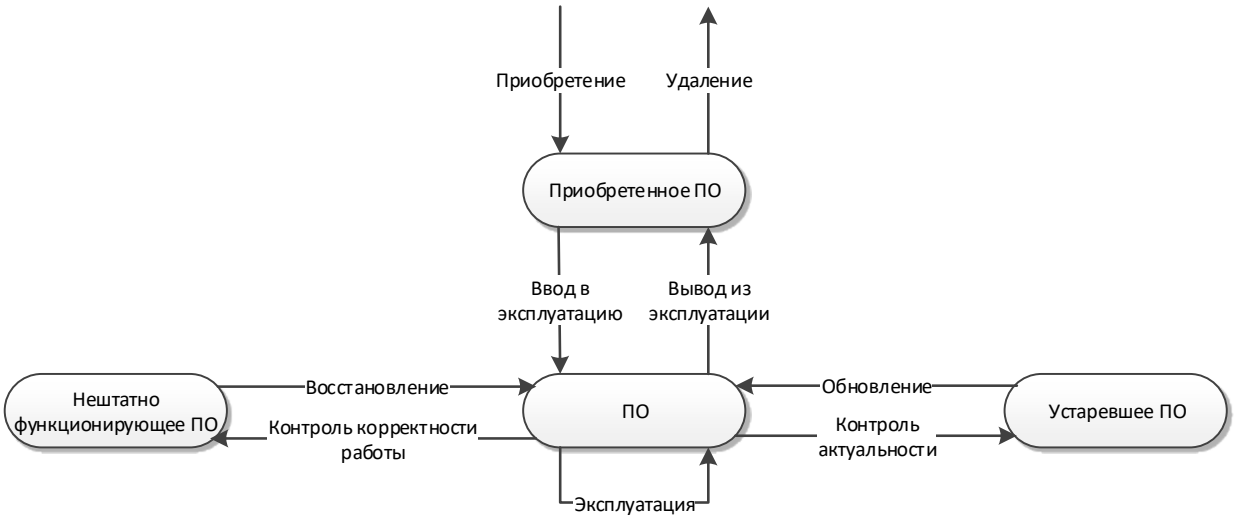

Рис. 1. Модель жизненного цикла программного и аппаратного обеспечения
(Fig. 1. Software and hardware lifecycle model)

Жизненный цикл программно-аппаратных средств защиты информации начинается с момента их приобретения. Основные задачи, выполняемые на этом этапе, – определение требований к продукту и определение потребности в нем [11].

Затем купленное или разработанное ПО вводится в эксплуатацию. В целях сопровождения программно-аппаратных средств защиты проводится контроль корректности работы. Контроль является одним из важных направлений работ по защите информации, его целью является выявление слабых мест, а также допущенных ошибок. Программное обеспечение не подвержено физическому износу, но в ходе его эксплуатации обнаруживаются неисправности, требующие исправления [12]. Неисправности могут также возникать при изменении условий использования программы.

При выявлении каких-либо ошибок в работе проводится восстановление работоспособности, исправление найденных ошибок [13].

При контроле актуальности выясняется степень устаревания продукта, за которым следует процесс обновления, если средство защиты устарело. Если было принято решение о приостановлении эксплуатации программного обеспечения, а именно прекращение доступа данного ПО на работу с конфиденциальной информацией, то происходит процесс вывода из эксплуатации [14] с последующей деактивацией программы (удалением).

Аналогичный жизненный цикл будет и у нормативной документации (рис. 2).

Функционирование нормативной документации является важным вопросом, так как именно ей определяются правила и требования, которые реализует персонал в совокупности с программно-аппаратным обеспечением. А от совокупности работы всех составляющих системы защиты информации и зависит надлежащий уровень информационной безопасности организации.

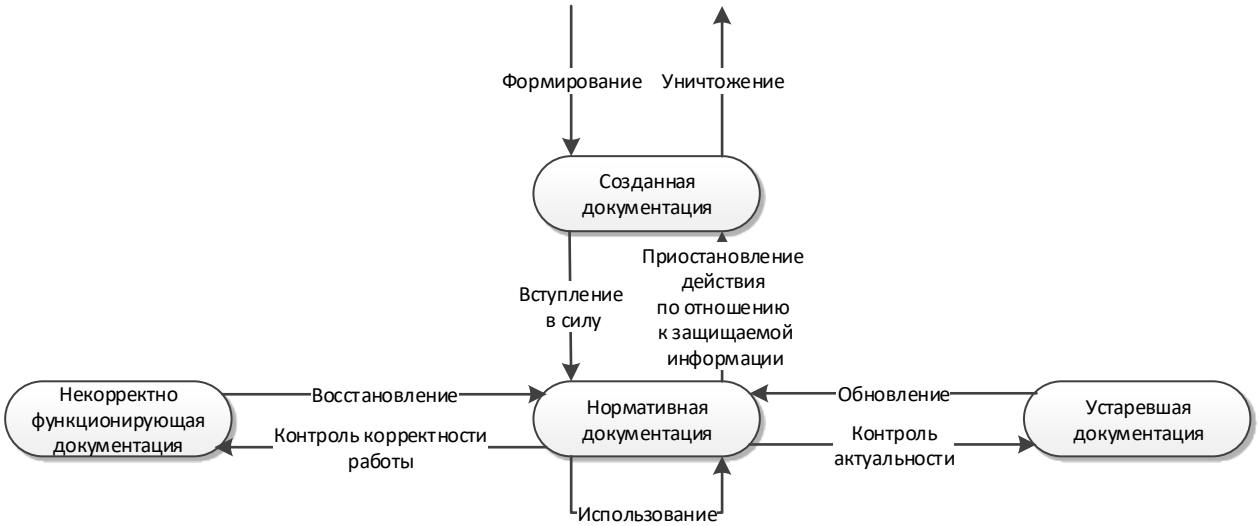

Рис. 2. Модель жизненного цикла нормативной документации
(Fig. 2. Life-cycle model of regulatory documents)

Сначала происходит решение о формировании конкретной документации, затем принимается решение о вступлении данной документации в силу. Далее происходят все те же процессы, что и с программно-аппаратными средствами защиты [15]. Процесс приостановления действия документации по отношению к защищаемой информации – это процесс, когда документация, относящаяся к конкретной защищаемой информации, становится недействующей по причине прекращения работы какого-либо продукта, функцией которого являлась защита информации, либо по причине прекращения потребности в защите определённого вида информации [16]. Затем по решению руководства данная документация полностью уничтожается.

Все аналогичные процессы управления относятся и к жизненному циклу сотрудников (рис. 3).

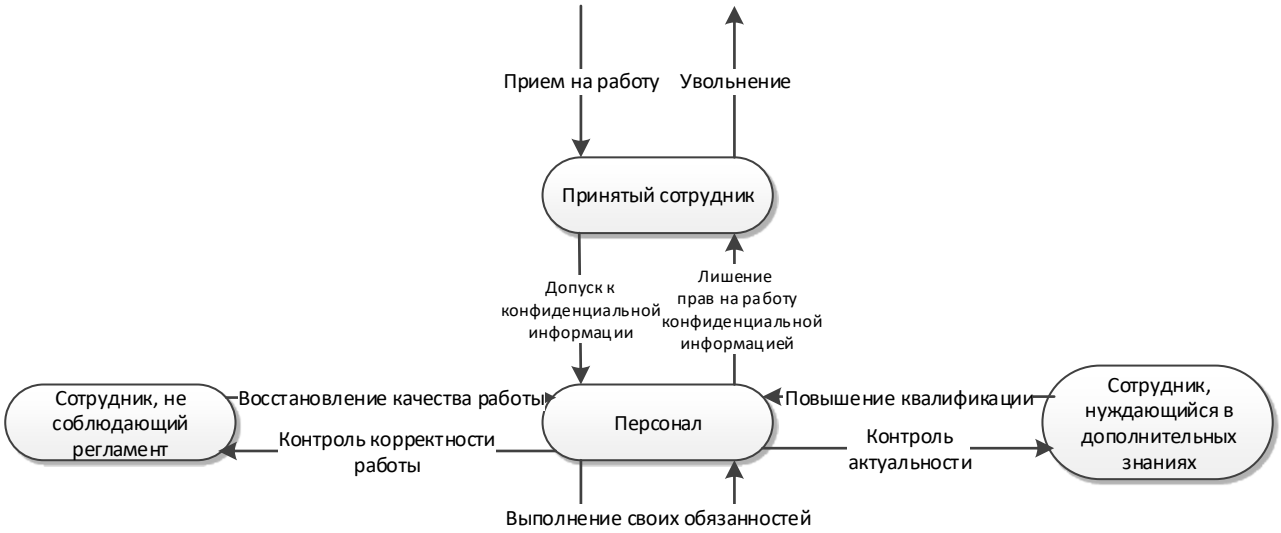

Рис. 3. Модель жизненного цикла сотрудников
(Fig. 3. Employee life cycle model)

Процессы управления сотрудниками это - целенаправленное воздействие на персонал, ориентированное на приведение в соответствие возможностей персонала и целей, стратегий и условий развития организации [17].

По данным моделям жизненного цикла программно-аппаратных средств защиты, нормативной документации и персонала была составлена типовая модель жизненного цикла системы защиты информации (рис. 4).

Были выделены основные этапы жизненного цикла [18]:

- планирование;
- ввод в эксплуатацию;
- эксплуатация;
- контроль за функционированием;
- улучшение;
- вывод из эксплуатации;
- уничтожение.

В рамках процесса планирования осуществляются разработка и утверждение плана мероприятий по обеспечению критической информационной инфраструктуры [19].

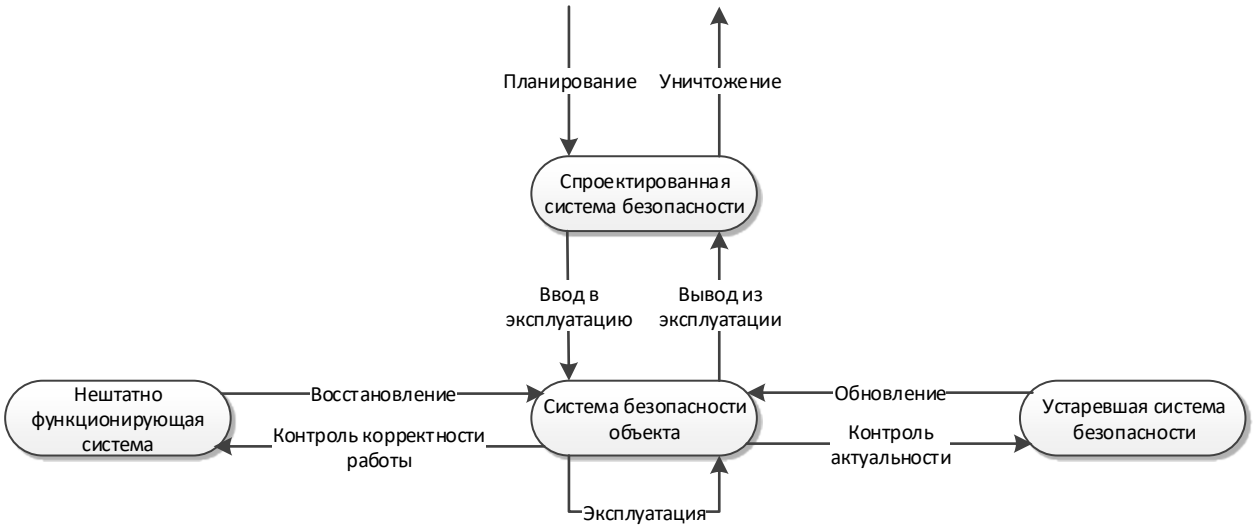

Рис. 4. Модель жизненного цикла системы защиты информации
(Fig. 4. Information security system life cycle model)

Модель жизненного цикла системы защиты информации отражает состояния и процессы управления ее составляющих, а именно: программно-аппаратных средств защиты, нормативной документации и персонала, также при ее построении были учтены основные этапы жизненного цикла системы.

Сравнивая данную модель с требованиями по обеспечению безопасности значимых объектов критической информационной инфраструктуры, можно отметить, что все процессы управления системой перекрываются мерами обеспечения безопасности, содержащимися в рассматриваемом нормативном документе. Например, «выявление компьютерных инцидентов» проводится на этапе контроля корректности работы системы, а «разделение полномочий пользователей» подчинено процессу допуска к конфиденциальной информации. Данное соответствие говорит об актуальности данной модели и о том, что при формировании политики информационной безопасности в организации будут учтены процессы управления системой защиты информации, что позволит обеспечить высокий уровень защищенности информационной инфраструктуры.

Также стоит отметить, что разработанная модель учитывает следующие требования по обеспечению безопасности значимых объектов информационной инфраструктуры, которые не рассматриваются выше указанным нормативным документом:

1. Лишение прав сотрудника на работу с критической информацией.
2. Восстановление корректности работы значимого объекта.
3. Требования по обеспечению безопасности на этапе вывода из эксплуатации значимого объекта.
4. Требования по обеспечению безопасности на этапе уничтожения или удаления значимого объекта.

Тем самым можно дополнить перечень требований по обеспечению безопасности, содержащийся в нормативном документе ФСТЭК России требованиями разработанной модели жизненного цикла системы защиты информации.

Заключение

На основе классификации процессов управления системы защиты информации были построены модели жизненного цикла программно-аппаратных средств защиты, нормативной документации и персонала организации, а также модель жизненного цикла самой системы защиты информации. Были выделены этапы жизненного цикла, на основе которых и проведена классификация процессов управления системой защиты информации.

По результатам сравнения с требованиями по обеспечению безопасности значимых объектов было выявлено, что все выделенные процессы управления системой защиты информации перекрываются мерами обеспечения безопасности, которые приведены в рассматриваемом нормативном документе. Разработанная модель включает в себя все процессы управления системы защиты информации, а также учитывает несколько требований по обеспечению безопасности значимых объектов информационной инфраструктуры, которые не рассматриваются в документах ФСТЭК России, что является преимуществом перед уже существующими подходами решения данной проблемы.

Построенная модель позволит рассмотреть каждый из классов процессов управления более подробно и в дальнейшем раскрыть перечень угроз, направленных непосредственно на процессы управления информационной безопасностью, нуждающиеся в регламентации. Соответственно, рассмотрев перечень угроз, можно будет описать механизмы защиты, направленные на минимизацию этих угроз, что обеспечит безопасность критической информационной инфраструктуры.

СПИСОК ЛИТЕРАТУРЫ:

1. О безопасности критической информационной инфраструктуры Российской Федерации: Федеральный закон от 26.07.2017 № 187-ФЗ // СПС КонсультантПлюс.
2. Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации: приказ ФСТЭК России от 25.12.2017 № 239 // СПС КонсультантПлюс.
3. Зайцев С.Е. Политики информационной безопасности в системах информационной безопасности // Научный вестник Московского государственного технического университета гражданской авиации (137) 2008. С. 37 – 44.
4. Конев А.А., Давыдова Е.М. Подход к описанию структуры системы защиты информации // Доклады ТУСУР. 2013. № 2 (28). С. 107 – 111.
5. Novokhrestov A., Konev A. Mathematical model of threats to information systems // AIP conference proceedings (Tomsk, 26 – 29 April 2016). Tomsk, 2016. Vol. 1772. P. 060015.
6. Новохрестов А.К., Конев А.А., Шелупанов А.А., Егошин Н.С. Модель угроз безопасности информации и ее носителей // Вестник Иркутского государственного технического университета. 2017. Т. 21. № 10. С. 93 – 104
7. ГОСТ Р 50922-96. Защита информации. Основные термины и определения. М.: Стандартинформ, 2008. – 12 с.
8. Грибунин В.Г. Комплексная система защиты информации на предприятии [Текст]: учебное пособие для студентов высших учебных заведений / В.Г. Грибунин, В.В. Чудовский. – М.: Издательский центр «Академия», 2009. – 416 с.
9. Об утверждении Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования: приказ Федеральной службы по техническому и экспортному контролю от 21 декабря 2017 г. № 235 // СПС КонсультантПлюс.
10. ГОСТ Р ИСО/МЭК 15288-2005. Информационная технология. Системная инженерия. Процессы жизненного цикла систем. М.: Стандартинформ, 2006. – 53 с.
11. И.А. Жуклинец, О.Н. Марков. Управление процессами ИБ в интересах бизнеса. Технологии безопасности № 1 (24) – 2013.
12. Доросинский Л. Г. Информационные технологии поддержки жизненного цикла изделия / Л.Г. Доросинский, О. М. Зверева. – Ульяновск: Издательство «Зебра», 2016. – 243 с. – ISBN 978-5-9908739-8-8.
13. Скопин И.Н. Понятия и модели жизненного цикла программного обеспечения: Учебное пособие Новосиб. гос. ун-т. – Новосибирск, 2012.
14. Дорофеев А.В., Марков А.С. Менеджмент информационной безопасности. Основные концепции. Вопросы кибербезопасности № 1(2) – 2014, С. 67 – 73.
15. ГОСТ Р ИСО/МЭК 27001 – 2006. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. М.: Стандартинформ, 2008. –31с.
16. РС БР ИББС-2.6-2014. Обеспечение информационной безопасности на стадиях жизненного цикла автоматизированных банковских систем [Электронный ресурс]. – Режим доступа: http://www.cbr.ru/credit/gubzi_docs/rs-26-14.pdf (дата обращения 18.05.2018).
17. Гришина Н.В. Организация комплексной системы защиты информации. [Текст] / Н.В. Гришина – М.: Гелиос АРВ, 2007. – 256 с.
18. Бочков С.И. О ценности информации на различных этапах жизненного цикла. Правовая информатика № 3 – 2016, С. 35 – 40.
19. Об утверждении формы направления сведений о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий: приказ Федеральной службы по техническому и экспортному контролю от 22.12.2017 г. № 236 // СПС КонсультантПлюс.

REFERENCES:

[1] On the Security of the Critical Information Infrastructure of the Russian Federation: Federal Law of July 26, 2017 No. 187-FZ. SPS ConsultantPlus.
[2] On approval of the Requirements for ensuring the security of significant objects of the critical information infrastructure of the Russian Federation: Order FSTEC of Russia of 25.12.2017 No. 239. ATP ConsultantPlus.
[3] Zaitsev S.E. Information security policies in information security systems. Scientific Bulletin of Moscow State Technical University of Civil Aviation (137) 2008. P. 37 – 44.
[4] Konev A.A., Davydova E.M. Approach to structuring information security systems. Doklady Tomskogo gosudarstvennogo universiteta sistem upravlenija i radiojelektroniki [Proceedings of Tomsk State University of Control Systems and Radioelectronics]. 2013, no. 2 (28), pp. 107 – 111.
[5] Novokhrestov A., Konev A. Mathematical model of threats to information systems. AIP conference proceedings (Tomsk, 26 – 29 April 2016). Tomsk, 2016, vol. 1772, pp. 060015.
[6] Novokhrestov A.K., Konev A.A., Shelupanov A.A., Egoshin N.S. Information and information carrier security threat model. Proceedings of Irkutsk State Technical University. 2017, vol. 21, no. 10, pp. 93–104.

[7] GOST R 50922-96. Data protection. Basic terms and definitions. Moscow: Standardinform, 2008. - 12 p.
[8] Gribunin V.G. Integrated system of information security at the enterprise [Text]: textbook for students of higher educational institutions. V.G. Gribunin, V.V. Chudovsky. - Moscow: Publishing Center "Academy", 2009. - 416 p.
[9] On approval of the Requirements for the creation of security systems for significant objects of the critical information infrastructure of the Russian Federation and ensuring their functioning: the order of the Federal Service for Technical and Export Control dated December 21, 2017 No. 235. SPS ConsultantPlus.
[10] GOST R ISO IEC 15288-2005. Information technology. System engineering. Processes of the life cycle of systems. Moscow: Standartinform, 2006. – 53 p.
[11] I.A. Zhukliniec, ON Markov. Management of IB processes in the interests of business. Security technologies №1 (24) – 2013.
[12] Dorosinsky LG Information technology to support the product life cycle. LG Dorosinsky, OM Zvereva. - Ulyanovsk: Zebra Publishing House, 2016. - 243 p. - ISBN 978-5-9908739-8-8.
[13] Skopin I.N. Concepts and models of the life cycle of software: Textbook Novosib. state. un-t. - Novosibirsk, 2012.
[14] Dorofeev AV, Markov AS Information Security Management. Basic concepts. Cybersecurity issues №1 (2) - 2014, pp. 67 – 73.
[15] GOST R ISO IEC 27001 - 2006. Information technology. Methods and means of ensuring security. Information security management systems. Moscow: Standardinform, 2008. - 31p.
[16] RS BR BRSI-2.6-2014. Ensuring information security at the stages of the life cycle of automated banking systems [Electronic resource]. - Access mode: http://www.cbr.ru/credit/gubzi_docs/rs-26-14.pdf (circulation date is May 18, 2018).
[17] Grishina N.V. Organization of a comprehensive information security system. [Text]. N.V. Grishina-M.: Helios ARV, 2007. – 256 p.
[18] Bochkov S.I. On the value of information at various stages of the life cycle. Legal Informatics № 3 - 2016, P. 35 – 40.
[19] On approval of the form for sending information on the results of assigning to the object a critical information infrastructure of one of the significance categories or about the absence of the need to assign to it one of such categories: the order of the Federal Service for Technical and Export Control dated December 22, 2017 No. 236. SPS ConsultantPlus.

Поступила в редакцию – 17 августа 2018 г. Окончательный вариант – 01 ноября 2018 г.
Received – August 17, 2018. The final version – November 01, 2018.