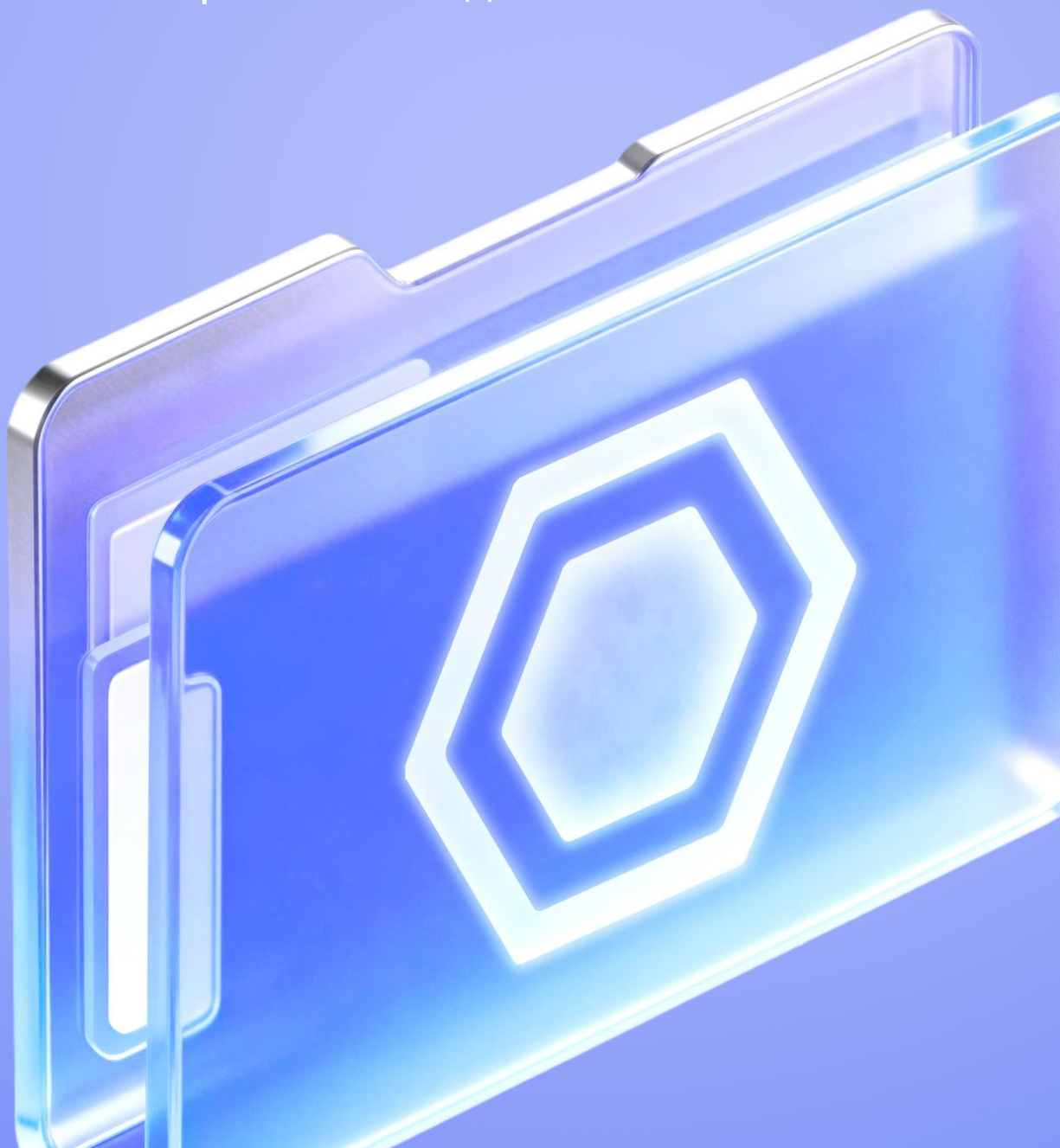
Кросстех

Регуляторный патч

Дайджест изменений законодательства
в сфере ИБ за 3 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 Кросстех

СОДЕРЖАНИЕ

Утверждены новые требования по защите информации с использованием криптографических средств для ГИС и КИИ 03

Принят закон, отменяющий «автоматическую» адекватность стран для передачи персональных данных 04

Изменятся правила проверок в области обработки персональных данных 06

В Приказе ФСТЭК РФ № 117 уточнен порядок оценки уровня зрелости подрядных организаций 08

В Приказе ФСТЭК РФ № 117 пропишут более детальные требования к ИИ 10

Субъекты КИИ обязали оценивать защищенность 11

Утвержден порядок взаимодействия с ГосСОПКА для операторов ГИС и ГосИС 11

Кросстех

Утверждены новые требования по защите информации с использованием криптографических средств для ГИС и КИИ

Открыть документ

31 августа был опубликован Приказ ФСБ России № 321, содержащий требования по защите информации в ГИС с использованием СКЗИ. Приказ ФСБ России № 117 утратил силу.

Детали

1. При вводе СКЗИ в эксплуатацию необходимо подтвердить возможность ввода актом, содержащим сведения о выполнении требований эксплуатационной и технической информации на СКЗИ.

2. Должны разрабатываться схемы криптографической защиты, содержащие: помещения размещения криптосредств, каналы связи, наименования и классы СКЗИ.

3. Детализированы требования к размещению СКЗИ — необходимо опечатывать (опломбировать) стойки с фиксацией фактов вскрытия и повторного опечатывания (опломбирования).

Рекомендуемые шаги

Организациям государственного сектора необходимо провести инвентаризацию СКЗИ и провести следующий комплекс мероприятий:

1. Оценить соответствие фактический условий эксплуатации СКЗИ требуемым: проверить среду функционирования СКЗИ, включая наличие оценки влияния, дополнительных средств защиты информации, если это требуется.

2. Разработать и утвердить схемы криптозащиты.

3. В случае размещения СКЗИ не в опечатываемых стойках провести процедуру опечатывания существующих стоек или переноса оборудования СКЗИ в новые стойки.

4. Провести оценку выполнения требований, не подвергшихся изменениям: актуальность правил доступа в помещения размещения СКЗИ и перечня лиц, имеющих доступ в эти помещения и т.д.

Кросстех

Принят закон, отменяющий «автоматическую» адекватность стран для передачи персональных данных

Федеральный закон **Приказ РКН**

Официально опубликован Федеральный закон от 26.07.2026 № 265-ФЗ, вносящий принципиальные изменения в статью 12 152-ФЗ. Реформа затрагивает правила формирования перечня государств, обеспечивающих адекватную защиту прав субъектов персональных данных. Закон вступил в силу со дня официального опубликования — 26 июля 2026 года. Также для общественного обсуждения представлен проект приказа Роскомнадзора «Об утверждении перечня иностранных государств, обеспечивающих адекватную защиту прав субъектов персональных данных».

Ключевая идея: формальное участие иностранного государства в Конвенции Совета Европы «О защите физических лиц при автоматизированной обработке персональных данных» (СДСЕ № 108) больше не является самостоятельной гарантией адекватной защиты персональных данных.



Для кого актуально

Компании, передающие ПДн зарубежным контрагентам, использующие иностранные ИТ-сервисы, облачную инфраструктуру или работающие в составе международных групп компаний.

Детали

1. Исключение упоминаний стороны Конвенции Совета Европы из частей 5, 10 и 11 статьи 12 «Трансграничная передача персональных данных». Теперь единственным юридически значимым ориентиром при осуществлении трансграничной передачи и получения сведений от иностранных контрагентов, которым планируется трансграничная передача персональных данных, до подачи уведомления, становится перечень, утверждаемый Роскомнадзором.

2. Новые критерии включения в перечень. Роскомнадзор, утверждая перечень, будет учитывать не только формальное соответствие положениям Конвенции, но и реально применяемые государством меры.

3. Статус стран — участниц Конвенции. Государства, признаваемые «адекватными» в силу членства в Конвенции, сохранят этот статус только через актуализированный перечень Роскомнадзора.

Что это означает для бизнеса

Раньше компании могли ориентироваться на формальное участие государства в Конвенции Совета Европы — теперь этого недостаточно. При планировании трансграничной передачи придется учитывать актуальный перечень Роскомнадзора. Подход к определению «адекватных» стран может стать более консервативным. Если государство не войдет в перечень Роскомнадзора, оценка правомерности передачи потребует тщательной оценки рисков, так как Роскомнадзор может запретить такую трансграничную передачу персональных данных.

Что пока не изменилось

Проект приказа, который должен утвердить обновленный перечень стран в соответствии с новыми правилами, пока находится на стадии общественного обсуждения. Он еще не принят и не зарегистрирован в Минюсте.

Рекомендуемые шаги

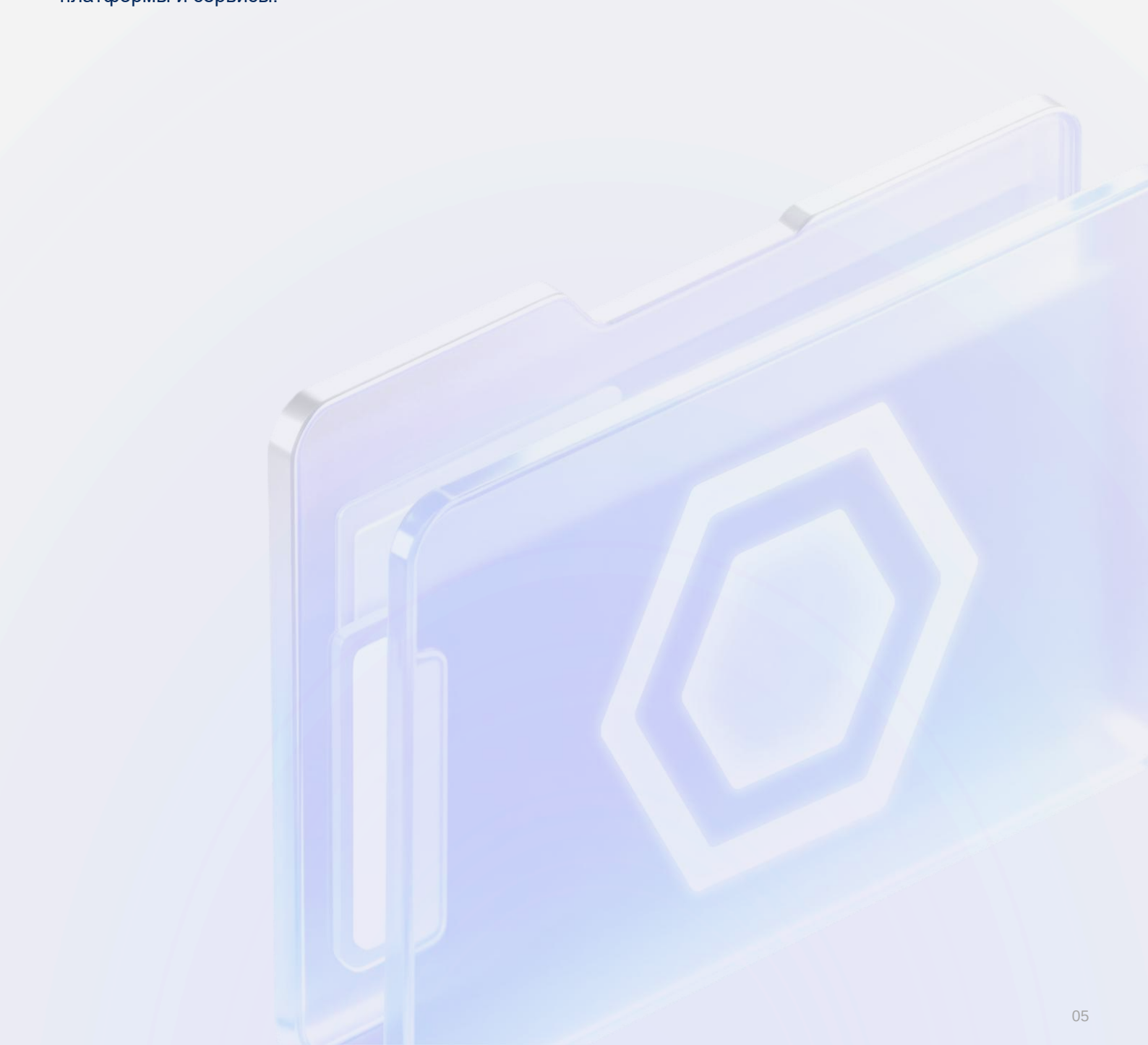
1. Инвентаризация трансграничных потоков. Составьте полный список всех стран, в которые передаются ПДн, учитывайте контрагентов, ИТ-сервисы, облачных провайдеров, головные компании.

2. Мониторинг перечня РКН. Дождитесь публикации актуализированного перечня и сверьте с ним свои маршруты трансграничной передачи.

3. Аудит договоров и юридических оснований. Проверьте контракты с зарубежными партнерами на наличие положений о защите ПДн. Если страна выбывает из перечня — оцените возможность применения иных оснований или необходимость получения разрешения Роскомнадзора.

4. Подготовка уведомлений. Проверьте, направлялись ли уведомления о трансграничной передаче в Роскомнадзор, в случае изменения перечня может потребоваться их корректировка или повторная подача.

5. Оценка рисков и альтернатив. Проанализируйте правовые основания трансграничной передачи данных, а также меры безопасности по соблюдению основополагающих принципов защиты, обеспечению конфиденциальности и безопасности персональных данных, применяемые принимающей стороной. Оцените риски приостановки потоков данных. Рассмотрите варианты перехода на российские облачные платформы и сервисы.



Кросстех

Изменятся правила проверок в области обработки персональных данных

Открыть документ



Для кого актуально

Любые юридические лица, государственные или муниципальные органы, которые обрабатывают персональные данные.

Роскомнадзор продолжает ужесточать контроль за обработкой персональных данных. Опубликован проект нормативного акта, который вносит серьезные изменения в проверочный лист из приказа РКН от 24.12.2021 № 253 и затронет многие аспекты работы с персональными данными. Проверки регулятора станут более детальными с пошаговой сверкой по каждому пункту нового чек-листа.

Детали

Отметим ключевые изменения относительно ранее опубликованного проекта, на которые нужно обратить внимание прямо сейчас.

1. Жесткий контроль за «сроком годности» данных. Теперь инспекторы будут проверять, как исполняется требование ч. 7 ст. 5 152-ФЗ: данные должны уничтожаться или обезличиваться, как только достигнута цель их сбора. Это обязательное требование, которое теперь под прицелом.

2. Согласие: «Конкретное, информированное и отдельное». Приказ добавляет проверку соответствия согласия сразу двум жестким требованиям.

В ч. 1 ст. 9 говорится, что согласие должно соответствовать критериям конкретности, предметности, информированности, сознательности и однозначности и оформляться отдельно от иных документов и информации. Что это значит на практике?

Конкретность и предметность — в согласии должны быть четко обозначены определенные действия с персональными данными, указан точный перечень собираемых сведений и конкретная цель сбора.

Информированность — читая согласие, субъект должен понимать, на что он соглашается, кто именно собирает данные (наименование и адрес оператора), как с ним связаться и каков срок действия согласия.

Сознательность и однозначность — согласие дается добровольно, без давления, только через активное действие субъекта (например, нажатием кнопки или проставлением галочки в чекбоксе, а не заранее проставленным флажком «по умолчанию»).

В ч. 9 ст. 9 указано, что согласие на распространение данных по форме и содержанию должно строго соответствовать требованиям Роскомнадзора (срок действия Приказа Роскомнадзора №18 ограничен 1 сентября 2027 года).

3. Уведомление в РКН: детализация по каждой цели обработки ПДн. Теперь будут проверять, соответствуют ли данные, указанные в реестре на сайте Роскомнадзора, требованию ч. 3.1 ст. 22 152-ФЗ. Уведомление об обработке должно быть с раскрытием по каждой цели.

4. Обезличивание: строго по правилам. Обезличивание должно осуществляться по требованиям и методам РКН (ч. 12 ст. 23 152-ФЗ и Приказ РКН №140 от 19.06.2025).

Из листа исключен вопрос об организационных мерах защиты ПДн. Но требования ч. 1 ст. 19 об организационных мерах и обязанность оператора по их исполнению остаются неизменными.

Кросстех

Рекомендуемые шаги

1. Аудит целей и хранения персональных данных. Проведите инвентаризацию бизнес-процессов обработки, для каждой цели сбора данных четко определите срок хранения и зафиксируйте в локальных нормативных актах порядок уничтожения или обезличивания информации.

2. Ревизия согласий. Проведите оценку имеющихся форм согласий, проверьте, соответствуют ли они критериям конкретности, предметности, информированности, сознательности и однозначности? Оформлены ли отдельным документом, а не «вшиты» в анкету или договор-оферту? Оцените форму и содержание согласия на распространение персональных данных на соответствие всем требованиям действующего Приказа Роскомнадзора от 24.02.2021 N 18.

3. Проверка уведомления в Роскомнадзор на содержание всей детальной информации по каждой цели. Сверьте свое уведомление в реестре операторов на сайте Роскомнадзора с реальными бизнес-процессами; убедитесь, что в нем раскрыта информация по каждой цели обработки, проверьте, все ли категории субъектов и данные, которые вы обрабатываете на практике, у вас указаны. При необходимости, направьте корректирующее уведомление.

4. Внедрение методов по обезличиванию, установленных Приказом Роскомнадзора № 140 (введение идентификаторов, изменение состава или семантики, перемешивание и декомпозиция).

Готовьтесь к тому, что контроль со стороны регулятора станет более системным и комплексным, а проверка – более детальной, охватывающей все этапы жизненного цикла персональных данных. Лучше подготовиться заранее.

Кросстех

В Приказе ФСТЭК РФ № 117 уточнен порядок оценки уровня зрелости подрядных организаций

Открыть документ

С 1 сентября 2026 г введена в действие актуализированная редакция Приказа ФСТЭК России № 117. Изменения в основном касаются формулировок, куда интереснее часть, которая вводится в действие с 1 марта 2027 года.

С этой даты предъявляется требование к оценке показателя уровня зрелости подрядных организаций, подключаемых к ГИС и ГосИС, а также уточнена возможность применения усиленной многофакторной аутентификации (ранее была указана только строгая аутентификация для удаленного и привилегированного доступа). Обратим внимание на фразу: «Расчет и оценка показателя уровня зрелости $У_{ЗИ}$ проводятся подрядной организацией до получения доступа к информационным системам, содержащейся в них информации, и (или) передачи им информации и далее не реже одного раза в два года».

Детали

С 1 марта 2027 г:

1. Любая подрядная организация, которая имеет или для которой предполагается в будущем доступ к ГИС и ГосИС, должна провести оценку уровня зрелости и предъявить данные сведения оператору ГИС или ГосИС до получения доступа. Оценка проводится в соответствии с Методическим документом ФСТЭК России.

2. Подрядные организации должны проводить данную оценку не реже раза в 2 года.

При этом предложенное изменение исключает из текста требований периодичность проведения оценки $У_{ЗИ}$ для самих операторов ГИС и ГосИС. Мы предполагаем, что формулировка еще претерпит изменения и периодичность оценки для операторов ГИС и ГосИС также будет установлена, как это приведено в текущей редакции требований.



На наш взгляд, отсутствие установленной периодичности в приказе не означает, что такую оценку следует проводить однократно и отказываться от её регулярного выполнения. Оценка уровня зрелости позволяет организации отслеживать изменения в состоянии процессов защиты информации, выявлять проблемные области и оценивать эффективность мероприятий по их совершенствованию, поэтому организациям целесообразно самостоятельно установить периодичность проведения оценки во внутренних документах (не реже одного раза в два года) и использовать $У_{ЗИ}$ в качестве инструмента регулярного самоконтроля

Ашраф Садыхбеков,
ведущий аудитор

Рекомендуемые шаги

Не стоит пытаться провести полноценную оценку всех направлений за две недели. Подготовку целесообразно организовать поэтапно.

1. Первичная инвентаризация. По каждому из 21 направления необходимо определить:

- Существует ли соответствующий процесс;
- Кто является его владельцем;
- Какими документами он регулируется;
- Какие инструменты применяются;
- Какие метрики собираются.

На первом этапе достаточно честной предварительной оценки: процесс существует, реализован частично либо отсутствует. Важно отражать фактическое положение дел, а не только наличие утвержденных документов.

2. Сформировать базу доказательств. Подготовьте материалы, которые уже существуют и могут быть оперативно представлены: приказы, регламенты, заявки, журналы, протоколы, отчеты, результаты сканирования и мониторинга, метрики, материалы обучения и планы устранения недостатков.

Такой сбор позволит понять, какие процессы действительно работают и подтверждаются проверяемыми свидетельствами, а какие существуют только формально или выполняются без документального подтверждения.

3. Провести анализ разрывов. На основании заполненной матрицы и собранных доказательств необходимо оценить каждое применимое направление по критериям методики и определить основные недостатки.

4. Разработать дорожную карту. По результатам анализа необходимо сформировать план проектирования, внедрения и развития отсутствующих или недостаточно зрелых процессов.

Кросстех

В Приказе ФСТЭК России № 117пропишут более детальные требования к ИИ

Открыть документ

Предполагается, что указанные изменения вступят в силу 1 марта 2027 года, но в настоящий момент проект изменений не принят. Ожидаем расширение методического документа, определяющего состав и содержание мероприятий и мер по защите информации, детализацией возможных механизмов защиты ИИ-моделей и ИИ-агентов.

Детали

Приказ содержит следующие изменения:

1. Обеспечение возможности исключения несанкционированного доступа и воздействия на информационные системы, распространения и модификации информации, а также использования ИС не по назначению за счет воздействия на применяемые модели и агенты ИИ.

2. Обеспечение выделенного сегмента ИС или вычислительной сети для размещения ИИ-моделей с доступом в сегмент с применением MFA.

3. В случае применения моделей ИИ 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.

4. Для ИИ-агентов также должны реализовываться меры защиты информации, направленные на предотвращение несанкционированного воздействия на ресурсы информационной системы, а также контроль и управление правами доступа агентов.



Для рынка новые требования означают смену драйвера: из „давайте попробуем, это интересное направление“ защита LLM переходит в разряд „надо, потому что требует регулятор“. Именно здесь AI Firewall перестаёт быть опцией и становится обязательным элементом архитектуры. Следим за финальной редакцией приказа, но вектор уже понятен.

Антон Редько,
руководитель группы по безопасной разработке

Кросстех

Субъекты КИИ обязали оценивать защищенность

Открыть документ

Детали

Для субъектов КИИ аналогично операторам ГИС и ГосИС введено требование по оценке показателя защищенности значимых объектов КИИ и оценке уровня зрелости субъекта КИИ со следующей периодичностью:

- Оценка $К_{ЗИ}$ — раз в полгода;
- Оценка $У_{ЗИ}$ — раз в три года.

Для подрядных организаций, получающих доступ к ЗОКИИ, также устанавливается требование по оценке $У_{ЗИ}$ до доступа к ЗОКИИ и не реже раза в 3 года. Ожидаем ввода в действие аналогичных требований в отношении операторов ПДн.

Утвержден порядок взаимодействия с ГосСОПКА для операторов ГИС и ГосИС

Открыть документ

Официально закреплен порядок взаимодействия операторов ГИС, ГосИС и НКЦКИ по вопросам информирования о компьютерных инцидентах (КИ) и угрозах информации безопасности (УБИ). Требования, применявшиеся ранее, распространялись только на КИИ.

Детали

С 1 сентября операторы ГИС и ГосИС обязаны информировать НКЦКИ о КИ и УБИ в отношении принадлежащих им объектов информатизации с использованием личного кабинета.

Для получения доступа к личному кабинету организации необходимо заключить соответствующий регламент взаимодействия с НКЦКИ, при этом доступ к личному кабинету возможен исключительно по защищенному каналу.

Допускается информирование о КИ посредством электронной почты в случае недоступности ЛК или канала связи до него.

При использовании любого доступного канала передачи данных о КИ предельный срок информирования с момента наступления КИ — 24 часа.

Рекомендуемые шаги

1. Забюджетировать и произвести покупку СКЗИ для организации канала с НКЦКИ.
2. Заключить регламент взаимодействия с НКЦКИ.
3. Настроить канал и получить доступ к личному кабинету.
4. Осуществлять обмен информацией с НКЦКИ в установленные регламентные сроки.

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