



МИНИСТЕРСТВО ЮСТИЦИИ РОССИЙСКОЙ ФЕДЕРАЦИИ

ЗАРЕГИСТРИРОВАНО

Регистрационный № 77896

от "16" апреля 2024 г.

**ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ
(ФСТЭК России)**

П Р И К А З

« 1 » декабря 2023 г.

Москва

№ 240

Об утверждении Порядка проведения сертификации процессов безопасной разработки программного обеспечения средств защиты информации

В соответствии с подпунктом 13 пункта 8 Положения о Федеральной службе по техническому и экспортному контролю, утвержденного Указом Президента Российской Федерации от 16 августа 2004 г. № 1085, и пунктом 9 приложения, утвержденного постановлением Правительства Российской Федерации от 15 мая 2010 г. № 330, **П Р И К А З Ы В А Ю:**

1. Утвердить прилагаемый Порядок проведения сертификации процессов безопасной разработки программного обеспечения средств защиты информации.
2. Установить, что настоящий приказ вступает в силу с 1 июня 2024 г.

**ДИРЕКТОР ФЕДЕРАЛЬНОЙ СЛУЖБЫ
ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ**

В.СЕЛИН

УТВЕРЖДЕН
приказом ФСТЭК России
от 1 декабря 2023 г. № 240

Порядок проведения сертификации процессов безопасной разработки программного обеспечения средств защиты информации

1. Сертификация процессов проектирования и производства программного обеспечения (далее – процессы безопасной разработки программного обеспечения) средств защиты информации, содержащей сведения, составляющие государственную тайну или относимые к охраняемой в соответствии с законодательством Российской Федерации иной информации ограниченного доступа, осуществляется на соответствие требованиям национального стандарта Российской Федерации ГОСТ Р 56939-2016 «Защита информации. Разработка безопасного программного обеспечения. Общие требования», утвержденного и введенного в действие приказом Федерального агентства по техническому регулированию и метрологии от 1 июня 2016 г. № 458-ст¹ (далее – требования по безопасной разработке).

2. Сертификация процессов безопасной разработки программного обеспечения (далее – сертификация) осуществляется на основании договора, заключаемого изготовителем средства защиты информации (далее – изготовитель) с органом по сертификации².

3. Изготовитель при намерении сертифицировать процессы безопасной разработки программного обеспечения выбирает для проведения сертификации аккредитованный ФСТЭК России орган по сертификации, согласовывает с ним сроки проведения сертификации.

4. Для получения сертификата соответствия изготовитель представляет в ФСТЭК России заявку на сертификацию (далее – заявка).

В заявке указываются:

- а) полное и сокращенное (при наличии) наименование изготовителя, его организационно-правовая форма;
- б) адрес юридического лица в пределах места нахождения юридического лица – изготовителя;
- в) адрес для корреспонденции изготовителя;
- г) фамилия, имя и отчество (при наличии) лица, ответственного за сертификацию;

¹ М., «Стандартинформ», 2016.

² Пункт 11 Положения о сертификации средств защиты информации, утвержденного постановлением Правительства Российской Федерации от 26 июня 1995 г. № 608.

- д) номер телефона и адрес электронной почты (при наличии) изготовителя;
- е) наименование органа по сертификации, в котором планируется проведение сертификации;
- ж) заявляемый срок действия сертификата соответствия.

Заявка подписывается руководителем изготовителя (лицом, которое в силу закона или учредительных документов выступает от его имени) и заверяется печатью изготовителя (при наличии печати) (рекомендуемый образец заявки приведен в приложении № 1 к настоящему Порядку).

5. К заявке прилагается руководство по безопасной разработке программного обеспечения, разработанное в соответствии с пунктом 4.10 требований по безопасной разработке.

6. Заявка с приложением направляется изготовителем в ФСТЭК России почтовым отправлением с уведомлением о вручении или представляется непосредственно в ФСТЭК России.

7. ФСТЭК России рассматривает заявку в течение 15 рабочих дней со дня получения заявки.

8. Заявка возвращается для доработки в случае отсутствия в ней сведений, предусмотренных пунктом 4 настоящего Порядка, а также в случае несоответствия руководства по безопасной разработке программного обеспечения пункту 4.10 требований по безопасной разработке.

9. Уведомление о необходимости доработки заявки вручается изготовителю или направляется ему почтовым отправлением в срок не позднее 15 рабочих дней со дня получения заявки.

10. Сертификация проводится на основании решения ФСТЭК России о проведении сертификации процессов безопасной разработки программного обеспечения (далее – решение). В решении указываются:

- а) номер и дата принятия решения;
- б) полное и сокращенное (при наличии) наименование изготовителя, его организационно-правовая форма;
- в) адрес юридического лица в пределах места нахождения юридического лица – изготовителя;
- г) наименование органа по сертификации, который будет проводить сертификацию.

Решение оформляется в трёх экземплярах, подписывается уполномоченным должностным лицом ФСТЭК России и направляется почтовым отправлением или вручается по одному экземпляру изготовителю и органу по сертификации. Один экземпляр решения остается в ФСТЭК России (рекомендуемый образец решения приведен в приложении № 2 к настоящему Порядку).

11. Оформление нового решения осуществляется в случае замены органа по сертификации, в том числе в связи с приостановлением или прекращением

действия аттестата аккредитации органа по сертификации³.

12. Обращение изготовителя с обоснованием необходимости оформления нового решения направляется в ФСТЭК России почтовым отправлением.

13. ФСТЭК России в срок не позднее 15 рабочих дней со дня получения обращения изготовителя оформляет новое решение и направляет его почтовым отправлением или вручает изготовителю и органу по сертификации.

14. Действие решения прекращается в случае получения ФСТЭК России обращения изготовителя о прекращении сертификации.

15. ФСТЭК России в срок не позднее 15 рабочих дней со дня получения обращения изготовителя направляет почтовым отправлением или вручает изготовителю и органу по сертификации уведомление о прекращении действия решения.

16. Для проведения сертификации изготовитель направляет органу по сертификации руководство по безопасной разработке программного обеспечения.

17. Орган по сертификации проводит сертификацию в сроки, установленные договором на проведение сертификации, заключенным с изготовителем.

18. Сертификация проводится на материально-технической базе изготовителя, используемой для разработки и поддержки безопасности программного обеспечения, расположенной на территории Российской Федерации.

19. В процессе сертификации осуществляются:

оценка соответствия руководства по безопасной разработке программного обеспечения и документации по безопасной разработке программного обеспечения, имеющейся у изготовителя, пунктам 4.10 и 4.12 требований по безопасной разработке соответственно;

проверка наличия у изготовителя средств разработки программного обеспечения, а также средств, предназначенных для проведения композиционного, статического и динамического анализа программного обеспечения, предусмотренных подпунктами 5.3.3.4 и 5.4.3.3 пункта 5.3 требований по безопасной разработке;

проверка реализации изготовителем процессов безопасной разработки программного обеспечения, приведенных в руководстве и в документации по безопасной разработке программного обеспечения;

³ Пункты 41 и 42 Правил выполнения отдельных работ по аккредитации органов по сертификации и испытательных лабораторий, выполняющих работы по оценке (подтверждению) соответствия в отношении продукции (работ, услуг), используемой в целях защиты сведений, составляющих государственную тайну или относимых к охраняемой в соответствии с законодательством Российской Федерации иной информации ограниченного доступа, и продукции (работ, услуг), сведения о которой составляют государственную тайну, в установленной ФСТЭК России сфере деятельности, утвержденных приказом ФСТЭК России от 10 апреля 2015 г. № 33 (зарегистрирован Минюстом России 20 мая 2015 г., регистрационный № 37342), с изменениями, утвержденными приказом ФСТЭК России от 27 июля 2023 г. № 148 (зарегистрирован Минюстом России 23 ноября 2023 г., регистрационный № 76062).

проверка реализации изготовителем процедур поддержки безопасности программного обеспечения;

проверка выполнения требований к обучению специалистов⁴ изготовителя, участвующих в реализации процессов безопасной разработки программного обеспечения.

20. По результатам проведения сертификации орган по сертификации оформляет протоколы сертификации, содержащие:

основание для проведения сертификации (номер и дату решения);

даты и места проведения сертификации;

описание процессов безопасной разработки программного обеспечения, реализованных изготовителем, в отношении которых была проведена сертификация;

описание результатов сертификации по каждому реализованному у изготовителя процессу безопасной разработки программного обеспечения;

выводы о соответствии (несоответствии) процессов безопасной разработки программного обеспечения, реализованных изготовителем, требованиям по безопасной разработке.

Протоколы сертификации подписываются экспертами органа по сертификации, проводившими сертификацию.

21. По завершении сертификации орган по сертификации оформляет экспертное заключение о соответствии (несоответствии) реализованных изготовителем процессов безопасной разработки программного обеспечения требованиям по безопасной разработке, содержащее:

основание для проведения сертификации (номер и дату решения);

описание процессов безопасной разработки программного обеспечения, реализованных изготовителем;

описание результатов сертификации по каждому процессу безопасной разработки программного обеспечения;

вывод о соответствии (несоответствии) реализованных изготовителем процессов безопасной разработки программного обеспечения требованиям по безопасной разработке;

выводы о возможности (невозможности) выдачи сертификата соответствия.

Экспертное заключение подписывается экспертами органа по сертификации, проводившими сертификацию, и утверждается руководителем органа по сертификации.

22. В случае несоответствия реализованных изготовителем процессов безопасной разработки программного обеспечения требованиям по безопасной разработке экспертное заключение, содержащее такой вывод, направляется

⁴ Подпункты 5.9.3.1 и 5.9.3.2 пункта 5.9 требований по безопасной разработке.

изготовителю.

Изготовитель устраняет выявленные несоответствия процессов (процедур) безопасной разработки программного обеспечения требованиям по безопасной разработке и информирует об этом орган по сертификации почтовым отправлением.

23. Орган по сертификации после устранения изготовителем несоответствий проводит повторную сертификацию в объеме, необходимом для проверки устранения изготовителем выявленных несоответствий.

По результатам повторной сертификации оформляются протоколы повторной сертификации и экспертное заключение.

24. В случае соответствия реализованных изготовителем процессов безопасной разработки программного обеспечения требованиям по безопасной разработке орган по сертификации подготавливает проект сертификата соответствия (рекомендуемый образец приведен в приложении № 3 к настоящему Порядку) и представляет материалы сертификации в ФСТЭК России.

Материалы сертификации должны включать:

экспертное заключение;

проект сертификата соответствия;

протоколы сертификации;

протоколы повторной сертификации и экспертное заключение (в случае проведения повторной сертификации);

руководство по безопасной разработке программного обеспечения;

документацию по безопасной разработке программного обеспечения, представленную изготовителем при проведении сертификации.

Материалы сертификации, за исключением документации по безопасной разработке программного обеспечения, представляются на бумажном носителе и в электронном виде. Документация по безопасной разработке программного обеспечения представляется в электронном виде.

25. В случае если в экспертном заключении содержится вывод о невозможности выдачи сертификата соответствия, ФСТЭК России в срок не позднее 5 рабочих дней со дня поступления материалов сертификации принимает решение об отказе в выдаче сертификата соответствия.

26. В случае если в экспертном заключении содержится вывод о возможности выдачи сертификата соответствия, ФСТЭК России в срок не более 30 календарных дней со дня поступления материалов сертификации рассматривает их и при отсутствии недостатков принимает решение о выдаче сертификата соответствия.

27. В случае выявления в материалах сертификации недостатков ФСТЭК России направляет органу по сертификации и изготовителю уведомление о выявленных в материалах сертификации недостатках с их описанием и

предложениями по устранению.

28. Орган по сертификации с участием изготовителя в срок не позднее 30 календарных дней со дня подписания уведомления о выявленных в материалах сертификации недостатках устраняет выявленные недостатки, при необходимости проводит повторную сертификацию и представляет в ФСТЭК России доработанные материалы сертификации.

29. В случае непредставления органом по сертификации в установленный пунктом 28 настоящего Порядка срок доработанных материалов сертификации ФСТЭК России принимает решение об отказе в выдаче сертификата соответствия.

Решение об отказе в выдаче сертификата соответствия подписывается уполномоченным должностным лицом ФСТЭК России и в срок не позднее 5 рабочих дней со дня подписания вручается изготовителю и органу по сертификации или направляется им почтовым отправлением.

30. В случае принятия ФСТЭК России решения о выдаче сертификата соответствия сертификат соответствия подписывается уполномоченным должностным лицом ФСТЭК России, сведения о сертификате соответствия учитываются в перечне сертификатов соответствия процессов безопасной разработки программного обеспечения требованиям по безопасной разработке (далее – перечень сертификатов соответствия).

Сертификат соответствия выдаётся на срок, указанный в заявке, но не более чем на пять лет.

Сертификат соответствия в течение 10 рабочих дней после дня подписания вручается изготовителю или направляется ему заказным почтовым отправлением.

31. В случае утраты сертификата соответствия изготовитель вправе обратиться в ФСТЭК России с заявлением о выдаче дубликата сертификата соответствия.

В течение 10 рабочих дней со дня регистрации заявления о выдаче дубликата сертификата соответствия ФСТЭК России оформляет дубликат на бланке сертификата соответствия с пометкой «дубликат, оригинал сертификата соответствия признается недействующим» и вручает изготовителю или направляет ему почтовым отправлением.

32. Выдача нового сертификата соответствия осуществляется в случае:

- а) реорганизации изготовителя;
- б) изменения наименования изготовителя;
- в) изменения адреса юридического лица в пределах места нахождения юридического лица – изготовителя.

33. Для выдачи нового сертификата соответствия изготовитель либо его правопреемник представляют в ФСТЭК России заявление о выдаче нового сертификата соответствия.

В заявлении о выдаче нового сертификата соответствия указываются новые

сведения об изготовителе или его правопреемнике.

Заявление о выдаче нового сертификата соответствия представляется непосредственно в ФСТЭК России или направляется почтовым отправлением.

34. ФСТЭК России в срок, не превышающий 10 рабочих дней со дня получения заявления о выдаче нового сертификата соответствия, осуществляет проверку достоверности содержащихся в заявлении сведений и принимает решение о выдаче нового сертификата соответствия или об отказе в его выдаче.

35. Основаниями для отказа в выдаче нового сертификата соответствия является наличие в заявлении о выдаче нового сертификата соответствия недостоверных сведений.

ФСТЭК России в течение 5 рабочих дней со дня принятия решения об отказе в выдаче нового сертификата соответствия вручает изготовителю или его правопреемнику уведомление об отказе в выдаче нового сертификата соответствия с указанием причин отказа или направляет его почтовым отправлением.

36. ФСТЭК России в течение 5 рабочих дней со дня принятия решения о выдаче нового сертификата соответствия направляет почтовым отправлением или вручает изготовителю или его правопреемнику уведомление о выдаче нового сертификата соответствия с приложением нового сертификата соответствия и вносит сведения о новом выданном сертификате соответствия в перечень сертификатов соответствия.

37. Изготовитель в течение 5 рабочих дней со дня получения нового сертификата соответствия представляет (направляет) в ФСТЭК России подлинник ранее выданного сертификата соответствия.

38. ФСТЭК России имеет право приостанавливать и (или) прекращать действие сертификатов соответствия⁵.

⁵ Пункт 11 приложения, утвержденного постановлением Правительства Российской Федерации от 15 мая 2010 г. № 330.

Приложение № 1
к Порядку сертификации процессов безопасной
разработки программного обеспечения средств
защиты информации, утвержденному приказом
ФСТЭК России от 1 декабря 2023 г. №240
Рекомендуемый образец

ЗАЯВКА

на сертификацию процессов безопасной разработки программного обеспечения

Полное и сокращенное (при наличии) наименование изготовителя, его организационно-правовая форма:	
Адрес юридического лица в пределах места нахождения юридического лица – изготовителя:	
Адрес для корреспонденции изготовителя:	
Фамилия, имя и отчество (при наличии) лица, ответственного за сертификацию процессов безопасной разработки программного обеспечения:	
Номер телефона и адрес электронной почты (при наличии) изготовителя:	
Наименование органа по сертификации, в котором планируется проведение сертификации:	
Заявляемый срок действия сертификата соответствия:	
Должность руководителя изготовителя	М.П. подпись, инициалы, фамилия (при наличии) « » 20 г.

Приложение № 2
к Порядку сертификации процессов безопасной
разработки программного обеспечения средств
защиты информации, утвержденному приказом
ФСТЭК России от 1 декабря 2023 г. № 240
Рекомендуемый образец

Федеральная служба по техническому и экспортному контролю

РЕШЕНИЕ

о проведении сертификации процессов безопасной разработки программного
обеспечения

№ от « » 20... г.

Изготовитель:

организационно-правовая форма и наименование изготовителя

Адрес юридического лица:

адрес юридического лица в пределах места нахождения
юридического лица – изготовителя

Орган по сертификации:

наименование органа по сертификации

Должность уполномоченного лица
ФСТЭК России

подпись

инициалы, фамилия

Приложение № 3
к Порядку сертификации процессов безопасной
разработки программного обеспечения средств
защиты информации, утвержденному приказом
ФСТЭК России от 1 декабря 2023 г. № 240
Рекомендуемый образец

**Система сертификации средств защиты
информации ФСТЭК России**
СЕРТИФИКАТ СООТВЕТСТВИЯ

№

номер сертификата соответствия

Выдан: _____
дата выдачи сертификата соответствия

Действителен до: _____
дата окончания срока действия сертификата соответствия

Дубликат, оригинал сертификата соответствия признается недействующим
(в случае предоставления дубликата)

Настоящий сертификат удостоверяет, что процессы безопасной
разработки,
реализованные _____,

наименование изготовителя

соответствуют требованиям национального стандарта ГОСТ Р 56939-2016
«Защита информации. Разработка безопасного программного обеспечения.
Общие требования», утвержденного и введенного в действие приказом
Федерального агентства по техническому регулированию и метрологии
от 1 июня 2016 г. № 458-ст.

Сертификат выдан на основании результатов сертификации, проведенной
органом по сертификации _____

наименование органа по сертификации

(аттестат аккредитации _____)

дата выдачи и номер аттестата аккредитации органа по сертификации

экспертное заключение от _____.

дата утверждения экспертного заключения

Должность уполномоченного лица ФСТЭК России

м.п.

подпись

инициалы, фамилия