Проект

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ
(ФСТЭК России)

П Р И К А З

« » августа 2026 г. Москва № _____

О внесении изменений в Требования о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений, утвержденные приказом Федеральной службы по техническому и экспортному контролю от 11 апреля 2025 г. № 117

В соответствии с частью 5 статьи 16 Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», 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. Внести в Требования о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений, утвержденные приказом Федеральной службы по техническому и экспортному контролю от 11 апреля 2025 г. № 117 (зарегистрирован Минюстом России 16 июня 2025 г., регистрационный № 82619), изменения согласно приложению к настоящему приказу.

2. Настоящий приказ вступает в силу с 1 марта 2027 г.

ДИРЕКТОР ФЕДЕРАЛЬНОЙ СЛУЖБЫ
ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ

В.СЕЛИН

ПРИЛОЖЕНИЕ
к приказу ФСТЭК России
от ____ августа 2026 г. №___

ИЗМЕНЕНИЯ,
которые вносятся в Требования о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений, утвержденные приказом ФСТЭК России от 11 апреля 2025 г. № 117

1. Подпункт «д» пункта 14 дополнить абзацем следующего содержания:

«порядок защиты информации при использовании искусственного интеллекта;».

2. В абзаце третьем пункта 49 слово «доверенных» исключить.

3. В сноске 17 к третьему абзацу пункта 49 слова «Подпункт «ц» заменить словами «Подпункт «а».

4. Пункт 60 изложить в следующей редакции:

«60. Посредством проведения мероприятий по обеспечению защиты информации при использовании для функционирования информационных систем искусственного интеллекта[20] должна быть обеспечена возможность исключения несанкционированного доступа к информации или воздействия на информационные системы, несанкционированного распространения и модификации информации, а также использования информационных систем
не по их назначению за счет воздействия на применяемые модели искусственного интеллекта[22] и их параметры[23], агенты искусственного интеллекта[24].

При применении моделей искусственного интеллекта оператором (обладателем информации) информационной системы должны быть реализованы мероприятия и меры защиты информации в соответствии с настоящими Требованиями, в том числе выделение моделей искусственного интеллекта

в отдельный сегмент информационной системы или информационно-телекоммуникационной инфраструктуры, если информационная система функционирует на базе информационно-телекоммуникационной инфраструктуры (далее – выделенный сегмент).

Привилегированный доступ пользователей в выделенный сегмент доложен осуществляться с использованием усиленной многофакторной аутентификации.

В выделенном сегменте должен быть реализован контроль доступа пользователей к моделям искусственного интеллекта и наделение их минимальными правами доступа, необходимыми для выполнения возложенных на пользователей функций.

Проводимые мероприятия должны включать регистрацию и анализ действий пользователей при доступе в выделенный сегмент.

В случае применения моделей искусственного интеллекта для обработки информации ограниченного доступа и (или) для реализации значимых функций оператора (обладателя информации) информационной системы дополнительно должны быть реализованы следующие меры:

контроль доступа пользователей к моделям искусственного интеллекта;

фильтрация входных данных (запросов) и выходных данных (ответов) моделей искусственного интеллекта;

квотирование (ограничение) количества входных данных (запросов) пользователей к моделям искусственного интеллекта;

ограничение и контроль функциональности моделей искусственного интеллекта.

Реализация мер защиты информации моделей искусственного интеллекта обеспечивается путем применения программного обеспечения, входящего
в состав информационной системы, и (или) отдельных средств защиты моделей искусственного интеллекта.».

5. Сноску 20 к первому абзацу пункта 60 изложить в следующей редакции:

«[20] Пункт 1 статьи 3 Федерального закона от 26 июля 2026 г. № 243-ФЗ «О поддержке развития технологий искусственного интеллекта в Российской Федерации».».

6. Сноску 21 к первому абзацу пункта 60 исключить.

7. Сноску 24 к первому абзацу пункта 60 изложить в следующей редакции:

«[24] Пункт 3.1.1 национального стандарта Российской Федерации ГОСТ Р 71476-2024 «Искусственный интеллект. Концепции и терминология искусственного интеллекта», введенного в действие приказом Росстандарта от 28 октября 2024 г. № 1550-ст.».

8. Пункт 61 изложить в следующей редакции:

«61. При применении агентов искусственного интеллекта, в том числе автономных агентов искусственного интеллекта, оператором (обладателем информации) информационной системы должны быть приняты меры защиты информации, направленные на предотвращение несанкционированного воздействия на ресурсы информационной системы, а также контроль и управление правами доступа агентов в соответствии с внутренними стандартами и регламентами по защите информации.

При использовании в информационных системах сервисов на основе моделей искусственного интеллекта осуществляемые подрядной организацией мероприятия и меры защиты информации устанавливаются во внутренних стандартах и регламентах по защите информации.».

9. Сноску 25 к одиннадцатому абзацу пункта 61 исключить.