ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ
(ФСТЭК России)

П Р И К А З

« » июля 2026 г. Москва № _____

Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных

В соответствии с частью 4 статьи 19 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных», пунктом 2 и подпунктом 9^1 пункта 8 Положения о Федеральной службе по техническому и экспортному контролю, утвержденного Указом Президента Российской Федерации от 16 августа 2004 г. № 1085, **П Р И К А З Ы В А Ю:**

1. Утвердить прилагаемые Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных.

2. Признать утратившими силу:

приказ ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» (зарегистрирован Минюстом России 14 мая 2013 г., регистрационный № 28375);

пункт 1 приложения к приказу ФСТЭК России от 23 марта 2017 г. № 49 «О внесении изменений в Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденные приказом Федеральной службы по техническому и экспортному контролю от 18 февраля 2013 г. № 21, и в Требования к обеспечению защиты

информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды, утвержденные приказом Федеральной службы по техническому и экспортному контролю от 14 марта 2014 г. № 31» (зарегистрирован Минюстом России 25 апреля 2017 г., регистрационный № 46487);

приказ ФСТЭК России от 14 мая 2020 г. № 68 «О внесении изменений в Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденные приказом Федеральной службы по техническому и экспортному контролю от 18 февраля 2013 г. № 21» (зарегистрирован Минюстом России 8 июля 2020 г., регистрационный № 58877).

3. Настоящий приказ вступает в силу с 1 сентября 2026 г.

ДИРЕКТОР ФЕДЕРАЛЬНОЙ СЛУЖБЫ
ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ

В.СЕЛИН

УТВЕРЖДЕННЫЕ
приказом ФСТЭК России
от ____ июля 2026 г. № ____

Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных

I. Общие положения

1. Настоящий документ определяет состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных (далее — меры по обеспечению безопасности персональных данных) для каждого из уровней защищенности персональных данных, установленных в Требованиях к защите персональных данных при их обработке в информационных системах персональных данных, утвержденных постановлением Правительства Российской Федерации от 1 ноября 2012 г. № 1119 (далее — Требования к защите персональных данных).

Меры по обеспечению безопасности персональных данных принимаются для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

2. При обработке в информационных системах персональных данных, содержащих сведения, составляющие государственную тайну, их защита обеспечивается в соответствии с требованиями по технической защите информации, содержащей сведения, составляющие государственную тайну[1].

3. При обработке информации, содержащей персональные данные, в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений применяются Требования к защите персональных данных и Требования о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных

[1] Подпункт 9[1] пункта 8 Положения о Федеральной службе по техническому и экспортному контролю, утвержденного Указом Президента Российской Федерации от 16 августа 2004 г. № 1085 (далее — Положение о ФСТЭК России).

органов, государственных унитарных предприятий, государственных учреждений, утвержденные приказом ФСТЭК России от 11 апреля 2025 г. № 117[2].

4. В случае если информационная система персональных данных является значимым объектом критической информационной инфраструктуры Российской Федерации, защита содержащейся в ней информации обеспечивается в соответствии с нормативными правовыми актами, принятыми на основании статьи 6 Федерального закона от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», и Требованиями к защите персональных данных.

5. В случае использования для защиты информации, содержащейся в информационных системах персональных данных, шифровальных (криптографических) средств защиты информации применяются требования о защите информации, установленные ФСБ России в соответствии с частью 4 статьи 19 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

6. Безопасность персональных данных при их обработке в информационной системе персональных данных (далее - информационная система) обеспечивает оператор или лицо, осуществляющее обработку персональных данных по поручению оператора в соответствии с законодательством Российской Федерации.

Для выполнения работ и услуг по обеспечению безопасности персональных данных при их обработке в информационной системе в соответствии с законодательством Российской Федерации могут привлекаться юридическое лицо или индивидуальный предприниматель, имеющие лицензию на деятельность по технической защите конфиденциальной информации.

7. Меры по обеспечению безопасности персональных данных реализуются в рамках системы защиты персональных данных, создаваемой в соответствии с Требованиями к защите персональных данных и должны быть направлены на нейтрализацию актуальных угроз безопасности персональных данных.

Определение актуальных угроз безопасности персональных данных осуществляется оператором с учетом архитектуры информационной системы, применяемых информационных технологий, особенностей функционирования информационной системы.

Решение о необходимости разработки модели угроз безопасности информации в ходе создания информационной системы принимается оператором. При разработке модели угроз безопасности персональных данных используются методические

---

[2] Зарегистрирован Минюстом России 16 июня 2025 г., регистрационный № 82619.

документы, утвержденные ФСТЭК России в соответствии с абзацем вторым пункта 5 и подпунктом 4 пункта 8 Положения о ФСТЭК России (далее — методические документы ФСТЭК России).

8. Меры по обеспечению безопасности персональных данных реализуются в том числе посредством применения в информационной системе средств защиты информации, прошедших в установленном порядке процедуру оценки соответствия, в случаях, когда применение таких средств необходимо для нейтрализации актуальных угроз безопасности персональных данных.

9. Оценка эффективности реализованных мер по обеспечению безопасности персональных данных проводится оператором самостоятельно или с привлечением юридических лиц или индивидуальных предпринимателей, имеющих лицензию на осуществление деятельности по технической защите конфиденциальной информации. В этих целях определяется показатель, который характеризует достаточность и эффективность реализованных мер по обеспечению безопасности персональных данных (показатель уровня зрелости $У_{зи}$), в соответствии с методическими документами ФСТЭК России. Указанная оценка проводится перед началом обработки персональных данных и далее не реже одного раза в 3 года, а также после компьютерного инцидента, произошедшего у оператора.

10. Оператором информационной системы в отношении лица, осуществляющего обработку персональных данных по поручению оператора в соответствии с законодательством Российской Федерации, устанавливается требование к значению показателя уровня зрелости $У_{зи,}$ оценка которого проводится перед началом обработки персональных данных и далее не реже одного раза в 3 года, а также после компьютерного инцидента, произошедшего у лица, осуществляющего обработку персональных данных по поручению оператора.

II. Состав и содержание мер по обеспечению безопасности персональных данных

11. Для обеспечения безопасности персональных данных при их обработке в информационных системах оператором реализуются:

выявление и оценка угроз безопасности информации;

контроль конфигураций информационных систем;

управление уязвимостями;

управление обновлениями;

защита информации при обработке, хранении и обращении с информацией, доступ к которой ограничен в соответствии с законодательством Российской Федерации;

защита информации при применении конечных устройств;

защита информации при применении мобильных устройств;

защита информации при удаленном доступе пользователей к информационным системам;

защита информации при беспроводном доступе пользователей к информационным системам;

защита информации при предоставлении пользователям доступа к информационным системам, предусматривающего чтение, выполнение, изменение, запись, удаление программ и (или) данных в информационных системах;

мониторинг информационной безопасности;

разработка безопасного программного обеспечения;

физическая защита информационных систем;

непрерывное функционирование информационных систем при возникновении нештатных ситуаций;

повышение уровня знаний и информированности пользователей по вопросам защиты информации;

защита информации при взаимодействии с подрядными организациями;

защита от компьютерных атак, направленных на отказ в обслуживании;

защита информации при использовании искусственного интеллекта;

меры по обеспечению безопасности персональных данных;

проведение контроля уровня защищенности персональных данных, содержащейся в информационных системах;

непрерывное взаимодействие с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации.

12. В информационных системах реализуются следующие меры по обеспечению безопасности персональных данных:

идентификация и аутентификация;

управление доступом;

регистрация событий безопасности;

защита виртуализации и облачных вычислений;

защита технологий контейнерных сред и их оркестрации;

защита сервисов электронной почты;

защита веб-технологий;

защита программных интерфейсов взаимодействия приложений;

защита конечных устройств;

защита мобильных устройств;

защита технологий интернета вещей[3];

защита точек беспроводного доступа;

антивирусная защита;

обнаружение и предотвращение вторжений на сетевом уровне;

сегментация и межсетевое экранирование;

защита от компьютерных атак, направленных на отказ в обслуживании;

защита каналов передачи данных и сетевого взаимодействия.

Состав мер по обеспечению безопасности персональных данных, необходимых для обеспечения их защиты от актуальных угроз безопасности персональных данных с учетом объема обрабатываемых персональных данных и их категории, устанавливается оператором в политике в отношении обработки персональных данных[4].

Содержание мер по обеспечению безопасности персональных данных, необходимых для обеспечения каждого из уровней защищенности персональных данных, определяется оператором с учетом применяемых информационных технологий с использованием методических документов ФСТЭК России.

13. Выбор мер по обеспечению безопасности персональных данных, подлежащих реализации в информационной системе в рамках системы защиты персональных данных, включает:

определение в информационных системах базовых мер по обеспечению безопасности персональных данных для установленного уровня защищенности персональных данных;

адаптацию базовых мер по обеспечению безопасности персональных данных применительно к архитектуре информационных систем, применяемым информационным технологиям, особенностям функционирования информационных систем;

верификацию адаптированных базовых мер по обеспечению безопасности персональных данных в соответствии с актуальными угрозами и возможностями нарушителей, их дополнение и (или) усиление.

14. При невозможности технической реализации отдельных выбранных мер по обеспечению безопасности персональных данных, а также с учетом экономической целесообразности на этапах адаптации базового набора мер и (или) верификации

---

[3] Подпункт «в» пункта 4 Стратегии развития информационного общества в Российской Федерации на 2017 — 2030 годы, утвержденной Указом Президента Российской Федерации от 9 мая 2017 г. № 203.

[4] Пункт 2 части 1 статьи 18.1 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

адаптированного базового набора мер могут разрабатываться иные (компенсирующие) меры, направленные на нейтрализацию актуальных угроз безопасности персональных данных.

В этом случае в ходе разработки системы защиты персональных данных должно быть проведено обоснование применения компенсирующих мер для обеспечения безопасности персональных данных.

15. В случае определения в соответствии с Требованиями к защите персональных в качестве актуальных угроз безопасности персональных данных 1-го и 2-го типов дополнительно к мерам по обеспечению безопасности персональных данных, указанным в пункте 8 настоящего документа, могут применяться следующие меры:

проверка системного и (или) прикладного программного обеспечения, включая программный код, на отсутствие уязвимостей и недекларированных возможностей с использованием автоматизированных средств и (или) без использования таковых в соответствии с методическими документами ФСТЭК России;

использование в информационной системе системного и (или) прикладного программного обеспечения, разработанного с учетом мер по разработке безопасного программного обеспечения[5].

16. Технические меры защиты персональных данных реализуются посредством применения средств защиты информации, в том числе программных (программно-аппаратных) средств, в которых они реализованы, имеющих необходимые функции безопасности.

При использовании в информационных системах сертифицированных по требованиям безопасности информации средств защиты информации:

в информационных системах 1 уровня защищенности персональных данных применяются средства защиты информации не ниже 4 класса и 4 уровня доверия;

в информационных системах 2 уровня защищенности персональных данных применяются средства защиты информации не ниже 5 класса и 5 уровня доверия;

в информационных системах 3 уровня защищенности персональных данных применяются средства защиты информации 6 класса и 6 уровня доверия;

в информационных системах 4 уровня защищенности персональных данных применяются средства защиты информации 6 класса и 6 уровня доверия.

---

[5] Пункты 4.1-5.25 национального стандарта Российской Федерации ГОСТ Р 56939-2024 «Защита информации. Разработка безопасного программного обеспечения. Общие требования», утвержденного и введенного в действие приказом Госстандарта от 24 октября 2024 г. № 1504-ст (М., ФГБУ «РСТ», 2024).

Классы защиты определяются в соответствии с нормативными правовыми актами, изданными в соответствии с подпунктом 13.1 пункта 8 Положения о ФСТЭК России.

Уровни доверия устанавливаются в соответствии с Требованиями по безопасности информации, устанавливающими уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий, утвержденными приказом ФСТЭК России от 2 июня 2020 г. № 76[6].

17. При использовании в информационных системах новых информационных технологий и выявлении дополнительных угроз безопасности персональных данных, для которых не определены меры обеспечения их безопасности, должны разрабатываться компенсирующие меры в соответствии с пунктом 10 настоящего документа.

18. На стадиях жизненного цикла информационных систем меры по обеспечению безопасности персональных данных принимаются оператором в соответствии с национальным стандартом Российской Федерации ГОСТ Р 51583-2014[7].

---

[6] Зарегистрирован Минюстом России 11 сентября 2020 г., регистрационный № 59772, с изменениями, внесенными приказом ФСТЭК России от 18 апреля 2022 г. № 68 (зарегистрирован Минюстом России 20 июля 2022 г., регистрационный № 69318).

[7] Пункты 5.1-5.26 национального стандарта Российской Федерации ГОСТ Р 51583-2014 «Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие требования», утвержденный и введенный в действие приказом Росстандарта от 28 января 2014 г. № 3-ст (М., ФГУП «Стандартинформ», 2014).