ОСОБЕННОСТИ ЛИЦЕНЗИРОВАНИЯ ДЕЯТЕЛЬНОСТИ ПРЕДПРИЯТИЙ И ОРГАНИЗАЦИЙ В ИНТЕРЕСАХ МИНИСТЕРСТВА ОБОРОНЫ РОССИЙСКОЙ ФЕДЕРАЦИИ

Иванов А.Е.[1], Спрогис И.А.[2], Шахалов И.Ю.[3]

Цель статьи: *улучшение существующей процедуры оценки соответствия организаций, предприятий промышленности и учреждений – разработчиков программного обеспечения и программно-аппаратных комплексов, применяемых в образцах вооружения и военной техники.*

Методы исследования: *системный анализ, разработка методик.*

Результат: *разработаны проекты методик проведения проверки архива при проведении специальных экспертиз предприятий и организаций – соискателей лицензии Минобороны России на деятельность по созданию средств защиты информации и проведения проверки соответствия процессов разработки программного обеспечения требованиям ГОСТ Р 56939-2016 при проведении специальной экспертизы лицензиатов Минобороны России в области создания средств защиты информации.*

Ключевые слова: *оценка соответствия, информационная безопасность, защита информации, сертификация, сертификационные испытания, специальные экспертизы, средства защиты информации, система лицензирования, разработка безопасного программного обеспечения, архивное хранение.*

DOI:10.21681/2311-3456-2021-5-63-74

Введение

Одной из составных частей Системы сертификации СЗИ Министерства обороны Российской Федерации является лицензирование деятельности в области создания средств защиты информации, то есть, по сути, оценка соответствия организаций, предприятий промышленности и учреждений установленным регулятором (Минобороны России) лицензионным требованиям.

Стоит отметить, что эта Лицензия, которая носит название «На проведение работ, связанных с созданием средств защиты информации» (далее – Лицензия на ССЗИ) является единственным официальным документом, который разрешает осуществление работ по проектированию, разработке, производству, реализации, установке, монтажу, наладке, испытаниям, ремонту и сервисному обслуживанию программных и программно-технических средств и программно-аппаратных комплексов, разрабатываемых и производимых в интересах Минобороны России (в соответствии с Положением, утвержденным приказом Министра обороны Российской Федерации 1998 года № 54) [1].

Вопросы лицензирования в Министерстве обороны Российской Федерации переданы в ведение Восьмого управления Генерального штаба Вооруженных Сил Российской Федерации.

История лицензирования

Само понятие «лицензирование», которое подразумевает наличие разрешительной политики государства относительно тех или иных видов деятельности предпринимателей, было введено в обиход отечественной науки предпринимательского права и административно-правовой науки в целом не столь давно.

В царской России не было понятия о лицензировании. Государственный контроль над предпринимателями не использовал таких методов. Единственный раз, когда подобная практика применялась в деятельности исполнительно-распорядительных органов в России периода правления Романовых, пришелся на период так называемой «континентальной блокады» (1811-12 гг.), когда из-за конфликта Франции и Англии европейские страны ограничили торговлю с последней, фактически объявив ей бойкот. В России тогда предпринимателям выдавались особые «льготные письма», которые, по сути, представляли собой лицензии для торговли с Англией.

В Советском Союзе проблема лицензирования не стояла по простой причине – отсутствия частного предпринимательства как такового. Государственные предприятия же в лицензировании не нуждались – зачем государству лицензировать самое себя?

Если же рассматривать постперестроечный период истории Российского государства, то в тот момент понятие «лицензирование отдельных видов деятельности» вновь появилось в новом российском праве. Оно возникло в законодательной практике 2 декабря 1990 г. в отношении банковской сферы, когда вступили в действие вновь принятые Законы РСФСР «О банках и банковской деятельности» и «О Центральном банке РСФСР (Банке России)». 25 декабря 1990 г. появилось более

1 Иванов Андрей Евграфович, сотрудник Восьмого управления ГШ ВС РФ, Москва, Россия. E-mail: is@cnpo.ru

2 Спрогис Иван Александрович, сотрудник Восьмого управления ГШ ВС РФ, Москва, Россия. E-mail: bai@cnpo.ru

3 Шахалов Игорь Юрьевич, доцент кафедры «Информационная безопасность» МГТУ им. Баумана, Москва, Россия. E-mail: i.shahalov@bmstu.ru

общее понятие о лицензировании предпринимательской деятельности, когда, согласно 4 пункту ст. 21 Закона РСФСР «О предприятиях и предпринимательской деятельности» начала действовать норма, предусматривающая такое лицензирование. Эта норма устанавливала, что отдельные виды деятельности предпринимателей в Российской Федерации могут осуществляться лишь на основании лицензии (специального разрешения компетентных органов). Предполагалось, что перечень видов предпринимательской деятельности, подлежащих лицензированию, будет определяться Правительством Российской Федерации [2-10].

Анализ существующего порядка лицензирования

В области защиты государственной тайны в те же годы было принято и действует по настоящее время Постановление Правительства Российской Федерации от 15 апреля 1995 года N 333 «О лицензировании деятельности предприятий, учреждений и организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны», которым было утверждено Положение с аналогичным (самому 333 ПП РФ) названием [11-13].

В самом начале Положения, в статье 1, определены направления лицензионной деятельности.

Это деятельность по проведению работ, связанных с:

- использованием сведений, составляющих государственную тайну;
- созданием средств защиты информации;
- осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны.

Как уже было сказано выше, мы в данной статье рассмотрим особенности лицензирования деятельности по проведению работ, связанных с созданием средств защиты информации (ССЗИ) Минобороны России [1].

Общий алгоритм процедуры получения лицензии ССЗКИ указан на Рис.1.

При проведении специальной экспертизы экспертная комиссия проводит оценку соответствия лицензиата или соискателя лицензии (Заявителя) лицензионным требованиям.

При этом проверяются основные вопросы: признаки отдельного российского юридического лица, место нахождения и место осуществления лицензируемого вида деятельности, адреса для открытой и закрытой переписки, основные виды деятельности, полученные лицензии и аттестаты аккредитации, основную продукцию, участие в НИОКР, наличие необходимых нормативно-правовых актов, нормативно-методических и нормативно-технических документов, порядок их актуализации, систему менеджмента качества, наличие необходимых технологических условий, включающих соответствующую базу вычислительных средств и производственного оборудования, с помощью которых осуществляется основная производственная деятельность, наличие объектов недвижимости для осуществления заявленной деятельности, достаточность и законность используемого программного обеспечения, состав и подготовленность сотрудников, принимающих участие в заявленной деятельности [10, 13-15].

Предложения по оценке деятельности архива заявителя

Особое внимание при проведении специальной экспертизы, 8 Управление ГШ ВС РФ обращает на организацию архивного хранения рабочей конструкторской, программной документации на бумажных носителях и программных изделий в электронном виде на машинных носителях информации. Это относится, в первую очередь, к программным и программно-аппаратным изделиям, сертифицированным в Системе сертификации Минобороны России, что обусловлено важностью задачи государственного уровня - гарантированным обеспечением эксплуатантов образцов вооружения и военной техники программными и программно-аппаратными изделиями, прошедшими оценку соответствия установленным порядком.

Рис.1. Алгоритм процедуры получения лицензии ССЗКИ

Организация и деятельность архива регулируются следующими нормативно-техническими и нормативно-методическими документами:

- ГОСТ 2.501-13 ЕСКД. Правила учета и хранения;
- ГОСТ 2.502-13 ЕСКД. Правила дублирования;
- ГОСТ 2.503-13 ЕСКД. Правила внесения изменений;
- ГОСТ 19.601-78 ЕСПД. Общие правила дублирования, учета и хранения;
- ГОСТ 19.602-78 ЕСПД. Правила дублирования, учета и хранения программных документов, выполненных печатным способом;
- ГОСТ 19.603-78 ЕСПД. Общие правила внесения изменений;
- ГОСТ 19.604-78 ЕСПД. Правила внесения изменений в программные документы, выполненные печатным способом;
- ГОСТ 28388-89 Системы обработки информации. Документы на магнитных носителях данных. Порядок выполнения и обращения;
- ГОСТ Р 7.02-2006 Консервация документов на компакт-дисках. Общие требования;
- Примерное положения об архиве организации, утвержденное Приказом Росархива от 11 апреля 2018 г. N 42.

В связи с важностью задачи, авторами был разработан проект документа «Методика проведения проверки архива при проведении специальных экспертиз предприятий и организаций – соискателей лицензии Минобороны России на деятельность по созданию средств защиты информации» (Приложение 1).

В Методике определен

- порядок и объем проведения проверок [16, 17]:
- основных функций архива;
- установленного порядка сдачи материалов на хранение в архив;
- порядка сдачи материалов на хранение в архив;
- порядка контроля целостности материалов, находящихся на архивном хранении;
- правильности оборудования помещения архива и режима хранения материалов.

Применение «Методики проведения проверки архива...» позволяет унифицировать требования к Заявителям, упростить процедуру проведения специальной экспертизы и разработать критерии оценки соответствия архива Организации требованиям Минобороны России.

Оценка соответствия требованиям ГОСТ Р 56939-2016

Необходимо отметить, что система лицензирования Министерства обороны Российской Федерации постоянно развивается, лицензионные требования корректируются в соответствии с изменениями правовой и нормативной базы в области информационной безопасности.

В связи с ростом сложности информационных систем все более актуальными становятся угрозы безопасности информации, связанные с наличием уязвимостей программ (уязвимостей кода), используемых в составе информационных систем. Для защиты от такого рода угроз, как правило, используется комплекс мер, реализуемый в процессах функционирования (эксплуатации) и сопровождения программного обеспечения. В то же время, для обеспечения необходимого уровня защиты информации требуется реализация мер, направленных на предотвращение появления и устранение уязвимостей программ в процессах жизненного цикла программного обеспечения, связанных с проектированием, реализацией и тестированием.

Поэтому, в 2016 году был утвержден и введен в действие ГОСТ Р 56939-2016 «Защита информации. Разработка безопасного программного обеспечения. Общие требования», инициированный и разработанный НПО «Эшелон» [20] в рамках работы Технического комитета ТК-362 «Защита информации».

Этот стандарт направлен на достижение целей, связанных с предотвращением появления и/или устранением уязвимостей программ, и содержит перечень мер, которые рекомендуется реализовывать на соответствующих этапах жизненного цикла программного обеспечения, а также устанавливает общие требования к содержанию и порядку выполнения работ, связанных с созданием безопасного (защищенного) программного обеспечения и формированием (поддержанием) среды обеспечения оперативного устранения выявленных пользователями ошибок программного обеспечения и уязвимостей программы и предназначен для разработчиков и производителей программного обеспечения, а также для организаций, выполняющих оценку соответствия процесса разработки программного обеспечения требованиям настоящего стандарта [18-20].

Учитывая важность и актуальность проведения оценки соответствия организаций – разработчиков программного обеспечения требованиям ГОСТ Р 56939-2016, авторы разработали проект документа «Методика проведения проверки соответствия процессов разработки программного обеспечения требованиям ГОСТ Р 56939-2016 при проведении специальной экспертизы лицензиатов Минобороны России в области создания средств защиты информации» (Приложение 2).

В Методике определены:

- порядок и объем проведения проверок;
- наличия и содержания требований по безопасности, предъявляемых к разрабатываемому программному обеспечению;
- наличия и содержания документации по моделированию угроз безопасности информации;
- использования при разработке ПО идентифицированных инструментальных средств;
- организации обеспечения защиты ПО от угроз безопасности информации, связанных с нарушением целостности, в процессе его передачи пользователю;
- организации обеспечения поставок пользователю эксплуатационных документов [21];
- организации использования системы управления конфигурацией ПО;
- организации защиты от несанкционированного доступа к элементам конфигурации ПО;
- организации резервного копирования элементов конфигурации ПО;

- организации регистрации событий, связанных с фактами изменения элементов конфигурации ПО;
- организации периодического обучения сотрудников [23].

Применение «Методики...» при проведении специальных экспертиз позволит оценить возможности Заявителя по созданию программного обеспечения без встроенных дефектов и недекларированных возможностей.

После внедрения «Методики...» в процесс проведения специальных экспертиз, предлагается использовать ее и при проверке производства в ходе проведения сертификационных испытаний.

Выводы

Система лицензирования деятельности в области создания средств защиты информации выполняет важную и ответственную задачу по оценке соответствия организаций, разработчиков отечественного программного обеспечения для образцов вооружения и военной техники.

Внедрение предложенных авторами методик позволит существенно улучшить процедуру проведения специальных экспертиз.

Литература

1. Трофимов В.В. Как стать разработчиком средств защиты информации для Министерства обороны Российской Федерации // Information Security, 2005, № 3. С. 27-28.
2. Альтерман А.Д., Лушников Н.Д. Информационная безопасность через лицензирование и сертификацию // Аллея науки. 2018. Т. 3. №6 (22). С. 897-900.
3. Борисова Е.А., Попов К.Г. Лицензирование как метод обеспечения информационной безопасности // Символ науки: международный научный журнал. 2016. № 7-2 (19). С. 36-38.
4. Долгов Д.С. Лицензирование как административно-правовое средство обеспечения информационной безопасности в российской федерации // Вестник Саратовской государственной академии права. 2008. № 4 (62). С. 196-197.
5. Жогаль А.В. Современные проблемы обеспечения информационной безопасности в России // Контекст и рефлексия: философия о мире и человеке. 2017. № 1А, Том 6. - С. 178-185.
6. Катаржнов А.Д. Лицензирование деятельности по технической защите конфиденциальной информации // Защита информации. Инсайд. 2012. № 2 (44). С. 16-20.
7. Нагорный С. И., Клиомфас Ю. В. Искушение законом // Защита информации. Инсайд. 2011. № 3. С. 26-29.
8. Скрипник Д.А. Общие вопросы технической защиты информации. М.: Национальный Открытый Университет «ИНТУИТ», 2016. 425 с.
9. Шапошников В.И. Некоторые проблемы правового регулирования отношений по лицензированию в области защиты информации // Актуальные проблемы российского права. 2007. № 2. С. 77-81.
10. Шахалов И.Ю. Лицензия как продукт осознанной необходимости лицензирование деятельности операторов персональных данных // Защита информации. Инсайд. 2010. № 2 (32). С. 53-55.
11. Законодательно-правовое и организационно-техническое обеспечение ... автоматизированных систем и информационно-вычислительных сетей / Котенко И.В., Котухов М.М., Марков А.С. и др. - СПб: ВУС, 2000. 190 с.
12. Марков А.С. Техническая защита информации. Курс лекций. М. АИСНТ. 2020. 234 с.
13. Шахалов И.Ю. Лицензирование деятельности по технической защите конфиденциальной информации // Вопросы кибербезопасности. 2013. № 1 (1). С. 49-54.
14. Шахалов И.Ю. Правовое обоснование сертификации средств защиты информации // Мониторинг правоприменения. 2015. № 3 (16). С. 64-68.
15. Марков А.С., Цирлов В.Л., Барабанов А.В. Методы оценки несоответствия средств защиты информации. М.: Радио и связь. 2012. 192 с.
16. Максимов Е.Е., Бурс К.В., Жереб Л.А. Актуальность и проблемы электронных архивов современных российских предприятий // Актуальные проблемы авиации и космонавтики. 2012. Т. 2. № 8. С. 184-185.
17. Саманцов А. П. Цифровые архивы предприятий: проблемы хранения данных // Вестник Юридического института МИИТ. 2021. № 2 (34). С. 143-148.
18. Гришин М.И., Марков А.С., Цирлов В.Л. Практические аспекты реализации мер по разработке безопасного программного обеспечения // ИТ-Стандарт. 2019. № 2 (19). С. 29-39.
19. Девянин П.Н., Мылицын Р.Н., Тележников В.Ю. Технологии безопасной разработки и обеспечения доверия к ОССН Astra Linux Special Edition. В сборнике: Состояние и перспективы развития современной науки по направлению «Информационная безопасность». Сборник статей III Всероссийской научно-технической конференции. Анапа, 2021. С. 13-23.
20. Barabanov A., Markov A., Fadin A., Tsirlov V., Shakhalov I. Synthesis of Secure Software Development Controls. In Proceedings of the 8th International Conference on Security of Information and Networks (Sochi, Russian Federation, September 08-10, 2015). SIN '15. ACM New York, NY, USA, 2015, pp. 93-97. DOI: 10.1145/2799979.2799998
21. Барабанов А.В. Марков А.С., Цирлов В.Л. О систематике информационной безопасности цепей поставки программного обеспечения. // Безопасность информационных технологий. 2019. Т. 26. № 3. С. 68-79.
22. Барабанов А.В., Марков А.С., Цирлов В.Л. Оценка соответствия средств защиты информации «Общим критериям» // Информационные технологии. 2015. Т. 21. № 4. С. 264-270.
23. Dorofeev A.V., Markov A.S., Rautkin Y.V. Ethical Hacking Training // CEUR Workshop Proceedings, 2019, Vol-2522, pp. 47-56.

Приложение 1

МЕТОДИКА

проведения проверки архива при проведении специальных экспертиз предприятий и организаций – соискателей лицензии Минобороны России на деятельность по созданию средств защиты информации (ПРОЕКТ)

Общие положения

Методика одержит общие требования по проверке организации и функционирования архива предприятия (учреждения, организации, лицензиата) – соискателя лицензии Минобороны России на деятельность по созданию средств защиты информации (далее – Лицензиата) по обеспечению сохранности, учета, отбора, упорядочения и использования документов, образовавшихся в процессе лицензируемой деятельности Лицензиата.

Настоящая Методика разработана с учетом требований следующих нормативно-технических и нормативно-методических документов:

ГОСТ 2.501-13 ЕСКД. Правила учета и хранения;

ГОСТ 2.502-13 ЕСКД. Правила дублирования;

ГОСТ 2.503-13 ЕСКД. Правила внесения изменений;

ГОСТ 19.601-78 ЕСПД. Общие правила дублирования, учета и хранения;

ГОСТ 19.602-78 ЕСПД. Правила дублирования, учета и хранения программных документов, выполненных печатным способом;

ГОСТ 19.603-78 ЕСПД. Общие правила внесения изменений;

ГОСТ 19.604-78 ЕСПД. Правила внесения изменений в программные документы, выполненные печатным способом;

ГОСТ 28388-89 Системы обработки информации. Документы на магнитных носителях данных. Порядок выполнения и обращения;

ГОСТ Р 7.02-2006 Консервация документов на компакт-дисках. Общие требования;

Примерное положения об архиве организации, утвержденное Приказом Росархива от 11 апреля 2018 г. N 42.

Проверка основных функций архива

1. Наличие структурного подразделения, на которое возложены функции по обеспечению сохранности, учета, отбора, упорядочения и использования документов (не содержащих сведений, составляющих государственную тайну), либо лица, ответственного за организацию архивного хранения.

При этом подлежат проверке указанные ниже документы (или аналогичные документы):

1.1. Приказ об организации архивного хранения;

1.2. Положение о подразделении, в котором организовано архивное хранение;

1.3. Инструкция по организации архивного хранения,

или их аналоги.

2. Порядок приема, регистрации, учета, систематизации технической документации в соответствии с установленными требованиями:

2.1. Учет и хранение подлинников, дубликатов, тиражирование и выдачу сотрудникам организации дубликатов материалов, находящихся в архиве.

2.2. Раздельное хранение подлинников и дубликатов.

2.3. Оформление учетных документов (журналов регистрации документов, находящихся на архивном хранении; карточек учета и т.п.).

2.4. Выдача в установленном порядке копий документов, необходимых для практической работы структурных подразделений лицензиата.

2.5. Инструктирование сотрудников лицензиата о порядке формирования, подготовки и сдачи документов (в печатном и электронном виде) в архив.

2.6. Проведение контроля целостности машинных носителей информации, находящихся на архивном хранении один раз в год сертифицированными средствами контроля целостности.

2.7. Составление установленной отчетности.

Проверка установленного порядка сдачи материалов на хранение в архив

Проверка определения номенклатуры передаваемых на хранение в архив следующих документов и материалов по лицензируемым видам деятельности:

DOI:10.21681/2311-3456-2021-5-63-74

подлинники машинных носителей информации, содержащих рабочую конструкторскую и программную документацию на разработанные изделия;

дубликаты машинных носителей информации, содержащих рабочую конструкторскую и программную документацию на разработанные изделия;

подлинники носителей, содержащих исходные тексты программных изделий, разработанных лицензиатом;

дубликаты машинных носителей информации, содержащих исходные тексты программных изделий, разработанных лицензиатом;

подлинники машинных носителей информации, содержащих дистрибутивы программных изделий, разработанных лицензиатом;

дубликаты машинных носителей информации, содержащих дистрибутивы программных изделий, разработанных лицензиатом;

бумажные версии рабочей конструкторской и программной документации на разработанные изделия.

Хранение подлинников и дубликатов должно осуществляться раздельно.

Проверка порядка сдачи материалов на хранение в архив

Внесение соответствующих записей в журнал учета документов архива, находящихся в архиве.

Наличие маркировки контейнера (для компакт-диска должна быть разработана и утверждена этикетка).

Соответствие контрольной суммы, указанной на этикетке машинного носителя информации, и контрольной суммы содержимого компакт-диска. Подсчет контрольных сумм должен осуществляться сертифицированным средством контроля целостности.

Присвоение инвентарного номера.

Проверка порядка контроля целостности материалов, находящихся на архивном хранении

Наличие ответственного сотрудника за проведение контроля целостности.

Периодичность (не менее одного раза в год) проведения контроля целостности информации, записанной на компакт-дисках, находящихся на архивном хранении, сертифицированными средствами подсчета контрольных сумм.

Регистрация результатов проведенного контроля целостности в соответствующем журнале под подпись ответственного лица.

Проверка правильности оборудования помещения архива и режима хранения материалов

Для обеспечения сохранности, создания необходимых условий для работы архиву должно быть отведено специально оборудованное помещение.

Архив должен размещаться в зданиях или отдельных помещениях здания, недоступных для посторонних лиц, сухих, безопасных в пожарном отношении.

Хранилище архива должно закрываться на замок повышенной надежности.

В хранилищах запрещается применение огня, использование нагревательных приборов, размещение посторонних объектов.

В помещении архива в качестве искусственного разрешено только электрическое освещение.

Рабочие комнаты архива могут быть обеспечены, кроме электрического освещения, естественным освещением и отделены от хранилища.

Должно быть запрещено использование не приспособленных подвальных помещений для хранения архивных материалов.

Помещение архива должно быть оборудовано пожарной и охранной сигнализацией, иметь выходы к лифтам и лестничным клеткам в случае эвакуации.

Работники архива должны пройти инструктаж по вопросам противопожарной безопасности, ознакомиться с правилами пользования противопожарным инвентарем.

Электропроводка должна быть скрытой или вмонтированной в пластиковый короб.

В помещении архива должно быть категорически запрещено курение.

В помещении архива должны соблюдаться температурно-влажностные, санитарно-гигиенические, световые условия, обеспечивающие длительную сохранность материалов и нормальные условия для работы с ними.

В хранилище должны приниматься меры, исключающие возможность появления плесени, насекомых, грызунов и накопления пыли, периодически проводиться санитарные дни для уборки пыли со стеллажей, коробок, связок и влажной уборки помещений.

Приложение 2

МЕТОДИКА
проведения проверки соответствия процессов разработки программного обеспечения требованиям ГОСТ Р 56939-2016 при проведении специальной экспертизы лицензиатов Минобороны России в области создания средств защиты информации (ПРОЕКТ)

1. Проверка наличия и содержания требований по безопасности, предъявляемых к разрабатываемому программному обеспечению (п. 5.1.3.1 ГОСТ Р 56939-2016)

1.1. Проверка наличия документов, содержащих требования по безопасности, предъявляемые к разрабатываемому программному обеспечению (ПО).

1.2. Проверка наличия в документации разработчика ПО перечня определенных требований по безопасности, предъявляемых к безопасному ПО.

1.3. Проверка реализации на практике мер по безопасной разработке в процессе разработки и производства ПО.

Примечание — В качестве источников для формирования требований разработчик ПО может использовать требования законов, нормативных правовых актов, отраслевых стандартов, перечень требований пользователя, сценарии применения ПО.

Например, могут быть определены следующие требования к ПО:

- к обеспечению идентификации и аутентификации;
- обеспечению защиты от несанкционированного доступа к информации;
- обеспечению регистрации событий;
- контролю точности, полноты и правильности данных, поступающих в программу;
- обработке программных ошибок и исключительных ситуаций.

Требования по безопасности, предъявляемые к разрабатываемому ПО, могут быть отражены в техническом задании, разрабатываемом по ГОСТ 19.201. При наличии в программе функциональных возможностей, обеспечивающих реализацию мер защиты информации, документ, содержащий требования по безопасности, предъявляемые к разрабатываемому ПО. следует разрабатывать в соответствии с требованиями класса ASE «Оценка задания по безопасности» по ГОСТ Р ИСО/МЭК 15408-3 [20].

2. Проверка наличия и содержания документации по моделированию угроз безопасности информации (п. 5.2.3.1 ГОСТ Р 56939-2016)

1.4. Проверка наличия документации, содержащей описание моделирования угроз безопасности, проводимого при разработке и производстве ПО.

1.5. Проверка наличия в указанной документации:

- описания используемой методологии моделирования угроз безопасности информации;
- списка выявленных потенциальных угроз безопасности информации;
- описания проектных решений и/или указаний по применению разрабатываемого ПО, направленных на нейтрализацию выявленных потенциальных угроз безопасности информации.

1.6. Проверка реализации на практике мер по безопасной разработке ПО, касающихся моделирования угроз безопасности информации.

Примечание — Входными данными для процесса моделирования угроз безопасности информации являются в первую очередь сведения о проекте архитектуры программы (предполагаемых компонентах программы, их интерфейсах и концепции их совместного выполнения), в том числе информация о заимствованных у сторонних разработчиков ПО компонентах и информация из открытых источников (например, из банка данных угроз безопасности информации Федеральной службы по техническому и экспортному контролю (ФСТЭК России)), связанная с типовыми сценариями компьютерных атак и угрозами безопасности информации.

Моделирование угроз безопасности информации выполняют с целью выявления потенциальных угроз безопасности информации, которые могут возникнуть вследствие применения ПО. связанных с ее проектными (архитектурными) особенностями на ранней стадии разработки (до начала выполнения процессов конструирования и комплексирования ПО) и уточнения проекта архитектуры программы без доработки исходного кода программы.

3. Проверка использования при разработке ПО идентифицированных инструментальных средств (п. 5.3.3.1 ГОСТ Р 56939-2016)

3.1. Проверка наличия документации, содержащей информацию об идентификации инструментальных средств, используемых при разработке и производстве ПО.

3.2. Проверка наличия в указанной документации следующих сведений:

- - наименование и идентификационные признаки инструментальных средств;
- - наименование разработчиков инструментальных средств;
- - ссылку на эксплуатационные документы инструментальных средств;
- - значения применяемых при создании программы опций (настроек) инструментальных средств.

3.3. Проверка реализации на практике мер по безопасной разработке ПО, касающихся идентификации инструментальных средств.

Примечание — к инструментальным средствам относятся, например, трансляторы, компиляторы, прикладные программы, используемые для проектирования и документирования, редакторы исходного кода программ, отладчики, интегрированные среды разработки.

2. Проверка организации обеспечения защиты ПО от угроз безопасности информации, связанных с нарушением целостности, в процессе его передачи пользователю (п. 5.5.3.1 ГОСТ Р 56939-2016)

4.1. Проверка наличия документации, содержащей сведения о мерах для обеспечения защиты ПО от угроз безопасности информации, связанных с нарушением целостности в процессе его передачи пользователю.

4.2. Проверка наличия в указанной документации следующих сведений:

- технические меры по выявлению модификации ПО и любого расхождения между эталонной версией ПО, и версией ПО, полученной пользователем;
- организационные меры, направленные на выявление модификации ПО и любого расхождения между эталонной версией ПО, и версией ПО, полученной пользователем.

4.3. Проверка реализации на практике мер по безопасной разработке ПО, касающихся обеспечения защиты ПО от угроз безопасности информации, связанных с нарушением целостности в процессе его передачи пользователю.

Примечание — для реализации данной меры могут быть использованы, например, средства контрольного суммирования поставляемого дистрибутива программы, пломбирование упаковки с поставляемым дистрибутивом программы и документацией наклейкой, разрываемой при первом вскрытии упаковки.

Описание процедуры передачи ПО пользователю следует разрабатывать в соответствии с требованиями семейства ALC_DEL «Поставка» по ГОСТ Р ИСО/МЭК 15408-3 [20].

5. Проверка организации обеспечения поставок пользователю эксплуатационных документов (п. 5.5.3.2 ГОСТ Р 56939-2016)

5.1. Проверка наличия документации, содержащей сведения о комплекте эксплуатационных документов, поставляемых пользователю ПО.

5.2. Проверка наличия в указанной документации:

- комплект поставки ПО;
- состав поставляемой эксплуатационной документации ПО;
- информация, достаточная для правильной настройки и безопасного применения ПО.

5.3. Проверка реализации на практике мер по безопасной разработке ПО, касающихся поставок пользователю эксплуатационных документов.

Примечание — в эксплуатационных документах следует определить перечень и эталонные значения конфигурационных параметров программы.

Данную информацию можно использовать для выявления уязвимостей программы, появившихся в результате определения конфигурации (параметров настройки) программы. Виды разрабатываемых эксплуатационных документов могут соответствовать ГОСТ 19.101. При наличии в программе функциональных возможностей, обеспечивающих реализацию мер защиты информации, эксплуатационные документы следует разрабатывать в соответствии с требованиями семейств AGD_OPE «Руководство пользователя по эксплуатации» и AGD_PRE «Подготовительные процедуры по ГОСТ Р ИСО/МЭК 15408-3 [20].*

6. Проверка организации использования системы управления конфигурацией программного обеспечения (п. 5.7.3.2 ГОСТ Р 56939-2016)

6.1. Проверка наличия документации, содержащей сведения о системе управления конфигурацией ПО, применяемой в процессе разработки и производства.

6.2. Проверка наличия в указанной документации следующих сведений:

- перечень элементов конфигурации, которые должны контролироваться системой управления конфигурацией ПО;
- описание методов, используемых для уникальной идентификации элементов конфигурации;
- порядок использования системы управления конфигурацией ПО;

- подтверждения использования системы управления конфигурацией ПО;
- перечень элементов конфигурации, связанных с реализацией функции безопасности ПО;
- порядок использования системы управления конфигурацией ПО с целью определения всех элементов конфигурации, на которые воздействует модификация данного элемента конфигурации.

6.3. Проверка системы управления конфигурацией ПО, которая должна обеспечивать:
- определение элементов конфигурации ПО, имеющие отношения к разрабатываемому ПО;
- уникальную идентификацию определенных элементов конфигурации;
- идентифицирование элементов конфигурации, которые связаны с реализацией функций безопасности ПО;
- определение всех элементов конфигурации, на которые воздействует модификация данного элемента конфигурации.

6.4. Проверка реализации на практике мер по безопасной разработке ПО, касающихся использования системы управления конфигурацией ПО, применяемой в процессе разработки и производства.

Примечание — в область действия системы управления конфигурацией ПО могут быть включены следующие элементы конфигурации:
- программа (дистрибутив программы);
- программные и эксплуатационные документы;
- исходный код программы;
- программные и загрузочные модули, в том числе модули сторонних разработчиков ПО;
- инструментальные средства и связанная с ними информация;
- информация, связанная с обновлениями ПО и устранениями уязвимостей программы;
- перечень выявленных уязвимостей программы.

7. Проверка организации защиты от несанкционированного доступа к элементам конфигурации ПО (п. 5.8.3.1 ГОСТ Р 56939-2016)

7.1. Проверка наличия документации, содержащей сведения о защищаемых элементах конфигурации ПО, а также описание применяемых технических и организационных мер, обеспечивающих их защиту от несанкционированного доступа.

7.2. Проверка наличия в указанной документации следующих сведений:
- перечень элементов конфигурации, которые должны быть защищены от угроз безопасности информации, связанных с нарушением конфиденциальности, целостности и доступности;
- описание применяемых технических и организационных мер, обеспечивающих защиту от несанкционированного доступа к элементам конфигурации.

7.3. Проверка реализации на практике мер по безопасной разработке ПО, касающихся технических и организационных процедур, обеспечивающих защиту элементов конфигурации ОО от несанкционированного доступа.

Примечание — Используемые меры направлены на обеспечение конфиденциальности и целостности следующих объектов среды разработки ПО и элементов конфигурации:
- *программа (дистрибутив программы);*
- *программные и эксплуатационные документы;*
- *исходный код программы;*
- *программные и загрузочные модули, в том числе модули сторонних разработчиков ПО;*
- *инструментальные средства и связанная с ними информация;*
- *информация, связанная с обновлениями ПО и устранениями уязвимостей программы;*
- *перечень выявленных уязвимостей программы.*

8. Проверка организации резервного копирования элементов конфигурации программного обеспечения (п. 5.8.3.2 ГОСТ Р 56939-2016)

8.1. Проверка наличия документации, содержащей сведения о резервном копировании элементов конфигурации ПО, применяемом в процессе разработки и производства.

8.2. Проверка наличия в указанной документации следующих сведений:
- перечень элементов конфигурации, подлежащих резервному копированию;
- сведения о периодичности резервного копирования;
- описание применяемых технических и организационных мер, обеспечивающих резервное копирование и восстановление определенных элементов конфигурации.

8.3. Проверка реализации на практике мер по безопасной разработке ПО, касающихся резервного копирования элементов конфигурации ПО, применяемого в процессе разработки и производства.

Примечание — Используемые меры направлены на обеспечение конфиденциальности и целостности следующих объектов среды разработки ПО и элементов конфигурации:
- *программа (дистрибутив программы);*
- *программные и эксплуатационные документы;*
- *исходный код программы;*
- *программные и загрузочные модули, в том числе модули сторонних разработчиков ПО;*
- *инструментальные средства и связанная с ними информация;*
- *информация, связанная с обновлениями ПО и устранениями уязвимостей программы;*
- *перечень выявленных уязвимостей программы.*

9. Проверка организации регистрации событий, связанных с фактами изменения элементов конфигурации ПО (п. 5.8.3.3 ГОСТ Р 56939-2016)

9.1. Проверка наличия документации, содержащей сведения о регистрации событий, связанных с фактами изменения элементов конфигурации ПО.

9.2. Проверка наличия в указанной документации следующих сведений:
- описание применяемых технических и организационных мер, обеспечивающих регистрацию всех событий, связанных с фактами изменения элементов конфигурации, в журнале регистрации событий.

9.3. Проверка реализации на практике мер по безопасной разработке ПО, касающихся регистрации событий, связанных с фактами изменения элементов конфигурации ПО.

Примечание — Используемые меры направлены на обеспечение конфиденциальности и целостности следующих объектов среды разработки ПО и элементов конфигурации:
- *программа (дистрибутив программы);*
- *программные и эксплуатационные документы;*
- *исходный код программы;*
- *программные и загрузочные модули, в том числе модули сторонних разработчиков ПО;*
- *инструментальные средства и связанная с ними информация;*
- *информация, связанная с обновлениями ПО и устранениями уязвимостей программы;*
- *перечень выявленных уязвимостей программы.*

10. Проверка организации периодического обучения сотрудников (п. 5.9.3.1 ГОСТ Р 56939-2016)

10.1. Проверка наличия документации, содержащей сведения о периодическом обучении сотрудников, участвующих в разработке и производстве ПО.

10.2. Проверка наличия в указанной документации следующих сведений:
- правила и программы обучения;
- сведения о периодичности обучения;
- сведения о прохождении сотрудниками обучения.

10.3. Проверка реализации на практике мер по безопасной разработке ПО, касающихся периодического обучения сотрудников, участвующих в разработке и производстве ПО.

Результаты проведения проверки соответствия процессов разработки программного обеспечения требованиям ГОСТ Р 56939-2016 отражаются в Акте специальной экспертизы отдельным пунктом.

FEATURES OF LICENSING THE ACTIVITIES OF ENTERPRISES AND ORGANIZATIONS IN THE INTERESTS OF THE MINISTRIES OF DEFENSE OF THE RUSSIAN FEDERATION

Ivanov A.E.[4], Sprogis I.A. [5], Shahalov I.Yu.[6]

The purpose of the article: *the best of the existing procedure for assessing the conformity of organizations, industrial enterprises and institutions - developers of software and hardware complexes used in weapons and military equipment.*

Research methods: *system analysis, development of methods.*

Result: *draft methods for checking the archive during special examinations of enterprises and organizations - applicants for a license of the Ministry of Defense of Russia for activities to create information security tools and verify the compliance of software development processes with the requirements of GOST R 56939-2016 during a special examination of licensees of the Ministry of Defense of Russia in the field of creating information security tools have been developed.*

Keywords: *conformity assessment, information security, information protection, certification, certification tests, special examinations, information security tools, licensing system, development of secure software, archival storage.*

References

1. Trofimov V.V. Kak stat` razrabotchikom sredstv zashchity` informatcii dlia Ministerstva oborony` Rossii`skoi` Federatcii // Information Security, 2005, № 3. S. 27-28.
2. Al`terman A.D., Lushnikov N.D. Informatcionnaia bezopasnost` cherez licenzirovanie i sertifikatciiu // Alleia nauki. 2018. T. 3. №6 (22). S. 897-900.
3. Borisova E.A., Popov K.G. Leecenzirovanie kak metod obespecheniia informatcionnoi` bezopasnosti // Simvol nauki: mezhdunarodny`i` nauchny`i` zhurnal. 2016. № 7-2 (19). S. 36-38.
4. Dolgov D.S. Leecenzirovanie kak administrativno-pravovoe sredstvo obespecheniia informatcionnoi` bezopasnosti v rossii`skoi` federatcii // Vestneyk Sarahtovskoi` gosudarstvennoi` akademii prava. 2008. № 4 (62). S. 196-197.
5. Zhogal` A.V. Sovremenny`e problemy` obespecheniia informatcionnoi` bezopasnosti v Rossii // Kontekst i refleksiia: filosofiia o mire i cheloveke. 2017. № 1A, Tom 6. - S. 178-185.
6. Katarzhnov A.D. Leecenzirovanie deiatel`nosti po tekhnicheskoi` zashchite konfidentcial`noi` informatcii // Zashchita informatcii. Insai`d. 2012. № 2 (44). S. 16-20.
7. Nagorny`i` S. I., Cliomfas Iu. V. Iskushenie zakonom // Zashchita informatcii. Insai`d. 2011. № 3. S. 26-29.
8. Skripnik D.A. Obshchie voprosy` tekhnicheskoi` zashchity` informatcii. M.: Natcional`ny`i` Otkry`ty`i` Universitet «INTUIT», 2016. 425 s.
9. Shaposhnikov V.I. Nekotory`e problemy` pravovogo regulirovaniia otnoshenii` po licenzirovaniiu v oblasti zashchity` informatcii // Aktual`ny`e problemy` rossii`skogo prava. 2007. № 2. S. 77-81.
10. Shahalov I.Iu. Leecenziia kak produkt osoznannoi` neobhodimosti licenzirovanie deiatel`nosti operatorov personal`ny`kh danny`kh // Zashchita informatcii. Insai`d. 2010. № 2 (32). S. 53-55.
11. Zakonodatel`no-pravovoe i organizatcionno-tekhnicheskoe obespechenie ... avtomatizirovanny`kh sistem i informatcionno-vy`chislitel`ny`kh setei` / Kotenko I.V., Kotuhov M.M., Markov A.S. i dr. - SPb: VUS, 2000. 190 s.
12. Markov A.S. Tekhnicheskaia zashchita informatcii. Kurs lektcii`. M. AISNT. 2020. 234 s.
13. Shahalov I.Iu. Leecenzirovanie deiatel`nosti po tekhnicheskoi` zashchite konfidentcial`noi` informatcii // Voprosy` kiberbezopasnosti. 2013. № 1 (1). S. 49-54.
14. Shahalov I.Iu. Pravovoe obosnovanie sertifikatcii sredstv zashchity` informatcii // Monitoring pravoprimeneniia. 2015. № 3 (16). S. 64-68.

4 Andrey Ivanov, Russian Defense Ministry employee, Moscow, Russia. E-mail: is@cnpo. ru

5 Ivan Sprogis, Russian Defense Ministry employee, Moscow, Russia. E-mail: bai@cnpo.ru

6 Igor Shahalov, Associate Professor of the Department of Information Security, Bauman Moscow State Technical University, Moscow, Russia. E-mail: i.shahalov@bmstu.ru

15. Markov A.S., Tcirlov V.L., Barabanov A.V. Metody` ocenki nesootvetstviia sredstv zashchity` informatcii. M.: Radio i sviaz`. 2012. 192 s.
16. Maksimov E.E., Burs K.V., Zhereb L.A. Aktual`nost` i problemy` e`lektronny`kh arhivov sovremenny`kh rossii`skikh predpriiatii` // Aktual`ny`e problemy` aviatcii i kosmonavtiki. 2012. T. 2. № 8. S. 184-185.
17. Samantcov A. P. Tcifrovy`e arhivy` predpriiatii`: problemy` khraneniia danny`kh // Vestneyk luridicheskogo instituta MIIT. 2021. № 2 (34). S. 143-148.
18. Grishin M.I., Markov A.S., Tcirlov V.L. Prakticheskie aspekty` realizatcii mer po razrabotke bezopasnogo programmnogo obespecheniia // IT-Standart. 2019. № 2 (19). S. 29-39.
19. Devianin P.N., My`litcy`n R.N., Telezhnikov V.Iu. Tekhnologii bezopasnoi` razrabotki i obespecheniia doveriia k OSSN Astra Linux Special Edition. V sbornike: Sostoianie i perspektivy` razvitiia sovremennoi` nauki po napravleniiu «Informatcionnaia bezopasnost`». Sbornik statei` III Vserossii`skoi` nauchno-tekhnicheskoi` konferentcii. Anapa, 2021. S. 13-23.
20. Barabanov A., Markov A., Fadin A., Tsirlov V., Shakhalov I. Synthesis of Secure Software Development Controls. In Proceedings of the 8th International Conference on Security of Information and Networks (Sochi, Russian Federation, September 08-10, 2015). SIN '15. ACM New York, NY, USA, 2015, pp. 93-97. DOI: 10.1145/2799979.2799998
21. Barabanov A.V. Markov A.S., Tcirlov V.L. O sistematike informatcionnoi` bezopasnosti tcepei` postavki programmnogo obespecheniia. // Bezopasnost` informatcionny`kh tekhnologii`. 2019. T. 26. № 3. S. 68-79.
22. Barabanov A.V., Markov A.S., Tcirlov V.L. Ocenka sootvetstviia sredstv zashchity` informatcii «Obshchim kriteriiam» // Informatcionny`e tekhnologii. 2015. T. 21. № 4. S. 264-270.
23. Dorofeev A.V., Markov A.S., Rautkin Y.V. Ethical Hacking Training // CEUR Workshop Proceedings, 2019, Vol-2522, pp. 47-56.