ФСТЭК РОССИИ

УПРАВЛЕНИЕ
ФЕДЕРАЛЬНОЙ СЛУЖБЫ
ПО ТЕХНИЧЕСКОМУ
И ЭКСПОРТНОМУ КОНТРОЛЮ
ПО ЦЕНТРАЛЬНОМУ
ФЕДЕРАЛЬНОМУ ОКРУГУ

Севастопольский пр-кт, д. 56/40, стр. 1, Москва, 117342
Тел.: (495) 334-42-47; тел./факс: (495) 334-16-21
e-mail: cfo@fstec.ru

26.08.2026 № 2916/10

На № _____ от _____

Губернатору
Московской области
А.Ю.ВОРОБЬЁВУ

Строителей бул., д. 1,
г. Красногорск-7, Московская обл.,
143407

О защите информации при использовании моделей искусственного интеллекта

Уважаемый Андрей Юрьевич!

В настоящее время органы исполнительной власти в целях улучшения качества и эффективности деятельности при создании государственных и иных информационных систем используют (планируют к использованию) технологии искусственного интеллекта, в том числе большие фундаментальные модели искусственного интеллекта (далее — модели искусственного интеллекта).

Учитывая, что применение моделей искусственного интеллекта создает дополнительные угрозы безопасности информации, связанные с возможностью нарушения функционирования информационных систем и утечки содержащейся в них информации, ФСТЭК России подготовлены рекомендации по защите информации при использовании моделей искусственного интеллекта (далее — рекомендации).

Прошу Ваших указаний соответствующим должностным лицам о направлении копий рекомендаций в органы государственной власти субъекта Российской Федерации, государственные организации (учреждения), подведомственные органам государственной власти.

О проделанной работе прошу письменно проинформировать Управление ФСТЭК России по Центральному федеральному округу. В письменном информировании необходимо указать наименования органов государственной власти и государственных организаций (учреждений), подведомственных органам государственной власти, в которые направлены копии рекомендаций.

С уважением,

Исполняющий обязанности руководителя В.Сульдин

Руководство Московской области
ВХ-25753
03.09.2026
Правительство Московской области

Приложение: 1. Копия рекомендаций ФСТЭК России «О защите информации при использовании моделей искусственного интеллекта», к вх. № 9408, в 1 экз., на 3 л., только в адрес.

Кузнецов М.А.
(495) 334-16-93

0036510

Правительство Московской области

КОПИЯ

Рекомендации ФСТЭК России «О защите информации при использовании моделей искусственного интеллекта»

В настоящее время федеральные органы исполнительной власти в целях улучшения качества и эффективности деятельности при создании государственных и иных информационных систем используют (планируют к использованию) технологии искусственного интеллекта, в том числе большие фундаментальные модели искусственного интеллекта (далее - модели искусственного интеллекта).

Применение моделей искусственного интеллекта в информационных системах государственных органов наряду с положительными эффектами создает дополнительные угрозы безопасности информации, связанные с возможностью нарушения функционирования информационных систем и утечки содержащейся в них информации.

Противодействие указанным угрозам безопасности информации осуществляется в рамках общих подходов по защите информации, определенных в соответствии с Требованиями о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений, утвержденными приказом ФСТЭК России от 11 апреля 2025 г. № 2026 г. № 117.

В рамках реализации данного подхода для обеспечения защиты информации моделей искусственного интеллекта применимы стандартные мероприятия и меры защиты информации, реализуемые в рамках системы защиты информации информационных систем.

При этом применение моделей искусственного интеллекта в информационных системах обуславливает появление дополнительных объектов защиты информации, включающих: модели искусственного интеллекта, их параметры и расширения (при размещении моделей искусственного интеллекта в информационной системе); агенты искусственного интеллекта, в том числе автономные агенты искусственного интеллекта; сервисы на основе моделей искусственного интеллекта, предоставляемые подрядными организациями.

В этой связи при создании и проектировании информационных систем должна быть проведена оценка угроз безопасности информации, связанных с применением моделей искусственного интеллекта. Сведения об угрозах безопасности информации моделей искусственного интеллекта содержатся в разделе банка данных угроз безопасности информации ФСТЭК России «Угрозы ИИ» (bdu.fstec.ru/threat/ai).

Правительство Московской области

По результатам оценки угроз безопасности информации в техническое задание включаются требования к реализации в информационной системе мер защиты информации, направленных на нейтрализацию указанных угроз.

При формировании требований к реализации мер защиты информации моделей искусственного интеллекта рекомендуется: выделить модели искусственного интеллекта в отдельный сегмент информационной системы или информационно-телекоммуникационной инфраструктуры, если информационная система функционирует на базе информационно-телекоммуникационной инфраструктуры (далее - выделенный сегмент);

обеспечить привилегированный доступ пользователей в выделенный сегмент с использованием усиленной многофакторной аутентификации; реализовать контроль доступа пользователей к моделям искусственного интеллекта и наделение их минимальными правами доступа, необходимыми для выполнения возложенных на пользователей функций; обеспечить 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 рекомендуется реализовать следующие меры: контроль доступа пользователей к моделям искусственного интеллекта; фильтрацию 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.

При применении агентов искусственного интеллекта, в том числе автономных агентов искусственного интеллекта, операторам рекомендуется принять меры защиты информации, направленные на предотвращение несанкционированного воздействия на ресурсы информационной системы, а также контроль и управление правами доступа агентов, в том числе включающие: наделение агентов искусственного интеллекта минимальными правами доступа, необходимыми для решения задач; управление доступом агентов искусственного интеллекта к программным, программно-аппаратным средствам информационных систем и содержащейся в них информации;

КОПИЯ ВЕРНА
подпись

Правительство Московской области

выделение агентов искусственного интеллекта в отдельный сегмент информационной системы; защиту программных интерфейсов взаимодействия агентов искусственного интеллекта;

обеспечение контроля конфигурации агентов искусственного интеллекта; мониторинг действий агентов искусственного интеллекта; подтверждение оператором выполнения агентами искусственного интеллекта значимых функций.

Эффективность реализации мер защиты информации, направленных на нейтрализацию угроз безопасности информации моделей искусственного интеллекта, оценивается в ходе проведения аттестационных испытаний (оценки эффективности принятых мер защиты информации).

При использовании в информационных системах сервисов на основе моделей искусственного интеллекта операторам рекомендуется установить в отношении подрядной организации требования о необходимости реализации мероприятий и мер защиты информации моделей искусственного интеллекта, установленных Требованиями о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений, утвержденными приказом ФСТЭК России от 11 апреля 2025 г. 2026 г. № 117, внутренними стандартами и регламентами, а также настоящими рекомендациями.

К вх. № 9408
Управление [illegible] службы
по техническому [illegible] контролю
по Центр[illegible]

Управление Федеральной службы по техническому и экспортному контролю по Центральному федеральному округу
отдел документационного обеспечения
(ФСТЭК России)

КОПИЯ ВЕРНА
подпись

Правительство Московской области