СБОРНИК **НАУЧНЫХ ТРУДОВ НГТУ. – 2019. – № 2 (95).** – 57–65

УДК 006.78.013 DOI: 10.17212/2307-6879-2019-2-57-65

АНАЛИЗ НОРМАТИВНО-ПРАВОВЫХ ДОКУМЕНТОВ НА ЭТАПЕ ПОДГОТОВКИ К РАЗРАБОТКЕ ПРОГРАММЫ И МЕТОДИКИ ИСПЫТАНИЙ ЗНАЧИМОГО ОБЪЕКТА КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ РФ (ИСПДн)*

А.А. ЕРОХИНА[1], В.В. СЕЛИФАНОВ[2]

[1] *630073, РФ, г. Новосибирск, пр. Карла Маркса, 20, Новосибирский государственный технический университет, студентка кафедры защиты информации. E-mail: eroxina1997@bk.ru*

[2] *630073, РФ, г. Новосибирск, пр. Карла Маркса, 20, Новосибирский государственный технический университет, старший преподаватель кафедры защиты информации. E-mail: sfo1@mail.ru*

Рассматривается проблема разработки программы и методик испытаний значимого объекта критической информационной инфраструктуры Российской Федерации, использование информационной системы персональных данных.

В данном случае информационная система является одновременно значимым объектом. Средства защиты информации, используемые в данной системе, должны пройти оценку соответствия в форме испытаний. По приказу ФСТЭК № 21 средства защиты информационной системы персональных данных не обязаны проходить оценку соответствия в форме обязательной сертификации, но по приказу ФСТЭК № 239 средства защиты значимого объекта должны пройти оценку соответствия в форме обязательной сертификации, испытаний или приемки.

Таким образом, наличие программы и методики испытаний, а также проведенные испытания оборудования, обязательное требование для получения разрешения на его применение. Именно поэтому данная проблема является актуальной. На многих значимых объектах критической информационной инфраструктуры Российской Федерации используется информационная система персональных данных, которая требует ввода в эксплуатацию соответствующих средств защиты информации.

В связи с этим возникает потребность в разработке программы и методик испытаний значимого объекта критической информационной инфраструктуры Российской Федерации информационной системы персональных данных, в которых будут описаны приемочные испытания, содержащие оценку соответствия требованиям по безопасности в форме испытаний для средств защиты информации, и требования к оборудованию, используемому на данном объекте.

* Статья получена 10 июня 2019 г.

Ключевые слова: безопасность КИИ, категорирование, объекты КИИ, значимость объектов, ИСПД, приемочные испытания, нормативно-правовые документы, система защиты ИСПДн, программа и методика испытаний, оценка требований СЗИ

ВВЕДЕНИЕ

Ввод в действие значимого объекта и его подсистемы безопасности осуществляется при положительном заключении (выводе) в акте приемки о соответствии значимого объекта установленным требованиям по обеспечению безопасности. Данный акт составляется после прохождения приемочных испытаний. По закону данные испытания не могут проводиться без написанных методик испытаний и программы. Поэтому встает необходимость в разработке программы и методик испытаний значимого объекта критической информационной инфраструктуры Российской Федерации. Поэтому целью работы является анализ нормативно-правовых документов в области критической информационной системы (КИИ), информационная система персональных данных (ИСПДн) и разработка программы и методики испытаний.

Для разработки программы и методик необходимо проанализировать исходные данные (модель угроз безопасности информации, результаты (акт) категорирования т. д.) и нормативно-правовые документы. Исходя из анализа разработать программу и методику испытаний.

Задачи:

– оценка нормативно-правовых данных и исходных данных для проведения испытаний;

– оценка нормативно-правовых данных в области КИИ;

– оценка нормативно-правовых данных в области ИСПДн.

1. ОЦЕНКА НОРМАТИВНО-ПРАВОВЫХ ДАННЫХ В ОБЛАСТИ КИИ И ИСПДн

В данном случае рассматривается информационная система персональных данных, которая одновременно является значимым объектом критической информационной инфраструктуры Российской Федерации.

Для определения требований по обеспечению безопасности обратимся к Приказу ФСТЭК от 25 декабря 2017 г. № 239 «Об утверждении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации». Для средств защиты информации, используемых на значимом объекте критической информационной инфраструктуры информационной системы персональных данных, должна быть

проведена оценка соответствия требованиям по безопасности в формах обязательной сертификации, испытаний или приемки. Это требование описано в пункте 28 вышеупомянутого приказа: «Для обеспечения безопасности значимых объектов критической информационной инфраструктуры должны применяться средства защиты информации, прошедшие оценку на соответствие требованиям по безопасности в формах обязательной сертификации, испытаний или приемки. Средства защиты информации, прошедшие оценку соответствия в форме обязательной сертификации, применяются в случаях, установленных законодательством Российской Федерации, а также в случае принятия решения субъектом критической информационной инфраструктуры. В иных случаях применяются средства защиты информации, прошедшие оценку соответствия в форме испытаний или приемки, которые проводятся субъектами критической информационной инфраструктуры самостоятельно или с привлечением организаций, имеющих в соответствии с законодательством Российской Федерации лицензии на деятельность в области защиты информации».

В пункте 5 Приказа ФСТЭК от 25 декабря 2017 г. № 239 сказано, что для обеспечения безопасности значимых объектов, являющихся информационными системами персональных данных, настоящие требования применяются с учетом требований, утвержденных Постановлением Правительства Российской Федерации от 1 ноября 2012 г. № 1119. Из Постановления Правительства № 1119 в пункте 4 узнаем, что выбор средств защиты информации для системы защиты персональных данных осуществляется в соответствии с нормативными правовыми актами Федеральной службой по техническому и экспортному контролю. Таким образом, переходим к Приказу ФСТЭК от 18 февраля 2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

В вышеупомянутом приказе в пункте 1 указано, что «меры по обеспечению безопасности персональных данных реализуются в том числе посредством применения в информационной системе средств защиты информации, прошедших в установленном порядке процедуру оценки соответствия, в случаях, когда применение таких средств необходимо для нейтрализации актуальных угроз безопасности персональных данных», то есть могут использоваться средства защиты информации (персональных данных), не прошедшие оценку соответствия требованиям по безопасности в форме обязательной сертификации, испытаний или приемки.

В данном случае информационная система является одновременно значимым объектом. Средства защиты информации, используемые в данной систе-

ме, должны пройти оценку соответствия в форме испытаний. По Приказу ФСТЭК № 21 средства защиты информационной системы персональных данных не обязаны проходить оценку соответствия в форме обязательной сертификации, но по приказу ФСТЭК № 239 средства защиты значимого объекта должны пройти оценку соответствия в форме обязательной сертификации, испытаний или приемки.

По Приказу ФСТЭК № 239 ввод в действие значимого объекта и его подсистемы безопасности осуществляется при положительном заключении (выводе) в акте приемки о соответствии значимого объекта установленным требованиям по обеспечению безопасности. Данный акт составляется после прохождения приемочных испытаний. По закону данные испытания не могут проводиться без написанных программы и методик испытаний.

2. ОЦЕНКА НОРМАТИВНО-ПРАВОВЫХ ДАННЫХ И ИСХОДНЫХ ДАННЫХ ДЛЯ ПРОВЕДЕНИЯ ИСПЫТАНИЙ

Программа и методика испытаний – это документ, входящий в комплект конструкторской документации, составляемой на автоматизированную систему. Программа и методики испытаний призваны установить технические данные, которые подлежат проверке во время испытаний всей системы в целом или ее отдельных компонентов.

Чтобы узнать, какие разделы должны быть включены в программу и методики испытаний, обратимся к ГОСТ 34.603-92 «Информационная технология (ИТ). Виды испытаний автоматизированных систем». В данном ГОСТе описаны программы и методики для всех испытаний (предварительных, опытной эксплуатации, приемочных). Программа и методика для приемочных испытаний должны содержать следующие разделы:

– перечень объектов, выделенных в системе для испытаний, и перечень требований, которым должны соответствовать объекты (со ссылкой на пункты ТЗ);
– критерии приемки системы и ее частей;
– условия и сроки проведения испытаний;
– средства для проведения испытаний;
– фамилии лиц, ответственных за проведение испытаний;
– методика испытаний и обработки их результатов;
– перечень оформляемой документации.

Так как среди средств защиты информации используются программные продукты, обращаемся к государственному стандарту ГОСТ 19.301-79, согласно которому «программа и методика испытаний» оформляются в соответ-

ствии с ГОСТ 19.105-78 (общие требования к оформлению программных документов) и должна содержать следующие разделы:

– объект испытаний (указывают наименование, область применения и обозначение испытуемой программы);

– цель испытаний (должна быть указана цель проведения испытаний);

– требования к программе (должны быть указаны требования, подлежащие проверке во время испытаний и заданные в техническом задании на программу);

– требования к программной документации (должны быть указаны состав программной документации, предъявляемой на испытания, а также специальные требования, если они заданы в техническом задании на программу);

– средства и порядок испытаний (должны быть указаны технические и программные средства, используемые во время испытаний, а также порядок проведения испытаний);

– методы испытаний (должны быть приведены описания используемых методов испытаний).

В методах испытаний должны быть приведены описания проверок с указанием результатов проведения испытаний (перечней тестовых примеров, контрольных распечаток тестовых примеров и т. п.).

С помощью программы и методики испытаний составляем содержание для разрабатываемой программы испытаний значимого объекта критической информационной инфраструктуры Российской Федерации информационной системы персональных данных. Данная программа испытаний будет включать в себя разделы:

1) объект испытаний (указывают наименование, область применения, перечень объектов, выделенных в системе для испытаний, и фамилии лиц, ответственных за проведение испытаний);

2) цель испытаний (должна быть указана цель проведения испытаний);

3) требования к программе (перечень требований, которым должны соответствовать объекты (со ссылкой на пункты ТЗ));

4) требования к программной документации (должен быть указан состав программной документации, предъявляемой на испытания);

5) средства и условия испытаний (должны быть указаны технические и программные средства, используемые во время испытаний, а также условия и сроки проведения испытаний);

6) методы испытаний (должны быть приведены описания используемых методов испытаний);

7) перечень оформляемой документации.

Для проведения приемочных испытаний должна быть предъявлена следующая документация:

– техническое задание на создание АС;

– акт приемки в опытную эксплуатацию;

– рабочие журналы опытной эксплуатации;

– акт завершения опытной эксплуатации и допуска АС к приемочным испытаниям.

В зависимости от категории значимости объекта критической информационной инфраструктуры, которая определяется по Постановлению Правительства РФ от 8 февраля 2018 г. № 127 «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений», в программе и методике испытаний прописываются требования к средствам защиты информации. Эти требования должны соответствовать мерам по обеспечению безопасности для значимого объекта прописанных в приложение к Требованиям по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации, утвержденным Приказом ФСТЭК России от 25 декабря 2017 г. № 239 «Состав мер по обеспечению безопасности для значимого объекта соответствующей категории значимости».

ЗАКЛЮЧЕНИЕ

В статье описано, как должна выглядеть структура данного документа и какие документы должны быть предъявлены до проведения испытаний на основе ГОСТ 34.603-92 «Информационная технология (ИТ). Виды испытаний автоматизированных систем». На основе Приказа ФСТЭК России от 25 декабря 2017 г. № 239 и Приказа ФСТЭК от 18 февраля 2013 г. № 21 описано, какие требования указывать для оценки соответствия (в форме обязательных испытаний) средств защиты информации значимого объекта критической информационной инфраструктуры Российской Федерации информационной системы персональных данных.

СПИСОК ЛИТЕРАТУРЫ

1. Постановление Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

2. Постановление Правительства Российской Федерации от 8 февраля 2018 г. № 127 «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений».

3. Приказ Федеральной службы по техническому и экспортному контролю от 18 февраля 2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

4. Приказ Федеральной службы по техническому и экспортному контролю от 25 декабря 2017 г. № 239 «Об утверждении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации».

5. ГОСТ 19.301–79. Программа и методика испытаний. Требования к содержанию и оформлению. – Введ. 01.01.80. – М.: Стандартинформ, 2010.

6. ГОСТ 34.603–92. Информационная технология (ИТ). Виды испытаний автоматизированных систем. – Взамен ГОСТ 24.104-85 в части разд. 3: введ. 01.01.93. – М.: Изд-во стандартов, 1992.

Ерохина Анастасия Алексеевна, студентка кафедры защиты информации Новосибирского государственного технического университета. E-mail: Valeria.Ivanova97@yandex.ru

Селифанов Валентин Валерьевич, старший преподаватель кафедры защиты информации Новосибирского государственного технического университета. E-mail: sfo1@mail.ru

DOI: 10.17212/2307-6879-2019-2-57-65

Analysis of legal documents in preparation for the development of programs and significant objects test procedures critical information infrastructure of the RF (PDIS)*

A.A. Erohina[1], V.V. Selifanov[2]

[1] *Novosibirsk State Technical University, 20 Karl Marks Avenue, Novosibirsk, 630073, Russian Federation, student of information security department. E-mail: eroxina1997@bk.ru*
[2] *Novosibirsk State Technical University, 20 Karl Marks Avenue, Novosibirsk, 630073, Russian Federation, candidate of Technical Sciences, Senior Lecturer at the Department of Information Security. E-mail: sfo1@mail.ru*

The commissioning of a significant object on which the personal data information system is used, and its security subsystem is carried out with a positive conclusion in the act of acceptance of the compliance of the significant object with the established safety requirements. This act is drawn up after passing the acceptance tests. Accordingly, to obtain permission for the use of significant objects requires a program and test methods. An up-to-date solution is the development of a program and test methods for a significant object of the critical information infrastructure of the Russian Federation, an information system for personal data, which will describe acceptance tests containing an assessment of compliance with safety requirements in the forms of mandatory certification, testing or acceptance for information security tools, equipment requirements, used on this site.
In this case, the information system is at the same time a significant object, the information security tools used in this system must be evaluated in the form of tests. By order of FSTEC № 21, the means of protecting the information system of personal data are not required to pass a conformity assessment in the form of mandatory certification, but by order of FSTEC № 239 the means of protection of a significant object must pass a conformity assessment in the form of mandatory certification, testing or acceptance. Analyzing these conditions, it was determined to develop a conformity assessment in the form of tests.
The program and testing methodology is a document included in the set of design documentation drawn up for an automated system. On the basis of regulatory documents, we prepare the content for the test program being developed.
Depending on the category of significance of the critical information infrastructure object, the requirements for information security tools must comply with the security measures for the relevant object and the prescribed order of FSTEC №239.

Keywords: security of critical information infrastructure, categorization, objects of critical information infrastructure, significance of objects, personal data information system, acceptance tests

* *Received 10 June 2019.*

REFERENCES

1. Decree of the Government of the Russian Federation of November 1, 2012 N 1119 “On approval of requirements for the protection of personal data when they are processed in personal data information systems”. (In Russian).

2. Decree of the Government of the Russian Federation of February 8, 2018 N 127 “On Approval of the rules for categorizing the objects of critical information infrastructure of the Russian Federation, as well as a list of indicators of the criteria of significance of the objects of critical information infrastructure of the Russian Federation and their values”. (In Russian).

3. Order of the FSTEC Russia of February 18, 2013 N 21 “On approval of the composition and content of organizational and technical measures to ensure the security of personal data when they are processed in personal data information systems”. (In Russian).

4. Order of the FSTEC Russia of December 25, 2017 N 239 “On approval of requirements for ensuring security of significant objects of critical information infrastructure of the Russian Federation”. (In Russian).

5. GOST 19.301–79. Program and methods of testing. Requirements for contents and form of presentation. Moscow, Standartinform Publ., 2010. (In Russian).

6. GOST 34.603–92. Information technology. Types tests automated systems. Moscow, Standads Publ., 1992.

Для цитирования:

Ерохина А.А., Селифанов В.В. Анализ нормативно-правовых документов на этапе подготовки к разработке программы и методики испытаний значимого объекта критической информационной инфраструктуры РФ (ИСПДн*)* // Сборник научных трудов НГТУ. – 2019. – № 2 (95). – С. 57–65. – DOI: 10.17212/2307-6879-2019-2-57-65.

For citation:

Erohina A.A., Selifanov V.V. Analiz normativno-pravovyh dokumentov na etape podgotovki k razrabotke programmy i metodiki ispytanij znachimogo ob"ekta kriticheskoj informacionnoj infrastruktury RF (ISPDn) [Analysis of legal documents in preparation for the development of programs and significant objects test procedures critical information infrastructure of the RF (PDIS)]. *Sbornik nauchnykh trudov Novosibirskogo gosudarstvennogo tekhnicheskogo universiteta – Transaction of scientific papers of the Novosibirsk state technical university*, 2019, no. 2 (95), pp. 57–65. DOI: 10.17212/2307-6879-2019-2-57-65.