СБОРНИК **НАУЧНЫХ ТРУДОВ НГТУ. – 2019. – № 2 (95).** – 66–74

УДК 004.056.5 DOI: 10.17212/2307-6879-2019-2-66-74

АНАЛИЗ ДОКУМЕНТОВ ПО РАЗРАБОТКЕ ПРОГРАММЫ И МЕТОДИК АТТЕСТАЦИОННЫХ ИСПЫТАНИЙ ЗНАЧИМОГО ОБЪЕКТА КРИТИЧЕСКОЙ ИНФРАСТРУКТУРЫ РФ (ГИС)*

В.А. ИВАНОВА[1], В.В. СЕЛИФАНОВ[2]

[1] *630073, РФ, г. Новосибирск, пр. Карла Маркса, 20, Новосибирский государственный технический университет, студентка кафедры защиты информации. E-mail: Valeria.Ivanova97@yandex.ru*
[2] *630073, РФ, г. Новосибирск, пр. Карла Маркса, 20, Новосибирский государственный технический университет, старший преподаватель кафедры защиты информации. E-mail: sfo1@mail.ru*

После вступления в силу 1 января 2018 года Федерального закона 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» перед организациями и специалистами, работающими в области информационной безопасности объектов критических инфраструктур, стали задачи выполнения этого закона и всего множества связанных с ним подзаконных актов.

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

Применяемые мероприятия по безопасности объектов КИИ определяются в соответствии с его категорией значимости. Для незначимого объекта КИИ должна быть обеспечена интеграция с ГосСОПКА. Категория значимости определяется исходя из «Правил категорирования объектов критической информационной инфраструктуры Российской Федерации» утвержденных соответствующим Постановлением Правительства от 8 февраля 2018 г. № 127.

Аттестация прописана для государственных информационных систем, являющихся значимыми объектами КИИ. Основополагающим документом является Приказ ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах». При аттестационных испытаниях проводится анализ уязвимостей средств защиты информации, технических средств и программного обеспечения. Если уязвимости обнаружены, то необходимо их устранение или снижение их применения за счет настройки имеющихся средств защиты.

*Статья получена 07 июня 2019 г.

Ключевые слова: безопасность КИИ, категорирование, объекты КИИ, значимость объектов, ГИС, аттестационные испытания, аттестация системы, программа и методика испытаний

ВВЕДЕНИЕ

1 января 2018 года вступил в силу Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации». Он необходим для регулирования отношений в области гарантирования безопасности объектов информационной инфраструктуры Российской Федерации. ФСТЭК России является органом исполнительной власти в области обеспечения безопасности критической информационной системы (КИИ). Объекты критической информационной инфраструктуры – информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления субъектов критической информационной инфраструктуры. Согласно статье 2 указанного закона, критическая информационная инфраструктура – объекты критической информационной инфраструктуры, а также сети электросвязи, используемые для организации взаимодействия таких объектов. К объектам критической информационной инфраструктуры относятся информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления субъектов критической информационной инфраструктуры, функционирующие в сфере здравоохранения, науки, транспорта, связи, энергетики, в банковской сфере и иных сферах финансового рынка, топливно-энергетического комплекса, в области атомной энергии, оборонной, ракетно-космической, горнодобывающей, металлургической и химической промышленности, а также российские юридические лица и (или) индивидуальные предприниматели, которые обеспечивают взаимодействие указанных систем или сетей.

1. КАТЕГОРИЯ ЗНАЧИМОСТИ

Критерии отнесения ИС к критически важным:

– критерий социальной значимости;

– критерий важности объекта КИИ РФ в части реализации управленческой функции;

– критерий важности объекта КИИ РФ в части предоставления значительного объема информационных услуг.

Под эти критерии легко подвести весь реестр федеральных ГИС.

Применяемые мероприятия по безопасности объектов КИИ определяются в соответствии с его категорией значимости. Для незначимого объекта КИИ

должна быть обеспечена интеграция с ГосСОПКА (государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак). Безопасность значимого объекта КИИ – это комплекс организационных и технических мер, в который входит создание системы безопасности, реагирование на инциденты ИБ, обеспечение действий в нештатных ситуациях, защита технических средств и систем.

Категория значимости определяется исходя из «Правил категорирования объектов критической информационной инфраструктуры Российской Федерации», утвержденных соответствующим Постановлением Правительства от 8 февраля 2018 г. № 127. Существует три категории значимости, где первая – самая высокая, третья – самая низкая. Категорирование проводится для существующих, создаваемых или модернизируемых объектов КИИ.

Категорирование включает:

– определение основных производственных процессов;

– выявление критических объектов;

– определение объектов критической информационной инфраструктуры, которые обрабатывают информацию, необходимую для обеспечения критических процессов, и (или) осуществляют управление, контроль или мониторинг критических процессов;

– формирование перечня объектов КИИ, подлежащих категорированию;

– оценку масштаба возможных последствий в случае возникновения компьютерных инцидентов;

– установку каждому объекту одной из категорий значимости либо решение об отсутствии необходимости присвоения ему категории значимости.

Пересмотр установленной категории значимости происходит не реже, чем один раз в пять лет.

2. ПРОГРАММА ИСПЫТАНИЙ

Цель работы заключается в разработке программы и методики аттестационных испытаний.

Программа и методика испытаний системы (подсистемы) на этапе опытного функционирования предназначена для установления данных, обеспечивающих получение и проверку проектных решений, выявление причин сбоев, определение качества работ и показателей качества функционирования системы (подсистемы), проверку соответствия системы требованиям техники безопасности, продолжительность и режим испытаний.

Программы испытаний должны содержать перечни конкретных проверок (решаемых задач), которые следует осуществлять при испытаниях для подтверждения выполнения требований ТЗ со ссылками на соответствующие методики (разделы методик) испытаний.

Согласно РД 50-34.698-90 «Автоматизированные системы. Требования к содержанию документов», программа испытаний содержит следующие разделы:

– объект испытаний (полное наименование системы, комплектность испытательной системы);

– цель испытаний (конкретные цели и задачи, которые должны быть достигнуты и решены);

– общие положения (перечень руководящих документов; место и продолжительность испытаний; организации, участвующие в испытаниях; перечень ранее проведенных испытаний; перечень предъявляемых на испытания документов);

– объем испытаний (перечень этапов испытаний и проверок; количественные и качественные характеристики, подлежащие оценке; последовательность проведения и режима испытаний; требования по испытаниям программных средств; перечень работ, проводимых после завершения испытаний);

– условия и порядок проведения испытаний (условия проведения испытаний; условия начала и завершения отдельных этапов испытаний; имеющиеся ограничения в условиях проведения испытаний; требования к техническому обслуживанию системы; меры, обеспечивающие безопасность и безаварийность проведения испытаний; порядок взаимодействия организаций; порядок привлечения экспертов для исследования возможных повреждений в процессе проведения испытаний, требования к персоналу);

– материально-техническое обеспечение испытаний (конкретные виды материально-технического обеспечения с распределением задач и обязанностей организации, участвующих в испытаниях);

– метрологическое обеспечение испытаний (перечень мероприятий по метрологическому обеспечению испытаний с распределением задач и ответственности организаций, участвующих в испытаниях, за выполнение соответствующих мероприятий);

– отчетность (указывают перечень отчетных документов, которые должны оформляться в процессе испытаний и по их завершении, с указанием организаций и предприятий, разрабатывающих, согласующих и утверждающих их, и сроки оформления этих документов. К отчетным документам относят акт и отчет о результатах испытаний, акт технического состояния системы после испытаний).

В документ включают приложения.

В зависимости от особенностей систем допускается объединять или исключать отдельные разделы при условии изложения их содержания в других разделах программы испытаний, а также включать в нее дополнительные разделы.

3. АТТЕСТАЦИОННЫЕ ИСПЫТАНИЯ

Обязательная аттестация прописана для государственных информационных систем, являющихся значимыми объектами КИИ.

Аттестация ГИС является обязательным условием для ввода ее в эксплуатацию. Аттестация государственной информационной системы инициализируется заказчиком системы.

При аттестационных испытаниях проводится анализ уязвимостей средств защиты информации, технических средств и программного обеспечения. Если уязвимости обнаружены, то необходимо их устранение или снижение их применения за счет настройки имеющихся средств защиты.

Отчет по анализу уязвимостей оформляется приложением к заключению по результатам аттестационных испытаний.

После проведения аттестационных испытаний разрабатываются протокол и заключение по результатам аттестационных испытаний.

При успешном прохождении аттестационных испытаний выдается аттестат соответствия.

Основополагающим документом является Приказ ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах». Так как объект КИИ одновременно является и государственной информационной системой, то его оценка защищенности проводится по тому же приказу.

Согласно Приказу ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» (п. 17.1), в качестве исходных данных, необходимых для аттестации информационной системы, используются модель угроз безопасности информации, акт классификации информационной системы, техническое задание на создание информационной системы и (или) техническое задание (частное техническое задание) на создание системы защиты информации информационной системы, проектная и эксплуатационная документация на систему защиты информации информационной системы, организационно-распорядительные документы по защите информации, результаты анализа уязвимостей информационной системы, материалы предварительных и приемочных испытаний системы защиты информации информационной системы, а также иные документы, разрабатываемые в соответствии с настоящими требованиями.

Аттестация системы проводится до обработки информации, подлежащей защите в информационной системе, в соответствии с программой и методикой

аттестационных испытаний с применением национальных стандартов, методических документов, разработанных ФСТЭК России.

Согласно приказу, при проведении аттестационных испытаний должны применяться следующие методы проверок (испытаний):

– экспертно-документальный метод, предусматривающий проверку соответствия системы защиты информации информационной системы установленным требованиям по защите информации, на основе оценки эксплуатационной документации, организационно-распорядительных документов по защите информации, а также условий функционирования информационной системы;

– анализ уязвимостей информационной системы, в том числе вызванных неправильной настройкой (конфигурированием) программного обеспечения и средств защиты информации;

– испытания системы защиты информации путем осуществления попыток несанкционированного доступа (воздействия) к информационной системе в обход ее системы защиты информации.

По окончании срока действия аттестата соответствия, который не может превышать 5 лет, или повышения класса защищенности информационной системы проводится повторная аттестация информационной системы. При увеличении состава угроз безопасности информации проводятся дополнительные аттестационные испытания в рамках действующего аттестата соответствия.

Ввод в действие информационной системы осуществляется в соответствии с законодательством Российской Федерации об информации, информационных технологиях и о защите информации, с учетом ГОСТ 34.601 и при наличии аттестата соответствия.

Согласно Приказу ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» (п. 19), обеспечение защиты информации при выводе из эксплуатации аттестованной информационной системы или после принятия решения об окончании обработки информации осуществляется оператором в соответствии с эксплуатационной документацией на систему защиты информации информационной системы и организационно-распорядительными документами по защите информации и включает:

– архивирование информации, содержащейся в информационной системе;

– уничтожение (стирание) данных и остаточной информации с машинных носителей информации и (или) уничтожение машинных носителей информации.

ЗАКЛЮЧЕНИЕ

В статье произведен анализ документов, связанных с программой и методикой для государственной информационной системы. Описана структура согласно РД 50-34.698-90 «Автоматизированные системы требования к содержанию документов» и аттестационные испытания согласно Приказу ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

СПИСОК ЛИТЕРАТУРЫ

1. Федеральный закон от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».

2. Приказ Федеральной службы по техническому и экспортному контролю от 21 декабря 2017 г. № 235 «Об утверждении Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования».

3. 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».

4. Постановление 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».

Иванова Валерия Александровна, 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: 10.17212/2307-6879-2019-2-66-74

Analysis of documents on development of the program and methodology of certification tests of a significant object of critical infrastructure of the RF (GIS)*

V.A. Ivanova[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: Valeria.Ivanova97@yandex.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*

After the entry into force on January 1, 2018 of the Federal Law 187-FZ "On the Security of the Critical Information Infrastructure of the Russian Federation", organizations and specialists working in the field of information security of critical infrastructures faced the implementation of this law and all the many him bylaws.
The program and testing methodology is a document included in the design documentation set up for an automated system or program at the development stage. The test procedure program is designed to establish technical data that is subject to verification during testing of the entire system or its individual components.
The applied measures for the safety of CII facilities are determined in accordance with its category of importance. For not significant object KII should be ensured integration with the GOSPKA. The category of significance is determined on the basis of the “Rules for categorizing objects of the critical information infrastructure of the Russian Federation” approved by the relevant government decree of February 8, 2018 No. 127.
Certification is registered for state information systems, which are significant objects of CII, the basic document is the Order of the FSTEC of Russia dated February 11, 2013 N 17 “On approval of requirements for the protection of information that is not part of the state secret contained in state information systems”. At certification tests, an analysis of vulnerabilities of information protection means, hardware and software is carried out. If vulnerabilities are found, then they must be eliminated or their use reduced by adjusting the available protection.

Keywords: safety of CII, categorization, objects of CII, significance of objects, GIS, certification tests, system certification, program and testing methodology

REFERENCES

1. Federal law of July 26, 2017 N 187-FZ "On the security of the critical information infrastructure of the Russian Federation".

2. Order of the FSTEC Russia of December 21, 2017 N 235 "On approval of requirements for the creation of security systems for significant objects of the critical information infrastructure of the Russian Federation and for their functioning".

* *Received 08 June 2019.*

3. Order of the FSTEC Russia of December 25, 2017 N 239 "On approval of the Security Requirements for the Important Objects of Critical Information Infrastructure of the Russian Federation".

4. Decree of the Government of the Russian Federation dated February 8, 2018 N 127 "On the approval of the Rules for categorizing objects of the critical information infrastructure of the Russian Federation, as well as a list of indicators of criteria for the significance of objects of critical information infrastructure of the Russian Federation and their values".

Для цитирования:

Иванова В.А., Селифанов В.В. Анализ документов по разработке программы и методик аттестационных испытаний значимого объекта критической инфраструктуры РФ (ГИС) // Сборник научных трудов НГТУ. – 2019. – № 2 (95). – С. 66–74. – DOI: 10.17212/2307-6879-2019-2-66-74.

For citation:

Ivanova V.A., Selifanov V.V. Analiz dokumentov po razrabotke programmy i metodik ispytanii znachimogo ob"ekta kriticheskoi infrastruktury RF GIS [Analysis of documents on development of the program and methodology of certification tests of a significant object of critical infrastructure of the RF GIS]. *Sbornik nauchnykh trudov Novosibirskogo gosudarstvennogo tekhnicheskogo universiteta – Transaction of scientific papers of the Novosibirsk state technical university*, 2019, no. 2 (95), pp. 66–74. DOI: 10.17212/2307-6879-2019-2-66-74.