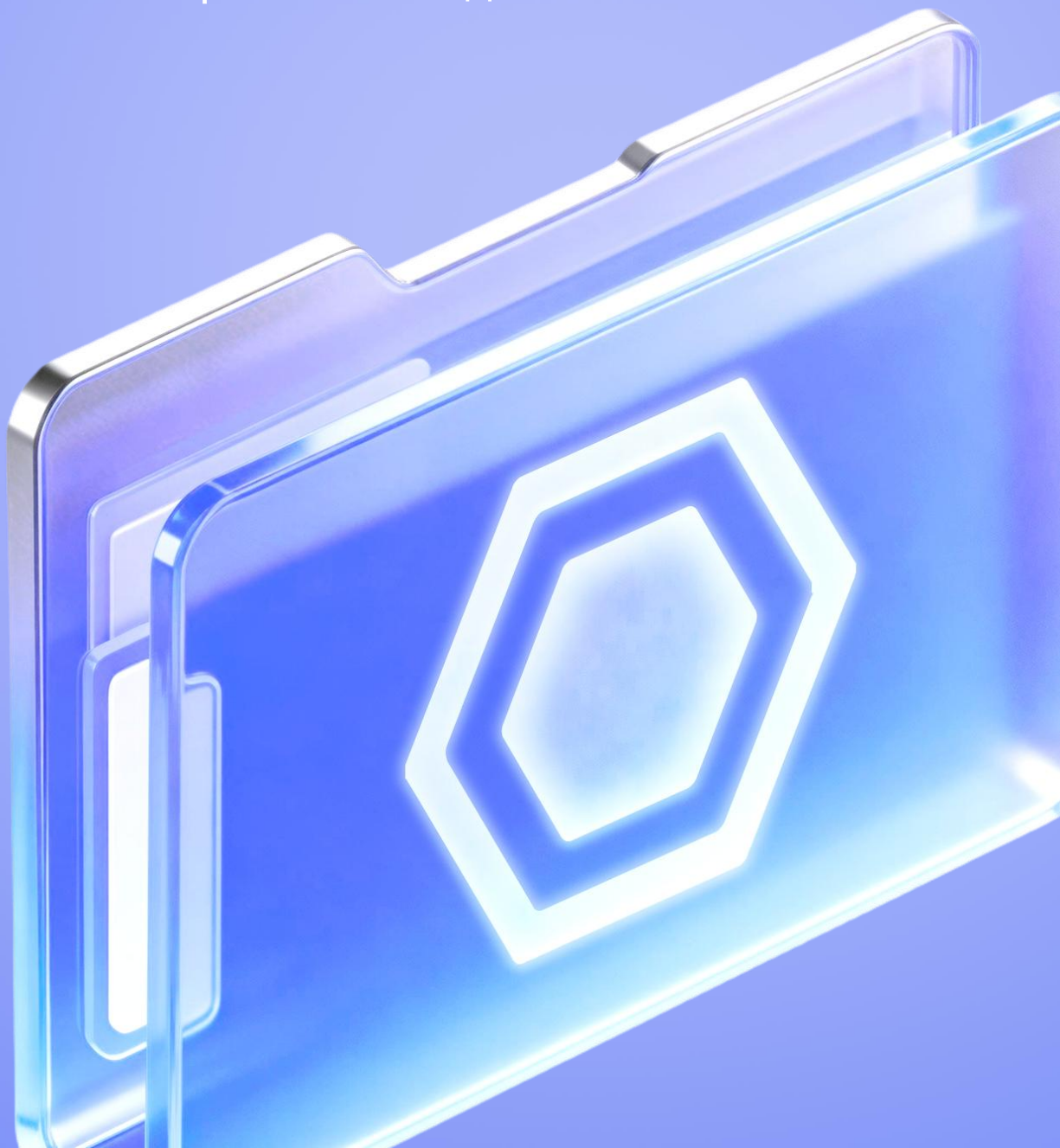
Кросстех

Регуляторный патч

Дайджест изменений законодательства
в сфере ИБ за 1 квартал 2026 года



2026

Кросстех

Вступительное слово



Законодательство в сфере ИБ стремительно меняется. Мы разработали этот дайджест, чтобы владельцы бизнеса, руководители, эксперты по ИБ и юристы могли перевести строки законов и стандартов в практическую плоскость.

В дайджесте вы найдете анализ изменений и рекомендованные шаги для повышения защищенности бизнеса.

Катерина Сашенко,
Директор департамента аудита, консалтинга и оценки соответствия Кросс технолоджис

СОДЕРЖАНИЕ

ФСТЭК представила проект методики по защите ГИС и не только 03

ФСТЭК рассказала, каким рекомендациям следовать, пока новая методика защиты ГИС не принята 04

Ужесточаются требования к лицензированию деятельности по технической защите конфиденциальной информации (ТЗКИ) 06

ИИ получит регулирование – опубликован проект профильного федерального закона 09

Опубликована предварительная версия стандарта по использованию ИИ и в КИИ 11

Кросстех

ФСТЭК представила проект методики по защите ГИС и не только

Мероприятия и меры по защите информации, содержащейся в информационных системах

Открыть документ

Для кого актуально

Для государственных органов, государственных унитарных предприятий, государственных и муниципальных учреждений.

Ведомство выпустило проект методического документа в феврале. Предполагалось, что он вступит в действие уже в марте, но итоговая версия пока не опубликована.



«Регулятор предлагает более комплексный подход к реализации систем защиты информации, делает упор не только на использование механизмов безопасности, но и выстраивание зрелых процессов обеспечения защиты информации. Это позволит ИБ идти в ногу со временем и отвечать на вызовы, связанные с расширением сервисов электронных услуг».

Катерина Сашенко,
Директор департамента аудита, консалтинга и оценки соответствия Кросс технолоджис

Детали

1. Ожидалось, что методический документ будет продолжением приказа ФСТЭК России № 117 и будет распространяться на информационные системы только в госсекторе, однако его зона действия также распространена на значимые объекты КИИ.

2. Базовые наборы мер защиты для различных классов систем не будут иметь такого разрыва, как ранее. Большинство мер применимы к системам различного класса, разница — в возможных усилениях.

3. В явном виде добавлены новые группы мер:

- защита технологий контейнерных сред и их оркестрации (ЗКС);
- защита сервисов электронной почты (ЗЭП);
- защита веб-технологий (ЗВТ);
- защита программных интерфейсов взаимодействия приложений (API) (ЗПИ);
- защита конечных и мобильных устройств (ЗКУ/ЗМУ);
- защита устройств «интернета вещей» (ЗИВ);
- защита точек беспроводного доступа (ЗБД);
- защита систем искусственного интеллекта (ЗИИ).

4. Помимо подробных описаний способов реализации мер защиты информации регулятор формализовал требования к организации процессов.

5. Приведены требования к содержанию стандартов по защите информации в отношении каждой технологии защиты.

Кросстех

ФСТЭК рассказала, каким рекомендациям следовать, пока новая методика защиты ГИС не принята

Информационное сообщение от 12 марта 2026 г. № 240/22/1492 «О разъяснении положений требований о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений, утвержденных приказом ФСТЭК России от 11 апреля 2025 г. № 117»

Открыть документ



Для кого актуально

Для государственных органов, государственных унитарных предприятий, государственных и муниципальных учреждений.

Пока методика из предыдущей новости не принята, регулятор предлагает пользоваться существующими рекомендациями, но не все так очевидно.

Детали

1. В проектах по созданию или модернизации систем, подписанных до 1 марта 2026 года, допускается проведение работ в соответствии с Требованиями о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденными приказом **ФСТЭК России от 11 февраля 2013 г. № 17.**

2. Если проект стартовал позже, необходимо руководствоваться методическим документом «Меры защиты информации в государственных информационных системах», **утвержденным ФСТЭК России 11 февраля 2014 г.** Но как только вступит в силу новая методика, ваша защита окажется вне закона, поэтому мы советуем уже сейчас проектировать системы по новым требованиям, пусть пока они прописаны довольно расплывчато.

Рекомендуемые шаги

- Составьте и утвердите план перехода, содержащий описание мероприятий и мер по защите информации, направленных на реализацию положений Требований 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, со сроками их реализации.

- Начните разработку и утверждение политики защиты информации, внутренних стандартов по защите информации, а также внутренних регламентов по защите информации — с вступлением в силу 117 приказа без этого никуда.



«Новым приказом вводятся требования по нормативному обеспечению ИБ, в том числе необходимость разработки «Политики по защите информации» — верхнеуровневого документа организации.

Эта политика определяет стратегию ИБ: цели, принципы, распределение ролей и ответственность. Она служит отправной точкой для всех последующих документов, мероприятий и процессов в области ИБ. В эти процессы обязательно входят действия по разработке, планированию, внедрению и корректировке мер защиты информации, что соответствует циклу управления Деминга-Шухарта и обеспечивает синхронизацию с требованиями ГОСТ Р ИСО/МЭК 27001-2021.

Ещё одним важным дополнением стало включение требований по использованию ИИ в информационных системах.

В совокупности эти изменения представляют собой значительный шаг к развитию единой концепции управления информационной безопасностью — на основе чётких процессов, систематического подхода, современной архитектуры и возможности оперативно реагировать на риски и угрозы в отношении ГИС».

Евгений Балк,
руководитель департамента архитектуры и развития

Кросстех

Ужесточаются требования к лицензированию деятельности по технической защите конфиденциальной информации (ТЗКИ)

Проект постановления Правительства Российской Федерации «О внесении изменений в Положение о лицензировании деятельности по технической защите конфиденциальной информации, утвержденное постановлением Правительства Российской Федерации от 3 февраля 2012 г. № 79»

Открыть документ

Для кого актуально

Действующие лицензиаты ФСТЭК России, а также юрлица и ИП, планирующие осуществление деятельности по ТЗКИ.

Грядущие изменения не являются косметическими: нас ждет ужесточение и уточнение формулировок настоящего постановления. Лицензия по ТЗКИ станет дороже и будет требовать более зрелых процессов у соискателей.

Ключевые изменения

1. Ужесточение требований к лицензиатам

Если ИП или руководитель компании имеют гражданство иностранного государства, лицензию им не получить.

2. Ужесточение требований к персоналу

Раньше требования предъявлялись только к образованию ограниченного количества персонала компании: одного руководителя и двух специалистов, вне зависимости от вида работ. Теперь регламентируются численность и квалификация сотрудников, которые будут задействованы в работах по лицензируемому виду деятельности: обязательная ИБ-подготовка или переподготовка, стаж. Требования зависят от того, какие услуги по ТЗКИ оказывает соискатель.

Кроме того, необходимо обеспечить повышение квалификации всех указанных в таблице специалистов — не реже 1 раза в 5 лет, что приведет к росту затрат на обучение. Если раньше при наличии трех сотрудников необходимо было забюджетировать три обучения за пять лет, то теперь объем обучения вырастет до 10 раз.

Подпункт пункта 4 Положения	Минимальное количество инженерно-технических работников	Требования к квалификации
«а», «б», «д», «е»	Не менее 5	Высшее образование в области ИБ или иное высшее образование, стаж от 3 лет; при непрофильном образовании - обязательная профессиональная переподготовка по программам, согласованным с ФСТЭК.
«г»	Не менее 9	Из них: не менее 3 сотрудников — высшее образование в ИБ (или иное высшее + стаж от 3 лет), переподготовка; остальные — высшее или среднее профобразование, переподготовка
«в»	Не менее 15	Из них: не менее 5 сотрудников — высшее или среднее профобразование в ИБ (или иное образование + стаж от 3 лет), переподготовка; не менее 10 — высшее или среднее профобразование, переподготовка
Все подпункты	Руководитель работ	Высшее образование в области ИБ, стаж от 3 лет или иное высшее образование, стаж от 5 лет; обязательная переподготовка по программам ФСТЭК

3. Обязательное импортозамещение

Наличие и использование оборудования и ПО преимущественно отечественного производства и расположенного в РФ становится обязательным. Преимущественно — поскольку не для всех решений можно найти отечественный аналог. Но если таковой существует, применять необходимо его, а не, например open source.

4. Требование к наличию системы контроля качества

Раньше контроль касался только работ из подпункта «в» (мониторинг) и только процесса подачи, теперь перечень расширен, а подтверждение необходимо поддерживать в течение всего срока действия лицензии.

Проверка будет затрагивать не только наличие кадрового состава и оборудования, но и то, как именно выполняются работы. Для получения лицензии необходимо предоставлять сведения и копии документов, подтверждающих наличие системы производственного контроля качества проводимых работ и (или) оказываемых услуг (при выполнении работ, указанных в подпункте «а», «б», «в», «г» пункта 4 Положения). Подойдут копия сертификата системы менеджмента качества, руководства по качеству или описание технологического процесса.

5. Новая логика оценки соответствия лицензионным требованиям

Контроль потенциально становится более жестким. Если раньше в документах фигурировала формулировка о том, что оценка проводится «в форме документарной оценки» то теперь к ней добавляется «выездная оценка».

Рекомендации

- Заблаговременно проведите оценку текущего кадрового состава, при необходимости – запланируйте профессиональную переподготовку, забюджетируйте будущий наем сотрудников, соответствующих предъявляемым требованиям.

- Действующим лицензиатам стоит подготовиться к проверкам по новым обязательным блокам требований.



Лицензия на ТЗКИ — это базовый разрешительный документ для оказания услуг в области ИБ. Новые требования существенно усложнят и удорожат её получение для новых игроков рынка.

На сегодняшний день в реестре ФСТЭК России насчитывается 3 440 действующих лицензиатов ТЗКИ, из них 196 получили статус в 2025 году — это очень много. Ожидаем сокращения их количества, ухода с рынка микропредприятий и МСП.

Клиенты могут ожидать улучшения качества оказываемых услуг в области ИБ, однако, рост накладных расходов на получение и поддержание лицензии на ТЗКИ повлечёт за собой также рост цен на данные услуги.

Артём Бормотов,
директор по кибербезопасности, Кросс технолоджис

Кросстех

ИИ получит регулирование — опубликован проект профильного федерального закона

Проект ФЗ «Об основах государственного регулирования сфер применения технологий искусственного интеллекта в Российской Федерации»

Открыть документ



Для кого актуально

Для разработчиков, операторов и пользователей систем с применением ИИ на территории РФ.

Ожидаемый срок вступления ФЗ в действие — 1 сентября 2027. Для бизнеса новый закон несет несколько рисков. Прежде всего — будет ограничено использование зарубежных моделей ИИ. Кроме того, возрастут требования к ИБ, качеству и документированию в отношении моделей. Появится ответственность за некорректные решения ИИ. И самое простое — понадобится перестройка клиентских и внутренних автоматизированных процессов.

Детали

1. Проектом ФЗ предусмотрено введение комплексного регулирования ИИ с охватом всего жизненного цикла: разработка → внедрение → эксплуатация.

2. Установлен риск-ориентированный подход к регулированию применения ИИ: необходимо оценивать вероятность негативных последствий от применения конкретной модели ИИ, в том числе риски вреда физическим, юридическим лицам и государству.

3. Появится институт «доверенных моделей ИИ» с акцентом на технологический суверенитет. Т.е. приоритет получат «национальные» и «суверенные» модели — с локальной разработкой, обучением, контролем и обеспечением ИБ.

4. Необходимо будет обеспечить прозрачность использования ИИ для пользователей: размещать в сервисах уведомление об использовании технологии, в случае отказа пользователя от работы с технологией - предусмотреть возможность оказания услуг без применения ИИ, продумать возможность компенсации вреда, причинённого в связи с использованием моделей.

5. Если результат, полученный с помощью ИИ, нарушает требования законодательства РФ, ответственность распределяется между разработчиком, владельцем, оператором и пользователем системы.

Рекомендации

- Проведите инвентаризацию, где и как используется ИИ.
- Оцените риски и критичность, особенно в клиентских решениях.
- Подготовьте документацию, описывающую модели ИИ, т.е. «паспорт» моделей и инструкции по безопасной эксплуатации. В них должна содержаться информация об архитектуре, данных, метриках качества, ограничениях, рисках.
- Внедрите функции:
  - уведомления пользователей;
  - маркировку контента;
  - учет инцидентов;
- Оцените зависимость от иностранных моделей.
- Обновите договоры на оказание услуг с использованием ИИ, в т.ч. с указанием ответственных за результаты применения технологии.



Сегодня бизнес в основном использует гибридные схемы: для чувствительных данных используются отечественные модели Алиса и GigaChat, а также open-source для творческих задач с возможностью дообучения. Переход на исключительно суверенные модели приведет к отставанию в технологиях — бизнес столкнется с разрывом в качестве.

Многое будет зависеть от подхода к аттестации. Жесткая аттестация моделей напрямую повлияет на их гибкость: если требования фиксируют архитектуру, веса или алгоритм принятия решений, требуя прозрачности или запрещая самообучение в рантайме, инфраструктура масштабируется не под производительность, а под соответствие. Это ведет к созданию инстансов (вариаций), где горизонтальное масштабирование возможно только через клонирование аттестованных копий, что резко снижает адаптивность ИИ к новым данным.

Однако если аттестация будет построена по риск-ориентированному подходу, а не через сертификацию конкретной модели, у компаний останется пространство для маневра они смогут масштабировать инфраструктуру горизонтально, используя конвейеры непрерывной интеграции для ИИ, где аттестации подлежит не статичная модель, а пайплайн контроля версий и качество разметки данных как это реализовано с ГОСТ 56939. В противном случае высок риск консервации технологического уровня и потери гибкости. Безопасность будет достигаться ценой невозможности адаптировать ИИ под реальные бизнес-процессы без длительных бюрократических процедур.

Антон Редько,
руководитель группы по безопасной разработке

Кросстех

Опубликована предварительная версия стандарта по использованию ИИ и в КИИ

Предварительный национальный стандарт Российской Федерации ПНСТ 1046-2026 «Искусственный интеллект в критической информационной инфраструктуре. Общие положения»

Открыть документ



Для кого актуально

Для субъектов критической информационной инфраструктуры.

Стандарт определяет принципы применения систем искусственного интеллекта (СИИ) в составе программно-аппаратных комплексов объектов КИИ и вводит уровни критичности СИИ.

Детали

1. Стандарт определяет принципы применения СИИ в КИИ, такие как обеспечение ИБ, надежность и управляемость, объяснимость (понятность и интерпретируемость для человека), доверенность, защита от НСД, контроль человека над критическими функциями, постоянное совершенствование, особенности применения, в т.ч. с учетом отраслевой специфики.

2. СИИ в КИИ должны классифицироваться по уровню автономности принятия решений (с минимальным, средним и высоким участием человека), по функциональному назначению (автоматизация процессов, обеспечение физической безопасности и др.), по области применения (сфера КИИ), по источнику данных (внутренние данные, внешние данные из доверенных источников, прочие внешние или публичные данные).

3. Всего устанавливается 4 уровня критичности СИИ, где 1 уровень — критический, а 4 — низкий.

Рекомендуемые шаги

- Разработайте и внедрите политику ИБ СИИ, а также соответствующие процедуры, регламентирующие обеспечение безопасности СИИ.
- Разработайте планы реагирования на инциденты ИБ в соответствии с ГОСТ Р 59711.
- Определите отраслевую специфику и категорию значимости объекта КИИ.
- Определите уровень автономности принятия решений СИИ.
- Определите уровень критичности СИИ.

При внесении проектных изменений в СИИ, изменении модели угроз или последствий возможных сбоев следует заново оценить уровень ее критичности.

Необходимо проводить оценку рисков безопасности СИИ на этапе планирования, проектирования и разработки СИИ или перед внедрением СИИ в эксплуатацию, а также периодически в процессе эксплуатации.

Кросстех

Поможем подготовиться к изменениям

Если вам нужно провести оценку защищенности систем, подключиться к центру ГосСОПКА, спланировать переход на российские СЗИ, провести пентест или решить любые другие задачи ИБ, напишите нам

Написать