o2 consulting

Поднимайтесь выше всех
Мы будем рядом

Приказ ФСТЭК № 117:

Что нужно знать об изменениях с 01.03.2026, в том числе разработчикам ИИ-решений для госсектора

Материал актуален
по состоянию на 25.03.2026

С 1 марта 2026 вступил в силу Приказ Федеральной службы по техническому и экспортному контролю России от 11.04.2025 № 117 «Об утверждении Требований о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений» (далее – Приказ ФСТЭК № 117), который существенно меняет подход к обеспечению безопасности государственных информационных систем (далее – ГИС).

Приказ ФСТЭК № 117 заменяет Приказ № 17 от 11.02.2013 г., распространяя требования на более широкий круг систем, вводя иную модель управления информационной безопасностью (далее – ИБ).

Впервые в акте ФСТЭК закреплены прямые требования к использованию систем искусственного интеллекта (далее – ИИ). Приказ №117 — первый нормативный акт ФСТЭК, детально регламентирующий использование ИИ в сфере ИБ. Ключевые требования сформулированы в пунктах 60 и 61 документа.

- Защита данных ГИС. При использовании ИИ необходимо обеспечить защиту от несанкционированного доступа к данным, от вмешательства в работу систем и от нецелевого использования. Кроме того, запрещено использовать конфиденциальные данные из госсистем для обучения и дообучения моделей.

- Контроль взаимодействия пользователей с ИИ. Варианты коммуникации между пользователем и ИИ должны закладываться ещё на этапе разработки. Это включает: при фиксированных сценариях — заранее определённые шаблоны допустимых вопросов и ответов; при свободном вводе — необходимость заранее задать запрещённые темы и форматы ответов, а система обязана фильтровать нарушения. Ошибки должны фиксироваться и анализироваться. Должен быть установлен запрет на автономное изменение параметров работы системы со стороны ИИ без подтверждения.

- Запрет на облачные ИИ-сервисы для защищенной информации. Приказ установил прямой запрет на использование облачных ИИ-сервисов для обработки данных, составляющих гостайну, или информации ограниченного доступа в мониторинге ИБ. Допускается использование доверенных технологий искусственного интеллекта для анализа событий безопасности, но при этом мониторинг должен быть непрерывным и осуществляться квалифицированным персоналом.

1. Расширение сферы действия

Новое регулирование закрепляет более широкий перечень лиц, на которых распространяются требования по защите информации.

Теперь они действуют не только в отношении операторов государственных и муниципальных информационных систем, но также в отношении:

- государственных и муниципальных органов;
- государственных учреждений и государственных унитарных предприятий;
- иных информационных систем органов власти;
- организаций, которые получают, обрабатывают либо используют информацию из государственных информационных систем.

Таким образом, требования применяются и к тем лицам, которые формально не являются операторами государственных информационных систем, но осуществляют взаимодействие с такими системами или обрабатываемой в них информацией, что существенно расширяет регуляторный периметр и повышает требования к участникам соответствующей инфраструктуры.

2. Переход к циклической модели управления защитой информации

Приказ № 117 закрепляет **обязанность оператора выстраивать управление защитой информации** в рамках единой организационной системы, возглавляемой руководителем организации либо назначенным им ответственным лицом.

Управление защитой информации в явном виде увязывается с циклом процессов, включающих:

- разработку и планирование мероприятий и мер по защите информации;
- реализацию и проведение соответствующих мероприятий и мер;
- оценку состояния (эффективности) защиты информации;
- последующее совершенствование применяемых мероприятий и мер.

По сути, закрепляется процессный подход к ИБ, близкий к модели постоянного улучшения (по типу PDCA), который ориентирован на регулярную переоценку и адаптацию системы защиты к изменению технологий и актуальных угроз.

3. Организационное закрепление функции по защите информации

Новая редакция требований уточняет и усиливает обязанность оператора формализовать функцию по защите информации на организационном уровне. Руководитель оператора (либо уполномоченное им ответственное лицо) должен предусмотреть создание (определение) специализированного структурного подразделения либо назначение отдельных специалистов, на которых прямо возлагаются обязанности по защите информации.

Фактически это означает, что:

- функция по защите информации должна быть институционализирована (через подразделение или назначенных специалистов), а не исполняться «по совместительству» без надлежащего закрепления;
- распределение обязанностей и ответственности за защиту информации подлежит формализации в организационных и локальных нормативных актах оператора.

4. Новые требования к квалификации персонала

Приказ № 117 конкретизирует требования к компетенциям работников, отвечающих за защиту информации. Вводится обязательное требование, согласно которому **не менее 30%** сотрудников специализированного подразделения по защите информации должны иметь профессиональное образование в области ИБ либо пройти программу профессиональной переподготовки.

Фактически это обязывает организации:

- **переоценить кадровый состав** и структуру подразделений, отвечающих за защиту информации;
- **организовать дополнительное обучение** и профессиональную переподготовку действующих сотрудников;
- **планировать формирование кадрового резерва** с учетом указанных квалификационных критериев.

5. Сроки реагирования на уязвимости

Приказ № 117 устанавливает конкретные сроки устранения уязвимостей:

- для критических уязвимостей – не более **24 часов;**
- для уязвимостей высокого уровня опасности – не более **7 календарных дней;**
- для средних и низких уровней – в порядке и сроки, закрепленные во внутренних регламентах оператора.

При выявлении уязвимостей, отсутствующих в банке данных угроз ФСТЭК России, оператор обязан в **течение 5 рабочих дней** направить сведения о такой уязвимости в ФСТЭК России, что требует формализованного процесса управления уязвимостями.

6. Обязательная передача показателей

Приказ № 117 вводит регулярную оценку **двух** ключевых показателей:

- показателя **защищенности Кзи** (не реже одного раза в **6** месяцев);
- показателя уровня **зрелости Пзи** (не реже одного раза в **2** года).

Результаты расчетов Кзи и Пзи подлежат направлению во ФСТЭК России не позднее **5** рабочих дней со дня их расчета, что фактически формирует новый для операторов обязательный контур отчетности перед регулятором по состоянию технической защиты информации и эффективности принимаемых мер.

7. Усиление требований к подрядным организациям

Приказ № 117 вводит прямые обязанности для подрядных организаций, которым предоставляется доступ к информационным системам оператора и (или) содержащейся в них информации.

Такие организации подлежат ознакомлению с политикой защиты информации оператора в относящейся к ним части, а обязанность соблюдения политики, внутренних стандартов и регламентов по защите информации должна быть прямо закреплена в договорах, технических заданиях и иных документах, на основании которых передается информация или предоставляется доступ.

При привлечении подрядчика к разработке программного обеспечения по решению руководителя в техническое задание могут включаться требования по разработке безопасного программного обеспечения в соответствии с **ГОСТ Р 56939 2024**, что формирует для операторов и подрядчиков дополнительный нормативный ориентир в части безопасной разработки.

8. Изменение подхода к выбору мер защиты

В отличие от Приказа № 17, новый Приказ № 117 не содержит привычной итоговой таблицы базовых мер по классам защищенности, а **опирается на концепцию системы управления защитой информации и оценку ее зрелости.**

Требования структурированы вокруг набора обязательных мероприятий и процессов, а формирование конкретного набора технических и организационных мер осуществляется оператором с учетом архитектуры информационных систем, актуальных угроз и принимаемой модели рисков.

При этом сохраняется обязательность использования сертифицированных средств защиты информации и криптографических средств, соответствующих требованиям ФСТЭК и ФСБ России, что ограничивает возможность применения «не стандартизированных» решений даже при более гибком, процессном подходе к построению системы защиты.

Потенциальные преимущества нового регулирования

При надлежащем внедрении новый приказ может обеспечить для организаций ряд **долгосрочных эффектов**, в том числе:

- **унификацию требований** к защите информации во всех государственных и приравненных к ним информационных системах, снижение регуляторной неопределенности;
- **повышение качества** и предсказуемости процессов защиты информации за счет перехода к процессной, циклической модели управления;
- **сокращение времени** реагирования на критические уязвимости и инциденты, снижение вероятности крупных сбоев и репутационных потерь;
- **стимулирование развития** внутренней экспертизы по ИБ и роста зрелости ИБ функции в целом.

Основные риски и вызовы для организаций

Исполнение новых требований может сопровождаться существенными организационными и финансовыми **нагрузками**, в том числе:

- **ростом совокупных затрат** на создание и поддержание системы защиты информации (кадры, процессы, средства защиты, отчетность);
- **необходимостью доукомплектования штатного состава** и (или) существенной переподготовки существующих сотрудников, отвечающих за защиту информации;
- **увеличением объемов и сложности обязательной отчетности,** в том числе по показателям защищенности и зрелости;
- **необходимостью переработки значительной части внутренней документации и договорной базы** с подрядчиками, а также перестройки устоявшихся практик взаимодействия.

Рекомендации

С учетом того, что приказ уже действует, целесообразно сфокусироваться на следующих шагах:

- **определить перечень затронутых информационных систем** и формально закрепить ответственных за их защиту;
- **проверить и при необходимости обновить** политики, регламенты и договоры с подрядчиками под новые требования;
- **формализовать цикл** управления защитой информации (планирование, реализация, оценка, улучшение);
- **настроить процесс управления** уязвимостями с учетом установленных сроков и обязанностей по уведомлению;
- **обеспечить регулярный расчет показателей** защищенности и зрелости и их направление регулятору;
- **оценить кадровый состав** ИБ функции и спланировать переподготовку/набор для выполнения 30-процентного требования.

Кроме того, следует учитывать, что аттестаты соответствия на государственные и иные информационные системы, выданные до **1 марта 2026 г.,** продолжают действовать, но при их продлении и переаттестации потребуется соблюдение новых требований.

Заказчики в госсекторе уже приходят с конкретными вопросами: можно ли сохранить текущую архитектуру, чем заменить внешние сервисы, как организовать проверку ответов модели и кто несёт ответственность за ошибки. **Разработчикам и интеграторам ИИ-решений теперь недостаточно просто создать работоспособный алгоритм — нужно пересматривать архитектуру решений для соответствия требованиям ФСТЭК.** Выполнение мер по ИБ становится обязательным условием договоров с подрядчиками. При этом стоит учитывать, что методик, разъясняющих техническую реализацию требований, пока нет, и параллельно развивается нормативная база через отраслевые ГОСТы — например, уже опубликован ПНСТ 1046-2026 от 30.01.2026 по ИИ в критической информационной инфраструктуре.

Наша компания оказывает услуги по правовому и организационному сопровождению исполнения новых требований, включая аудит, актуализацию документов и **поддержку проектов по выстраиванию процессов защиты информации и регуляторного комплаенса для ИТ и решений на базе искусственного интеллекта.**

o2 consulting

Софья Смирнова

Советник M&A и корпоративной практики, Директор по цифровой трансформации

Направление AI & Legal Tech

Дарья Носова

Партнер и руководитель практики цифрового права и интеллектуальной собственности

Направление AI & Legal Tech

o2consult.com

ss@o2consult.com

+7 (499) 288 05 55

@O2ConsultingTeam

канал Софьи
про AI и M&A