



ПРЕДВАРИТЕЛЬНЫЙ
НАЦИОНАЛЬНЫЙ
СТАНДАРТ
РОССИЙСКОЙ
ФЕДЕРАЦИИ

ПНСТ
1009—
2025

Критическая информационная инфраструктура

**ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ
ДЛЯ ДОВЕРЕННЫХ
ПРОГРАММНО-АППАРАТНЫХ КОМПЛЕКСОВ**

Общие положения

Издание официальное

Москва
Российский институт стандартизации
2025

Предисловие

1 РАЗРАБОТАН Федеральным государственным бюджетным учреждением «Российский институт стандартизации» (ФГБУ «Институт стандартизации»), Акционерным обществом «Научно-производственное объединение «Критические информационные системы» (АО «НПО «КИС») и рабочей группой «Программное обеспечение для доверенных программно-аппаратных комплексов» ТК 167 «Программно-аппаратные комплексы для критической информационной инфраструктуры и программное обеспечение для них»

2 ВНЕСЕН Техническим комитетом по стандартизации ТК 167 «Программно-аппаратные комплексы для критической информационной инфраструктуры и программное обеспечение для них»

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 24 июня 2025 г. № 20-пнст

Правила применения настоящего стандарта и проведения его мониторинга установлены в ГОСТ Р 1.16—2011 (разделы 5 и 6).

Федеральное агентство по техническому регулированию и метрологии собирает сведения о практическом применении настоящего стандарта. Данные сведения, а также замечания и предложения по содержанию стандарта можно направить не позднее чем за 4 мес до истечения срока его действия разработчику настоящего стандарта по адресу: 117418 Москва, Нахимовский проспект, д. 31 к. 2 и/или в Федеральное агентство по техническому регулированию и метрологии по адресу: 123112 Москва, Пресненская набережная, д. 10, стр. 2.

В случае отмены настоящего стандарта соответствующая информация будет опубликована в ежемесячном информационном указателе «Национальные стандарты» и также будет размещена на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет (www.rst.gov.ru)

© Оформление. ФГБУ «Институт стандартизации», 2025

Настоящий стандарт не может быть полностью или частично воспроизведен, тиражирован и распространен в качестве официального издания без разрешения Федерального агентства по техническому регулированию и метрологии

II

ПРЕДВАРИТЕЛЬНЫЙ НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Критическая информационная инфраструктура

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ
ДЛЯ ДОВЕРЕННЫХ ПРОГРАММНО-АППАРАТНЫХ КОМПЛЕКСОВ

Общие положения

Critical information infrastructure. Software for trusted engineered system. General provisions

Срок действия — с 2025—10—01
до 2028—10—01

1 Область применения

Настоящий стандарт устанавливает общие положения в области программного обеспечения (ПО), предназначенного для применения в доверенных программно-аппаратных комплексах (ДПАК) и обеспечивающего соответствие ДПАК требованиям технологической независимости критической информационной инфраструктуры (КИИ), функциональности, надежности и защищенности.

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие стандарты:

ГОСТ 19.101 Единая система программной документации. Виды программ и программных документов

ГОСТ IEC 61508-3 Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 3. Требования к программному обеспечению

ГОСТ Р 51904 Программное обеспечение встроенных систем. Общие требования к разработке и документированию

ГОСТ Р 54145 Менеджмент рисков. Руководство по применению организационных мер безопасности и оценки рисков. Общая методология

ГОСТ Р 56939 Защита информации. Разработка безопасного программного обеспечения. Общие требования

ГОСТ Р 58412 Защита информации. Разработка безопасного программного обеспечения. Угрозы безопасности информации при разработке программного обеспечения

ГОСТ Р 58771 Менеджмент риска. Технологии оценки риска

ГОСТ Р 59193 Управление конфигурацией. Основные положения

ГОСТ Р 59194 Управление требованиями. Основные положения

ГОСТ Р ИСО 31000 Менеджмент риска. Принципы и руководство

ГОСТ Р ИСО/МЭК 12207 Информационная технология. Системная и программная инженерия. Процессы жизненного цикла программных средств

ГОСТ Р ИСО/МЭК 15026 Информационная технология. Уровни целостности систем и программных средств

ГОСТ Р ИСО/МЭК 15026-4 Системная и программная инженерия. Гарантирование систем и программного обеспечения. Часть 4. Гарантии жизненного цикла

ГОСТ Р ИСО/МЭК 16085 Менеджмент риска. Применение в процессах жизненного цикла систем и программного обеспечения

Издание официальное

1

ГОСТ Р ИСО/МЭК 25010 Информационные технологии. Системная и программная инженерия. Требования и оценка качества систем и программного обеспечения (SQuARE). Модели качества систем и программных продуктов

ГОСТ Р ИСО/МЭК 27001 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования

ГОСТ Р ИСО/МЭК 27002 Информационные технологии. Методы и средства обеспечения безопасности. Свод норм и правил применения мер обеспечения информационной безопасности

ГОСТ Р ИСО/МЭК 27005 Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности

ГОСТ Р ИСО/МЭК ТО 12182 Информационная технология. Классификация программных средств

ГОСТ Р МЭК 62628 Надежность в технике. Руководство по обеспечению надежности программного обеспечения

Примечание — При пользовании настоящим стандартом целесообразно проверить действие ссылочных стандартов в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет или по ежегодному информационному указателю «Национальные стандарты», который опубликован по состоянию на 1 января текущего года, и по выпускам ежемесячного информационного указателя «Национальные стандарты» за текущий год. Если заменен ссылочный стандарт, на который дана недатированная ссылка, то рекомендуется использовать действующую версию этого стандарта с учетом всех внесенных в данную версию изменений. Если заменен ссылочный стандарт, на который дана датированная ссылка, то рекомендуется использовать версию этого стандарта с указанным выше годом утверждения (принятия). Если после утверждения настоящего стандарта в ссылочный стандарт, на который дана датированная ссылка, внесено изменение, затрагивающее положение, на которое дана ссылка, то это положение рекомендуется применять без учета данного изменения. Если ссылочный стандарт отменен без замены, то положение, в котором дана ссылка на него, рекомендуется применять в части, не затрагивающей эту ссылку.

3 Термины и определения

В настоящем стандарте применены следующие термины с соответствующими определениями:

3.1 программное обеспечение доверенного программно-аппаратного комплекса; ПО ДПАК: Совокупность программ и документации, необходимых для эксплуатации и обеспечивающих функционирование доверенного программно-аппаратного комплекса.

Примечание — ПО ДПАК подразделяют на встроенное, системное, прикладное, специальное.

3.2 встроенное программное обеспечение для доверенного программно-аппаратного комплекса; встроенное ПО ДПАК: Программное обеспечение, входящее в состав доверенного программно-аппаратного комплекса, обеспечивающее функционирование его элементов электронной компонентной базы и не являющееся средой исполнения других типов программного обеспечения.

3.3 системное программное обеспечение для доверенного программно-аппаратного комплекса; системное ПО ДПАК: Программное обеспечение, реализующее функции управления доверенным программно-аппаратным комплексом в целом и его отдельными элементами, а также обеспечивающее функционирование прикладного и (или) специального программного обеспечения.

3.4 прикладное программное обеспечение для доверенного программно-аппаратного комплекса; прикладное ПО ДПАК: Программное обеспечение, с помощью которого в доверенном программно-аппаратном комплексе выполняются прикладные задачи.

3.5 специальное программное обеспечение для доверенного программно-аппаратного комплекса; специальное ПО ДПАК: Программное обеспечение, разработанное для применения в конкретном доверенном программно-аппаратном комплексе или в системах на их основе для выполнения заданных функций, в том числе без применения системного программного обеспечения.

Примечание — Примером специального программного обеспечения является программное обеспечение для конкретных отраслей промышленности.

3.6 репозиторий программного обеспечения для доверенного программно-аппаратного комплекса; репозиторий ПО ДПАК: Инфраструктура разработки программного обеспечения для доверенного программно-аппаратного комплекса с возможностью сборки, поддержки, хранения и верификации исходного кода, программных пакетов и библиотек, находящаяся на территории Российской

Федерации, технологически не зависящая от зарубежных пакетных репозиторий и созданных на их основе дистрибутивов.

3.7

инструментальное средство: Компьютерная программа, используемая как средство разработки, тестирования, анализа, производства или модификации других программ или документов на них.
[ГОСТ Р 51904—2002, пункт 3.17]

3.8

жизненный цикл продукции; ЖЦП: Совокупность взаимосвязанных процессов последовательного изменения состояния продукции от обоснования ее разработки до окончания эксплуатации и последующей ликвидации.
[ГОСТ Р 15.000—2016, пункт 3.1.2]

3.9

стадия жизненного цикла продукции; СЖЦП: Часть жизненного цикла продукции, характеризующая совокупностью выполняемых работ и их конечными результатами.
[ГОСТ Р 15.000—2016, пункт 3.1.3]

3.10

дистрибутив: Форма распространения программного обеспечения, обычно содержащая программу-установщик (для выбора режимов и параметров установки) и набор файлов, содержащих отдельные части программного средства.
[ГОСТ Р 53623—2009, пункт 3.3]

3.11

управление требованиями: Совокупность видов инженерной и управленческой деятельности по формированию требований к изделию, их анализу, структурированию, документированию, взаимному согласованию, утверждению, учету выполнения, а также согласованное и контролируемое изменение требований при необходимости.
[ГОСТ Р 59194—2020, пункт 3.1.22]

4 Общие положения

4.1 ПО ДПАК должны соответствовать требованиям настоящего стандарта, [1], стандартов и/или технических условий (ТУ) на ПО ДПАК конкретного типа.

4.2 Классификация ПО ДПАК — по ГОСТ Р ИСО/МЭК ТО 12182. Пример классификации приведен в [2].

4.3 Общие требования к ПО ДПАК:

- прикладное ПО ДПАК, функционирующее под управлением операционной системы, должно быть совместимым с одной операционной системой и/или более, сведения о которой(ых) включены в Единый реестр российских программ для электронных вычислительных машин и баз данных и/или Единый реестр программ для электронных вычислительных машин и баз данных из государств — членов Евразийского экономического союза (см. [3]);

- ПО ДПАК должно быть совместимым с радиоэлектронной продукцией (в том числе телекоммуникационным оборудованием и техническими средствами), соответствующей требованиям [4];

- ПО ДПАК, используемого в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений, должно соответствовать требованиям защиты информации, установленным в [5];

- ПО ДПАК должно быть совместимым с одним российским процессором/контроллером или более, ЖЦ которого(ых) обеспечивают организации, находящиеся в юрисдикции и на территории Российской Федерации и не находящиеся под контролем иностранного государства и/или международной организации;

- программные и технические средства хранения исходного текста и объектного кода ПО ДПАК должны находиться на территории и в юрисдикции Российской Федерации, соответствовать требованиям настоящего стандарта, стандартов и/или ТУ на ДПАК конкретного типа;

- сборочная среда ПО ДПАК, включая программные и технические средства компиляции и сборки, должна быть размещена на территории и в юрисдикции Российской Федерации и соответствовать требованиям ГОСТ Р 56939, настоящего стандарта, стандартов и/или ТУ на ДПАК конкретного типа;

- программные средства обеспечения хранения исходного кода должны быть включены в Единый реестр программ для электронных вычислительных машин и баз данных из государств — членов Евразийского экономического союза (см. [3]);

- должен быть обеспечен технический контроль целостности и доступности технических средств хранения исходных текстов и объектного кода ПО, а также целостности и доступности сборочной среды ПО ДПАК;

- функционирование технических средств, обеспечивающих автоматизированный способ активации, выпуска, распространения, управления лицензионными ключами ПО ДПАК не должно зависеть от ПО, находящегося вне территории и в юрисдикции Российской Федерации, не должно контролироваться зарубежными организациями или не гражданами Российской Федерации, или гражданами Российской Федерации, аффилированными с зарубежными организациями;

- в ПО ДПАК должна отсутствовать техническая возможность несанкционированного управления, обновления, мониторинга средствами, расположенными за пределами территории и в юрисдикции Российской Федерации; иностранными физическими и юридическими лицами или при реализации в ПО ДПАК функционала принудительного обновления/управления/мониторинга должна обеспечиваться возможность идентификации/авторизации и отключения пользователем ДПАК источника удаленного принудительного обновления, управления и мониторинга;

- ПО ДПАК должно быть разработано на принципах технологического лидерства и в соответствии с требованиями к содержанию и порядку выполнения работ, связанных с созданием безопасного (защищенного) ПО, по ГОСТ Р 56939 и в зависимости от назначения ДПАК с учетом требований [6]—[10];

- интерфейсы управления ПО ДПАК (при наличии) должны обеспечивать механизмы, ограничивающие возможность осуществления как преднамеренных, так и непреднамеренных попыток нанесения ущерба, нарушения функционирования ПО ДПАК и аппаратного обеспечения;

- при наличии программных механизмов контроля и разграничения доступа к управлению компонентами ДПАК их следует рассматривать как функции защиты информации;

- должна осуществляться регистрация событий, действий и операций по управлению и настройке оборудования, изменению параметров его работы, параметров и настроек ПО ДПАК (при наличии); регистрация событий должна осуществляться с возможностью сохранения на внешних носителях или передачи на централизованные сборщики регистрируемых событий;

- должны быть предусмотрены механизмы обновления ПО в составе ДПАК, обеспечивающие его резервирование и/или возможность восстановления из аварийной/резервной копии;

- интерфейсы взаимодействия с ПО в составе ДПАК должны предусматривать возможность чтения, изменения, сброса и восстановления настроек ПО (при наличии).

4.4 Соответствие ПО ДПАК требованиям настоящего стандарта должно быть подтверждено наличием у разработчика:

- среды разработки ПО ДПАК, находящейся на территории и в юрисдикции Российской Федерации и соответствующей требованиям ГОСТ Р 56939;

- собственного или арендованного репозитория исходного кода, программных пакетов и библиотек, разработанного в соответствии с [11] и находящегося на территории и в юрисдикции Российской Федерации, контролируемого российскими организациями или гражданами Российской Федерации, не аффилированными с зарубежными организациями, а также инструментальных средств обеспечения целостности этого репозитория;

- необходимой программной, эксплуатационной и конструкторской документации на ПО ДПАК, в объеме, достаточном для его эксплуатации и сопровождения;

- инструментальных средств для подготовки и последующего проведения испытаний ПО ДПАК;

- прав на использование или возможности публичного использования исходного кода ПО ДПАК, дающего право на модификацию и распространение ПО ДПАК в составе ДПАК, в том числе в исполняемом виде;

- возможности обеспечения соответствия процессов разработки ПО ДПАК требованиями ГОСТ Р 56939, ГОСТ Р 58412 и ГОСТ Р ИСО/МЭК 12207.

4.5 Соответствие ПО ДПАК требованиям настоящего стандарта обеспечивают участники процессов ЖЦ по ГОСТ Р ИСО/МЭК 12207, осуществляемых на территории и в юрисдикции Российской Федерации на основе рационального (необходимого и достаточного) сочетания:

- анализа достоверной и полной информации о процессах ЖЦ (контролем ЖЦ);
- результатов проведенных испытаний, проверок, тестирования (при недостатке достоверной информации о процессах ЖЦ).

Управление требованиями и их контроль на стадиях ЖЦ ПО ДПАК — по ГОСТ Р 59194. Управление конфигурацией и ее контроль на стадиях ЖЦ ПО ДПАК — по ГОСТ Р 59193.

При этом контроль на стадиях ЖЦ ПО ДПАК осуществляют организации, находящиеся на территории и в юрисдикции Российской Федерации, в том числе осуществляя проверку независимости ПО ДПАК от зарубежных репозиторий и дистрибутивов.

При проведении оценок качества ПО ДПАК на стадиях ЖЦ рекомендуется применять риск-ориентированный подход и руководствоваться требованиями ГОСТ ИЕС 61508-3, ГОСТ Р ИСО/МЭК 15026, ГОСТ Р ИСО/МЭК 15026-4, ГОСТ Р ИСО/МЭК 16085, ГОСТ Р ИСО/МЭК 27001, ГОСТ Р ИСО/МЭК 27002, ГОСТ Р ИСО/МЭК 27005, ГОСТ Р ИСО 31000, ГОСТ Р 51904, ГОСТ Р 54145, ГОСТ Р 58771.

Виды документов на ПО ДПАК на стадиях ЖЦ — по ГОСТ 19.101.

На стадиях ЖЦ ПО ДПАК следует применять актуальные методы, обеспечивающие реализацию технических требований, качество, удобство, применимость к использованию существующих программных и технических средств.

4.6 ПО ДПАК должно соответствовать требованиям, предъявляемым к его качеству, по ГОСТ Р ИСО/МЭК 25010, на основе которого реализуется уверенность потребителя (заказчика) в возможности использования ДПАК на объектах КИИ в соответствии с его предназначением на всех этапах ЖЦ и в заданных условиях.

4.7 Для ПО ДПАК, реализующего функцию защиты информации, должны выполняться требования нормативных правовых актов и национальных стандартов в области защиты информации.

4.8 Общие требования к надежности и процессам обеспечения надежности ПО ДПАК соответствующего назначения — по ГОСТ Р МЭК 62628.

Библиография

- [1] Требования к программному обеспечению, в том числе в составе программно-аппаратных комплексов, используемому органами государственной власти, заказчиками, осуществляющими закупки в соответствии с Федеральным законом «О закупках товаров, работ, услуг отдельными видами юридических лиц» (за исключением организаций с муниципальным участием), на принадлежащих им значимых объектах критической информационной инфраструктуры Российской Федерации, утвержденные постановлением Правительства Российской Федерации от 22 августа 2022 г. № 1478
- [2] Классификатор программ для электронных вычислительных машин и баз данных, утвержденный приказом Минцифры России от 22 сентября 2020 г. № 486
- [3] Правила формирования и ведения Единого реестра российских программ для электронных вычислительных машин и баз данных и Единого реестра программ для электронных вычислительных машин и баз данных из государств — членов Евразийского экономического союза, за исключением Российской Федерации, утвержденные постановлением Правительства Российской Федерации от 16 ноября 2015 г. № 1236
- [4] Требования к промышленной продукции, предъявляемые в целях ее отнесения к российской промышленной продукции, утвержденные постановлением Правительства Российской Федерации от 17 июля 2015 г. № 719 (приложение)
- [5] Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»
- [6] Федеральный закон от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»
- [7] Федеральный закон от 28 декабря 2024 г. № 523-ФЗ «О технологической политике в Российской Федерации и о внесении изменений в отдельные законодательные акты Российской Федерации»
- [8] Указ Президента Российской Федерации от 1 мая 2022 г. № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации»
- [9] Указ Президента Российской Федерации от 30 марта 2022 г. № 166 «О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации»
- [10] Правила перехода субъектов критической информационной инфраструктуры Российской Федерации на преимущественное применение доверенных программно-аппаратных комплексов на принадлежащих им значимых объектах критической информационной инфраструктуры Российской Федерации, утвержденные постановлением Правительства Российской Федерации от 14 ноября 2023 г. № 1912
- [11] Методические рекомендации по обеспечению информационной безопасности при создании и эксплуатации открытых репозиториях программного обеспечения, утвержденные Минцифры России 29 марта 2023 г.

УДК 004.3:006.354

ОКС 35.020

Ключевые слова: критическая информационная инфраструктура, доверенные программно-аппаратные комплексы, программное обеспечение, общие положения

Редактор *Е.В. Якубова*
Технический редактор *В.Н. Прусакова*
Корректор *Р.А. Ментова*
Компьютерная верстка *И.Ю. Литовкиной*

Сдано в набор 27.06.2025. Подписано в печать 01.07.2025. Формат 60×84%. Гарнитура Ариал.
Усл. печ. л. 0,93. Уч.-изд. л. 0,68.

Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

Создано в единичном исполнении в ФГБУ «Институт стандартизации»
для комплектования Федерального информационного фонда стандартов,
117418 Москва, Нахимовский пр-т, д. 31, к. 2.
www.gostinfo.ru info@gostinfo.ru