

Продукты и услуги Информационно-правовое обеспечение ПРАЙМ Документы ленты ПРАЙМ Проект Приказа Федеральной службы по техническому и экспортному контролю "Об утверждении Порядка сертификации процессов безопасной разработки программного обеспечения средств защиты информации" (подготовлен ФСТЭК России 29.10.2023)

 [Обзор документа](#)

Проект Приказа Федеральной службы по техническому и экспортному контролю "Об утверждении Порядка сертификации процессов безопасной разработки программного обеспечения средств защиты информации" (подготовлен ФСТЭК России 29.10.2023)

3 ноября 2023

Досье на проект

Пояснительная записка

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. N 1085, и пунктом 9 Положения, утвержденного постановлением Правительства Российской Федерации от 15 мая 2010 г. N 330, приказываю:

1. Утвердить прилагаемый Порядок 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 В. Селин
по техническому и экспортному контролю
УТВЕРЖДЕНО
приказом ФСТЭК России
от ____ ноября 2023 г. N ____

Порядок сертификации процессов безопасной разработки программного обеспечения средств защиты информации

1. Сертификация процессов безопасной разработки программного обеспечения средств защиты информации (далее - программное обеспечение) проводится в целях подтверждения соответствия процессов безопасной разработки программного обеспечения, внедренных изготовителем средства защиты информации (далее - изготовитель), требованиям национального стандарта ГОСТ Р 56939-2016 "Защита информации. Разработка безопасного программного обеспечения. Общие требования" (далее - требования по безопасной разработке).
2. Сертификация процессов безопасной разработки программного обеспечения осуществляется на основании договора, заключаемого изготовителем с органом по сертификации*(1).
3. Изготовитель при подготовке к сертификации процессов безопасной разработки программного обеспечения:

внедряет и реализует процессы безопасной разработки программного обеспечения в соответствии с требованиями по безопасной разработке;

разрабатывает руководство по безопасной разработке программного обеспечения, регламентирующее процессы безопасной разработки программного обеспечения;

выбирает для проведения сертификации аккредитованный ФСТЭК России в соответствующей области аккредитации орган по сертификации*(2), согласовывает с ним возможность и сроки проведения сертификации.

4. Для получения сертификата соответствия изготовитель представляет в ФСТЭК России заявку на сертификацию процессов разработки программного обеспечения (далее - заявка).

В заявке указываются:

- а) наименование изготовителя, его организационно-правовая форма;
- б) адрес юридического лица в пределах места нахождения юридического лица;
- в) адрес для корреспонденции изготовителя;
- г) фамилия, имя и отчество (при наличии) лица, ответственного за сертификацию процессов безопасной разработки программного обеспечения;
- д) номер телефона и адрес электронной почты (при наличии) изготовителя;
- е) наименование органа по сертификации, в котором планируется проведение сертификации.

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 N 1 к настоящему Порядку.

5. К заявке прилагается руководство по безопасной разработке программного обеспечения средств защиты информации, разработанное в соответствии с требованиями по безопасной разработке.

6. Заявка и прилагаемые к ней документы направляются изготовителем в ФСТЭК России почтовым отправлением с уведомлением о вручении или представляются 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, прилагаемого к заявке на сертификацию, требованиям 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. В случае принятия решения о проведении сертификации процессов безопасной разработки программного обеспечения средств защиты информации (далее - решение) в решении указываются:

- а) номер и дата принятия решения;
- б) наименование изготовителя, его организационно-правовая форма;
- в) адрес юридического лица в пределах места нахождения юридического лица;
- 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 (рекомендуемый образец приведен в приложении N 2 к настоящему Порядку).

11. Решение подлежит переоформлению в случае замены органа по сертификации, в том числе в связи с приостановлением или прекращением действия аттестата аккредитации органа по сертификации.
12. Обращение изготовителя с обоснованием необходимости переоформления решения направляется в ФСТЭК России почтовым отправлением.
13. ФСТЭК России в срок не позднее 15 рабочих дней со дня получения обращения изготовителя переоформляет решение и направляет его почтовыми отправлениями или вручает изготовителю и органу по сертификации.
14. Решение аннулируется в случае получения от изготовителя обращения о прекращении сертификации процессов безопасной разработки программного обеспечения.
15. ФСТЭК России в срок не позднее 15 рабочих дней со дня получения обращения изготовителя направляет почтовыми отправлениями или вручает изготовителю и органу по сертификации уведомление об аннулировании решения.
16. Для проведения сертификации внедренных изготовителем процессов безопасной разработки программного обеспечения изготовитель направляет органу по сертификации руководство по безопасной разработке программного обеспечения.
17. Орган по сертификации в срок не позднее 20 рабочих дней со дня получения от изготовителя руководства по безопасной разработке программного обеспечения разрабатывает программу и методику проведения сертификации процессов безопасной разработки программного обеспечения (далее - программа и методика), согласовывает их с изготовителем.

Программа и методика должны содержать описание процессов безопасной разработки программного обеспечения, внедренных изготовителем, сроки проведения сертификации, порядок проведения сертификации, методы сертификации, требования к документации по безопасной разработке программного обеспечения изготовителя.

18. Орган по сертификации проводит сертификацию в соответствии с программой и методикой.
19. Сертификация проводится в сроки, установленные договором на проведение сертификации.
20. Сертификация проводится на материально-технической базе изготовителя, используемой для разработки и поддержки безопасности программного обеспечения, расположенной на территории Российской Федерации.

21. Сертификация включает:

оценку соответствия руководства по безопасной разработке программного обеспечения и документации по безопасной разработке программного обеспечения, имеющихся у изготовителя, требованиям по безопасной разработке;

проверку наличия у изготовителя средств разработки программного обеспечения, а также средств, предназначенных для проведения композиционного анализа программного обеспечения, статического и динамического анализа исходного кода программного обеспечения;

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

проверку реализации изготовителем процедур поддержки безопасности программного обеспечения;

проверку знаний и навыков специалистов изготовителя, участвующих в реализации процессов безопасной разработки программного обеспечения.

22. По результатам проведения сертификации орган по сертификации оформляет протоколы сертификации, которые должны содержать:

основание для проведения сертификации (номер и дату решения);

даты и места проведения сертификации;

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

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

выводы о соответствии процессов безопасной разработки программного обеспечения средств защиты информации, реализованных изготовителем, установленным требованиям.

Протоколы сертификации подписываются экспертами органа по сертификации, проводившими сертификацию.

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

основание для проведения сертификации (номер и дата 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 утверждается руководителем органа по сертификации.

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

Изготовитель устраняет выявленные несоответствия процессов (процедур) безопасной разработки программного обеспечения средств защиты информации установленным требованиям и информирует об этом орган по сертификации.

25. Повторная сертификация проводится в объеме, необходимом для проверки устранения выявленных несоответствий.

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

26. В случае соответствия реализованных изготовителем процессов безопасной разработки программного обеспечения средств защиты информации требованиям по безопасной разработке орган по сертификации подготавливает проект сертификата соответствия (рекомендуемый образец приведен в приложении N 3 к настоящему Порядку) и представляет материалы сертификации в ФСТЭК России.

Материалы сертификации должны включать:

программу и методику;

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.

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

27. В случае если в экспертном заключении сделан 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.

28. В случае если в экспертном заключении сделан вывод о возможности выдачи сертификата соответствия, ФСТЭК России в срок не более 30 календарных дней рассматривает материалы сертификации и при отсутствии недостатков принимает решение о выдаче сертификата соответствия.

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.

29. Орган по сертификации и изготовитель в срок не позднее 30 календарных дней со дня подписания уведомления о выявленных в материалах сертификации недостатках должны устранить выявленные недостатки, при необходимости провести повторную сертификацию и представить в ФСТЭК России доработанные материалы сертификации.

30. В случае непредставления в установленный 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 решения об отказе вручается изготовителю или направляется ему почтовым отправлением.

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

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

32. 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 недействительным" и вручает изготовителю или направляет ему почтовым отправлением.

33. Сертификат соответствия подлежит переоформлению в случае:

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

34. Для переоформления сертификата соответствия изготовитель либо его правопреемник представляют в ФСТЭК России заявление о переоформлении сертификата соответствия.

В заявлении о переоформлении сертификата соответствия указываются новые сведения об изготовителе или его правопреемнике.

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

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

36. Основаниями для отказа в переоформлении сертификата соответствия является наличие в заявлении о переоформлении сертификата соответствия недостоверных сведений.

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

38. ФСТЭК России в течение 5 рабочих дней со дня принятия решения о переоформлении сертификата соответствия направляет почтовым отправлением или вручает изготовителю или его правопреемнику уведомление о переоформлении сертификата соответствия с приложением переоформленного сертификата соответствия и вносит сведения о переоформленном сертификате соответствия в перечень сертификатов соответствия.

39. Изготовитель в течение 5 рабочих дней со дня получения переоформленного сертификата соответствия должен представить (направить) в ФСТЭК России подлинник ранее выданного сертификата соответствия.

40. Действие сертификата соответствия приостанавливается в случаях:

- а) установления факта несоответствия процессов безопасной разработки, реализованных изготовителем, требованиям по безопасной разработке на основании поступившей в ФСТЭК России информации;
- б) обращения изготовителя о приостановлении действия сертификата соответствия.

41. Решение о приостановлении действия сертификата соответствия оформляется приказом ФСТЭК России.

Действие сертификата соответствия может быть приостановлено на срок не более 90 календарных дней.

42. ФСТЭК России в течение 5 рабочих дней со дня принятия решения о приостановлении действия сертификата соответствия направляет почтовым отправлением или вручает изготовителю уведомление о приостановлении действия сертификата соответствия.

43. В случае приостановления действия сертификата соответствия на основании подпункта "а" пункта 40 настоящего Порядка изготовитель устраняет выявленные несоответствия требованиям по безопасной разработке, проводит с привлечением органа по сертификации дополнительную сертификацию в части процессов безопасной разработки, в которых были установлены несоответствия требованиям по безопасной разработке, представляет в ФСТЭК России экспертное заключение органа по сертификации и протокол дополнительной сертификации.

44. Действие сертификата соответствия возобновляется в случае:

устранения изготовителем несоответствия процессов безопасной разработки программного обеспечения требованиям по безопасной разработке;

обращения изготовителя о возобновлении действия сертификата соответствия в случае, если действие сертификата соответствия было приостановлено на основании подпункта "б" пункта 40 настоящего Порядка.

45. Решение о возобновлении действия сертификата соответствия оформляется приказом ФСТЭК России.

ФСТЭК России в течение 5 рабочих дней со дня принятия решения о возобновлении действия сертификата соответствия направляет почтовым отправлением или вручает изготовителю уведомление о возобновлении действия сертификата соответствия.

46. ФСТЭК России вносит сведения о приостановлении и возобновлении действия сертификата соответствия в перечень сертификатов соответствия.

47. Действие сертификата соответствия прекращается в случаях:

а) непредставления изготовителем в установленный срок материалов, подтверждающих устранение несоответствия процессов безопасной разработки программного обеспечения требованиям по безопасной разработке;

б) обращения изготовителя о прекращении действия сертификата соответствия.

48. Решение о прекращении действия сертификата соответствия оформляется приказом ФСТЭК России.

ФСТЭК России в течение 5 рабочих дней со дня принятия решения о прекращении действия сертификата соответствия направляет почтовым отправлением или вручает изготовителю уведомление о прекращении действия сертификата соответствия.

49. ФСТЭК России вносит сведения о прекращении действия сертификата соответствия в перечень сертификатов соответствия.

50. В случае прекращения действия сертификата соответствия на основании подпункта "а" пункта 47 настоящего Порядка изготовитель может подать заявку на сертификацию процессов безопасной разработки программного обеспечения только через 12 месяцев с даты принятия ФСТЭК России решения о прекращении действия сертификата соответствия.

Приложение N 1

к Порядку сертификации процессов безопасной разработки программного обеспечения средств защиты информации, утвержденному приказом ФСТЭК России от ноября 2023 г. N

Рекомендуемый образец

ЗАЯВКА

на сертификацию процессов безопасной разработки программного обеспечения

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

*(1) Пункт 11 Положения о сертификации средств защиты информации, утвержденного постановлением Правительства Российской Федерации от 26 июня 1995 г. N 608.

*(2) Реестр аккредитованных ФСТЭК России органов по сертификации и испытательных лабораторий размещается на официальном сайте ФСТЭК России в информационно-телекоммуникационной сети "Интернет" в соответствии с Порядком ведения реестра аккредитованных ФСТЭК России органов по сертификации и испытательных лабораторий, утвержденным приказом ФСТЭК России от 18 июня 2015 г. N 67 "Об утверждении формы и порядка ведения реестра аккредитованных ФСТЭК России органов по сертификации и испытательных лабораторий" (зарегистрирован Минюстом России 10 июля 2015 г., регистрационный N 37974).

Обзор документа

Сертификация процессов безопасной разработки ПО средств защиты информации будет проводиться на основании договора между изготовителем и органом по сертификации. Для получения сертификата соответствия нужно будет подать заявку с приложением руководства по безопасной разработке ПО. Документы можно будет отправить почтой или принести в ФСТЭК лично. Они будут рассмотрены в течение 15 рабочих дней.

Для проведения сертификации изготовитель направляет руководство по безопасной разработке ПО в орган по сертификации, который в течение 20 рабочих дней разрабатывает программу и методику проведения сертификации и согласовывает их с изготовителем.

Сертификация проводится на материально-технической базе изготовителя, используемой для разработки и поддержки безопасности ПО, расположенной в России.

В ходе проведения сертификации оформляются протоколы, а после ее завершения - экспертное заключение.

Орган по сертификации готовит проект сертификата соответствия и направляет материалы сертификации в ФСТЭК, которая в течение 30 дней принимает решение о выдаче сертификата соответствия.

Для просмотра актуального текста документа и получения полной информации о вступлении в силу, изменениях и порядке применения документа, воспользуйтесь поиском в Интернет-версии системы ГАРАНТ:

Проект Приказа Федеральной службы по техническому и экспортному 