



Аналитический отчет по ключевым изменениям в законодательстве за 2025 год

Настоящий отчет посвящен комплексному анализу изменений нормативных правовых актов в сфере информационной безопасности, защиты информации и обработки данных, вступивших в силу в 2025 году. В материале рассматриваются не только отдельные законодательные новеллы, но и формирующиеся взаимосвязи между федеральными законами, подзаконными актами и методическими документами, а также их совокупное влияние на практику обеспечения безопасности в государственных и корпоративных информационных системах.

Основная задача отчета заключается в выявлении ключевых тенденций развития правового регулирования, оценке трансформации требований и определении практических последствий для организаций, эксплуатирующих государственные информационные системы, значимые объекты критической информационной инфраструктуры и иные информационные ресурсы. Отдельное внимание уделено вопросам импортозамещения, управления уязвимостями, реагирования на инциденты и защиты персональных данных как элементам единой системы управления рисками.

Содержание

Развитие регулирования КИИ и ГосСОПКА	3
Изменения в 187-ФЗ	3
ГосСОПКА: системная перестройка регулирования.....	4
Аккредитация центров ГосСОПКА	5
Категорирование и оценка значимости.....	6
Реестры доверенного и ПО для собственных нужд.....	8
Государственные информационные системы.....	9
Управление уязвимостями, тестирование и оценка защищенности	10
Персональные данные.....	12
Недопустимые события и реагирование.....	13
Заключение	13

Развитие регулирования КИИ и ГосСОПКА

Изменения в 187-ФЗ

Изменения, внесенные в [Федеральный закон от 26.07.2017 № 187-ФЗ](#) «О безопасности критической информационной инфраструктуры Российской Федерации» (далее – 187-ФЗ) в 2025 году, стали одним из ключевых событий года и существенно расширили само понимание безопасности значимых объектов критической информационной инфраструктуры (далее – КИИ). Если ранее регулирование было сосредоточено преимущественно на противодействии компьютерным атакам и реагировании на инциденты, то в новой редакции закон фактически охватывает вопросы технологической устойчивости и управляемости используемых решений.

Принципиально новым элементом стало нормативное закрепление требований по импортозамещению как составной части обеспечения безопасности значимых объектов КИИ. До 2025 года требования к использованию отечественного программного обеспечения (далее – ПО), программно-аппаратных комплексов и технических средств формировались фрагментарно и вытекали преимущественно из указов Президента Российской Федерации (далее – РФ) и постановлений Правительства РФ, в частности [Постановления Правительства РФ от 14.11.2023 № 1912](#) «О порядке перехода субъектов критической информационной инфраструктуры Российской Федерации на преимущественное применение доверенных программно-аппаратных комплексов на принадлежащих им значимых объектах критической информационной инфраструктуры Российской Федерации» (далее – ПП-1912), а также из ведомственных разъяснений. При этом прямая юридическая связь между нарушением политики импортозамещения и нарушением требований 187-ФЗ отсутствовала, что позволяло рассматривать эти направления как параллельные.

После внесения изменений требования к происхождению и доверенности применяемых решений были встроены непосредственно в 187-ФЗ. Безопасность значимых объектов КИИ стала трактоваться шире и теперь включает контроль цепочек поставок, технологическую независимость, управляемость обновлений и снижение рисков, связанных с использованием недоверенных компонентов. Тем самым была сформирована правовая основа для дальнейшего ужесточения подзаконного регулирования в области импортозамещения.

В результате внесенных изменений в 187-ФЗ закреплены обязанности субъектов КИИ по переходу на доверенные программно-аппаратные комплексы в соответствии с ПП-1912, а также ориентация на использование отечественного ПО. При этом детальные правила перехода на российское ПО подлежат установлению отдельным [постановлением Правительства РФ](#) и на момент подготовки настоящего обзора находятся в стадии проектирования.

Кроме того, в законе закреплены понятия перечней типовых отраслевых объектов КИИ и отраслевых особенностей их категорирования. В развитие данных положений профильными федеральными органами исполнительной власти подготовлены проекты перечней типовых объектов и проектов отраслевых особенностей, размещенные для общественного обсуждения и межведомственного согласования, а также [проект нормативного правового акта](#), предусматривающий утверждение Перечней типовых отраслевых объектов КИИ. По состоянию на конец 2025 года соответствующие [отраслевые особенности](#) утверждены только для атомной отрасли – в рамках нормативных документов Государственной корпорации по атомной энергии «Росатом». По остальным отраслям подготовленные перечни и особенности продолжают находиться в статусе проектов:

[здравоохранение ↗](#)
[ТЭК и энергетика ↗](#)
[металлургическая промышленность ↗](#)
[ракетно-космическая промышленность ↗](#)
[связь ↗](#)
[оборонная промышленность ↗](#)
[наука ↗](#)
[государственная регистрация прав на недвижимое имущество и сделки с ним ↗](#)
[горнодобывающая промышленность ↗](#)
[транспорт ↗](#)
[химическая промышленность ↗](#)

ГосСОПКА: системная перестройка регулирования

В 2025 году изменения, внесенные в 187-ФЗ, существенно расширили нормативные полномочия государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ (далее – ГосСОПКА). В частности, в закон были включены положения, устанавливающие обязанности по взаимодействию с ГосСОПКА не только для субъектов КИИ, но и для более **широкого круга организаций**, включая федеральные органы исполнительной власти, органы государственной власти субъектов РФ, государственные унитарные предприятия и учреждения, государственные внебюджетные фонды, государственные корпорации, государственные компании, а также иные российские юридические лица, находящиеся под контролем РФ либо субъекта РФ или контролируемые ими (далее – государственные органы и организации).

Одновременно в 187-ФЗ была расширена информационная обязанность участников системы: если ранее закон прямо оперировал обязанностью информирования о компьютерных инцидентах, то в обновленной редакции закреплена обязанность передачи сведений также о компьютерных атаках, включая информацию, выявленную на ранних стадиях до наступления последствий.

Ввиду указанных законодательных изменений потребовалась актуализация ведомственного регулирования, прежде всего нормативных актов Федеральной службы безопасности РФ (далее – ФСБ России), определяющих порядок реагирования и взаимодействия в рамках ГосСОПКА. Соответствующие изменения были реализованы в обновленных редакциях приказов ФСБ России, устанавливающих правила информирования Национального координационного центра по компьютерным инцидентам (далее – НКЦКИ) и центров ГосСОПКА о компьютерных инцидентах и атаках, таких как:

- [приказ ФСБ России от 23.12.2025 № 539](#);
- [приказ ФСБ России от 25.12.2025 № 546](#),
ввиду утверждения приказа был отменен [приказ ФСБ России от 24.07.2018 г. №368](#);
- [приказ ФСБ России от 25.12.2025 № 547](#),
ввиду утверждения приказа был отменен [приказ ФСБ России от 19.06.2019 г. № 282](#);
- [приказ ФСБ России от 25.12.2025 № 548](#);
- [приказ ФСБ России от 26.12.2025 № 553](#),
ввиду утверждения приказа был отменен [приказ ФСБ России от 19.06.2019 г. № 281](#);
- [приказ ФСБ России от 26.12.2025 № 554](#),
ввиду утверждения приказа был отменен [приказ ФСБ России от 06.04.2019 г. № 196](#).

При этом для субъектов КИИ существенного пересмотра сроков информирования не произошло. Как и ранее, сохранены следующие временные параметры: не позднее 24 часов – для

объектов КИИ, не отнесенных к значимым; не позднее 3 часов – для значимых объектов КИИ; а также не позднее 48 часов – для представления информации о ходе расследования компьютерного инцидента на значимых объектах КИИ. Данные требования закреплены в приказах ФСБ России, регулирующих порядок представления информации в систему ГосСОПКА.

В то же время для государственных органов и организаций впервые были установлены **сроки и процедуры информирования о компьютерных атаках и инцидентах**: при инциденте в информационном ресурсе государственного органа или организации – в течение 24 часов, а при компьютерной атаке независимо от наступления последствий – также не позднее 24 часов. Дополнительно предусмотрена обязанность до начала мероприятий по ликвидации последствий определить планируемые меры и направить соответствующую информацию в НКЦКИ, а также после завершения восстановительных работ сообщить в НКЦКИ результаты восстановления в течение 24 часов.

Отдельного внимания заслуживает закрепление **обязанности по непрерывному взаимодействию с НКЦКИ для субъектов КИИ**, эксплуатирующих значимые объекты КИИ, а также для государственных органов и организаций. Указанная обязанность определена в нормативных актах ФСБ России, регулирующих функционирование ГосСОПКА, и предполагает **подключение к технической инфраструктуре НКЦКИ**, использование личных кабинетов в системе НКЦКИ и обеспечение круглосуточного обмена данными о выявленных атаках и инцидентах.

В рамках развития указанных положений 187-ФЗ были также обновлены **технические требования к установке и эксплуатации средств ГосСОПКА**, а также **порядок обмена информацией о компьютерных атаках и инцидентах и получения сведений от НКЦКИ**. Соответствующие изменения закреплены в ведомственных нормативных правовых актах ФСБ России, регламентирующих требования к средствам обнаружения, правила интеграции с инфраструктурой ГосСОПКА и форматы информационного взаимодействия.

Аккредитация центров ГосСОПКА

В августе 2025 года **приказом ФСБ России от 21.07.2025 № 282** «О внесении изменения в **приказ ФСБ России от 01.11.2022 № 543** «Об определении переходного периода, предусмотренного подпунктом «б» пункта 5 **Указа Президента Российской Федерации от 01.05.2022 № 250**» был продлен переходный период, в течение которого органы и организации, подпадающие под действие указа Президента РФ, вправе привлекать сторонние организации, не имеющие аккредитации в качестве центров ГосСОПКА, для реализации мероприятий по обнаружению, предупреждению и ликвидации последствий компьютерных атак и реагированию на компьютерные инциденты. В указанный период, действующий до 2027 года, субъекты КИИ и иные организации могут осуществлять взаимодействие с такими сторонними организациями при условии, что последние заключили с НКЦКИ соглашение о сотрудничестве (взаимодействии) в области обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты.

В связи с необходимостью формирования окончательных требований к аккредитуемым центрам ГосСОПКА был разработан **проект приказа** ФСБ России «Об утверждении Порядка аккредитации центров государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации и Требованиям к центрам государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, а также к аккре-

дитованным центрам». Согласно публикуемому проекту, аккредитация центров предполагает:

01

Установление требований к составу специалистов центра, включая квалификационные критерии и требования к опыту работы в области информационной безопасности (далее – ИБ) и анализа компьютерных атак;

02

Наличие действующей лицензии на право осуществления работ, связанных с использованием сведений, составляющих государственную тайну, для выполнения работ по мониторингу и реагированию в рамках ГосСОПКА;

03

Определение минимальных параметров технической инфраструктуры, необходимой для обеспечения круглосуточного взаимодействия с НКЦКИ и другими центрами ГосСОПКА.

Категорирование и оценка значимости

Как было отмечено выше, в 187-ФЗ внесены изменения, конкретизирующие процедуру категорирования объектов КИИ – закреплены обязанности субъектов КИИ по использованию перечней типовых отраслевых объектов КИИ и отраслевых особенностей категорирования объектов КИИ.

В связи с изменениями 187-ФЗ были внесены корректировки в [Правила категорирования объектов КИИ РФ, а также перечень показателей критериев значимости объектов КИИ РФ и их значений, утвержденные Постановлением Правительства РФ от 08.02.2018 № 127](#) (далее – Правила категорирования). Изменения в Правила категорирования были утверждены [Постановлением Правительства РФ от 07.11.2025 № 1762](#).

Так, одним из ключевых моментов в обновленных Правилах категорирования является исключение понятия критических процессов. Ранее категорирование объектов КИИ проводилось путем определения критических процессов – процессов, нарушение которых могло привести к негативным социальным, политическим, экономическим, экологическим последствиям, последствиям для обеспечения обороны страны, безопасности государства и правопорядка, – и выявления систем и сетей, обеспечивающих реализацию соответствующих процессов. На текущий момент, согласно Правилам категорирования, категорированию подлежат объекты КИИ, которые соответствуют типам информационных систем, информационно-телекоммуникационных сетей, автоматизированных систем управления, включенным в перечни типовых отраслевых объектов КИИ. То есть субъекты КИИ категорируют в первую очередь те системы и сети, которые соответствуют типовым объектам КИИ из утвержденных перечней. Однако стоит отметить, что субъекты КИИ фактически должны провести анализ всех своих систем и сетей на соответствие показателям критериев значимости. Так, если масштаб возможных негативных последствий для отдельной системы или сети соответствует показателям значимости (то есть полученные значения по показателям требуют присвоение категории, и фактически система или сеть является значимым объектом КИИ), но при этом система или сеть не соответствует типовым объектам КИИ из утвержденных перечней, то субъект КИИ обязан присвоить указанному объекту КИИ категорию значимости и предоставить сведения о таком объекте в Федеральную службу по техническому и

экспортному контролю Российской Федерации (далее – ФСТЭК России). Таким образом, субъект КИИ выступает инициатором по внесению дополнений в перечни типовых отраслевых объектов КИИ.

Стоит отметить, что в июле 2025 года [приказом ФСТЭК России № 247](#) была изменена форма направления сведений о результатах присвоения объекту КИИ одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий, утвержденная [приказом ФСТЭК России от 22.12.2017 № 236](#). Теперь субъекты КИИ в направляемых сведениях о результатах категорирования для каждого объекта КИИ обязаны указывать наименование типового отраслевого объекта КИИ в соответствии с утвержденными перечнями, а также указывать доменные имена и внешние сетевые адреса объектов КИИ (при их наличии). В [информационном сообщении от 22.10.2025 № 240/84/3451](#) ФСТЭК России разъяснила, что до утверждения перечней типовых отраслевых объектов КИИ в соответствующем поле сведений ставится прочерк. В том числе ФСТЭК России объяснила, что необходимо указывать доменное имя, предназначенное для адресации в сети Интернет в целях обеспечения доступа к информации, размещенной в сети Интернет, а также указывать внешний (публичный) IP-адрес, назначаемый объекту КИИ при подключении к сети связи с целью подключения к сети Интернет. При использовании динамического IP-адреса рекомендуется указывать адрес DNS сервера провайдера. В случае отсутствия подключения КИИ к сети Интернет заполнять соответствующее поле не требуется.

Также в Правилах категорирования в явном виде закреплены обязанности субъекта КИИ по учету утвержденных отраслевых особенностей при категорировании объектов КИИ. При этом были дополнены положения об осуществлении ведомственного мониторинга по актуальности и достоверности сведений о результатах категорирования, которые предоставляют субъекты КИИ (пункт 19.2 Правил категорирования). Согласно нововведениям, государственные органы и российские юридические лица, осуществляющие мониторинг в установленной сфере деятельности, обязаны передавать в ФСТЭК России результаты таких контрольных мероприятий, в том числе предоставлять сведения:

- о нарушении сроков работ по категорированию;
- о нарушении отраслевых особенностей категорирования;
- о представлении в ФСТЭК России неактуальных либо недостоверных сведений;
- о выявлении информационных систем, информационно-телекоммуникационных сетей, автоматизированных систем управления, которые соответствуют типовым объектам КИИ, включенным в перечни типовых отраслевых объектов КИИ, и категорирование которых не проведено.

Помимо актуализации Правил категорирования также были обновлены перечень показателей критериев значимости и их значения. В частности, внесены следующие изменения:

- показатель № 3 (транспортная деятельность) дополнен новыми критериями для оценки и их значениями (добавлены подпункты в и г);
- скорректированы критерии и значения показателей № 4 (функционирование сетей связи), № 6 (деятельность государственных органов и организаций), № 10 (деятельность по переводу денежных средств), № 10.3 (деятельность пенсионных фондов) и 10.4 (деятельность страховых организаций);
- введены новые показатели № 10.6 (деятельность микрофинансовых организаций) и № 10.7

(деятельность кредитных бюро), а также показатель № 13.1 (реализация государственных оборонных заказов).

Таким образом, Правила категорирования, как подзаконный акт, были актуализированы с учетом изменений 187-ФЗ, а также были внедрены новые критерии для оценки возможных негативных последствий и определения значимости объектов КИИ.

Реестры доверенного и ПО для собственных нужд

В 2025 году требования по импортозамещению получили дальнейшее развитие в контуре обеспечения ИБ, в том числе через их прямую увязку с обязанностями субъектов КИИ и владельцев государственных информационных систем (далее – ГИС). В результате вопросы происхождения ПО и средств защиты информации (далее – СрЗИ) стали рассматриваться не изолированно, а как элемент выполнения требований по защите информации и устойчивости функционирования информационных систем.

Одним из ключевых элементов этой трансформации стало ужесточение ответственности за использование несертифицированных СрЗИ в ГИС закреплено [Федеральным законом от 23.05.2025 № 104-ФЗ](#) «О внесении изменений в статьи 4.5 и 13.12 Кодекса РФ об административных правонарушениях (далее – КоАП РФ) и статью 1 Федерального закона «О внесении изменений в Кодекс Российской Федерации об административных правонарушениях». Указанным законом были продлены сроки давности привлечения к административной ответственности по [статье 13.12 КоАП РФ](#) «Нарушение правил защиты информации», а также существенно увеличены размеры административных штрафов за использование несертифицированных СрЗИ и нарушение установленных требований по защите информации.

	Прежний размер штрафов	Текущий размер штрафов
Должностные лица	1500 руб – 2500 руб	5000 руб – 10 000 руб
Индивидуальные предприниматели	2500 руб – 3000 руб	10 000 руб – 50 000 руб
Юридические лица	20 000 руб – 25 000 руб	50 000 руб – 100 000 руб

Аналогичным образом повышены санкции по иным частям статьи 13.12 КоАП РФ, включая составы, связанные с нарушением порядка обработки конфиденциальной информации и несоблюдением требований к защите информации.

Дальнейшее развитие логики импортозамещения связано с принятием [Федерального закона от 31.07.2025 № 325-ФЗ](#) «О внесении изменений в отдельные законодательные акты Российской Федерации», который внес изменения в [Федеральный закон от 07.04.2025 №58-ФЗ](#) «О внесении изменений в Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации». Указанные изменения заложили правовую основу для формирования механизма реестра доверенного ПО и определения требований к программным продуктам,

допускаемым к использованию в значимых объектах КИИ и ГИС. Соответствующий **проект постановления Правительства РФ о ведении реестра доверенного ПО** был размещён для обсуждения и анализировался в профильных отраслевых обзорах, однако, по состоянию на конец 2025 года окончательная редакция документа не утверждена.

Одновременно положения формируют предпосылки для пересмотра подходов к регулированию самописного ПО – ПО, разработанного для собственных нужд организации. Детальные правила учёта и допустимости использования такого ПО были закреплены **постановлением Правительства РФ от 28.11.2025 № 1936**, которым установлен специальный порядок применения самописного ПО в значимых объектах КИИ и ГИС.

В совокупности с изменениями в 187-ФЗ и развитием подзаконного регулирования формируется единая надзорная конструкция, в рамках которой происхождение ПО, его включение в реестры доверенных или допустимых решений и факт сертификации СрЗИ напрямую влияют на правомерность эксплуатации информационных систем. Ожидаемые постановления Правительства РФ по импортозамещению ПО на значимых объектах КИИ должны окончательно закрепить эту связку и устранить оставшиеся разрывы между требованиями информационной безопасности и требованиями к используемым технологиям.

Практическим следствием данных изменений становится необходимость комплексного пересмотра ИБ-ландшафтов. Формальный подход, при котором импортозамещение реализуется отдельно от выполнения требований по безопасности, становится неустойчивым. Для организаций возрастает значение инвентаризации ПО, оценки его правового статуса, выстраивания процессов управления жизненным циклом решений и документирования обоснований допустимости использования отдельных продуктов.

Государственные информационные системы

Изменения 2025 года в регулировании ГИС стали важным этапом упорядочивания и рационализации требований в сфере защиты информации, обрабатываемой государственными органами и организациями.

В **Федеральный закон 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»** (далее – 149-ФЗ) были внесены уточнения **Федеральным законом от 29.12.2025 № 568-ФЗ «О внесении изменений в Федеральный закон «Об информации, информационных технологиях и о защите информации»**, закрепившие терминологическое разграничение между федеральными государственными информационными системами, государственными информационными системами субъектов РФ, а также иными информационными системами государственных органов.

Ключевым подзаконным актом, развивающим данный подход, стал **приказ ФСТЭК 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 России № 117). В отличие от прежних редакций требований, данный приказ прямо распространил обязательные меры защиты информации, включая использование сертифицированных СрЗИ, не только на ГИС, но также на иные информационные системы, эксплуатируемые государственными органами, государственными унитарными предприятиями и государственными учреждениями. В

отношении муниципальных информационных систем приказ предусматривает, что защита информации обеспечивается в соответствии с требованиями приказа ФСТЭК России № 117, если иное не предусмотрено законодательством РФ. Требования по обязательной реализации мер защиты и применению сертифицированных СрЗИ адресованы не всему государственному сектору в целом, а ограниченному кругу организаций с определенными организационно-правовыми формами, перечисленными ранее, эксплуатирующим информационные системы вне периметра специальных и закрытых контуров.

Одновременно приказ ФСТЭК России № 117 сохранил подход к обязательной аттестации исключительно в отношении ГИС. Действующие аттестаты соответствия продолжают сохранять юридическую силу в течение установленного срока их действия, при условии соблюдения требований к эксплуатации и изменению конфигурации систем. Тем самым в нормативном виде закрепляется последовательность: первичное выполнение установленных требований по защите информации, а затем – прохождение процедуры аттестации как формы внешнего подтверждения соответствия для ГИС.

Для иных информационных систем государственных органов, государственных учреждений и государственных унитарных предприятий аттестация не устанавливается в качестве обязательной процедуры, однако возлагается обязанность реализации всех предусмотренных приказом мер защиты, включая применение сертифицированных СрЗИ, ведение эксплуатационной документации и обеспечение контроля соответствия.

Приказ ФСТЭК России № 117 значительно расширяет и углубляет требования по сравнению с [Приказом ФСТЭК России от 11.02.2013 № 17](#) «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в ГИС», делая акцент на процессное управление ИБ, актуальность угроз, контроль исполнения и внедрение современных технологий.

Управление уязвимостями, тестирование и оценка защищенности

Изменения 2025 года в области управления уязвимостями, тестирования и оценки защищенности отражают общий сдвиг надзорной логики от формальной проверки наличия мер к оценке реальной способности организаций выявлять, приоритизировать и устранять технические риски. Контролирующие органы все в меньшей степени интересуются разовыми мероприятиями и все в большей – устойчивостью и воспроизводимостью процессов.

Ключевым элементом этой трансформации стало утверждение ФСТЭК России [методики оценки критичности уязвимостей](#) в 2025 году. Документ формализует подходы к определению значимости уязвимостей и устраняет ранее распространенную практику субъективной приоритизации. Критичность уязвимости теперь должна определяться не абстрактно, а с учетом контекста конкретной информационной системы, ее архитектуры, категории значимости и потенциальных последствий эксплуатации. Тем самым управление уязвимостями напрямую увязывается с моделями угроз, категорированием и требованиями к реагированию.

Практическое значение методики заключается в том, что она задает проверяемый стандарт. Решения об отсрочке устранения уязвимостей, выборе компенсирующих мер или принятии рисков должны быть обоснованы и документированы. Формальный перечень выявленных уязвимостей без выстроенной логики их обработки перестает восприниматься как достаточная мера

соответствия требованиям.

Дополняющим элементом стали методические рекомендации по проведению тестирований на проникновение, опубликованные ФСТЭК России в [Информационном сообщении ФСТЭК России от 08.09.2025 № 240/24/4734](#). Указанная Методика имеет ограничительный гриф (для служебного пользования), предназначена для применения в ГИС и иных информационных системах государственных органов и предоставляется организациям по официальному запросу в ФСТЭК России. Документ определяет порядок проведения испытаний, требования к объему и глубине тестирования, а также правила оформления результатов и использования выводов при оценке эффективности реализованных мер защиты. Также ФСТЭК России утвердила [Методику анализа защищенности информационных систем](#), введенную в действие 25.11.2025. Документ устанавливает единый подход к организации и проведению работ по выявлению уязвимостей в информационных системах, включая автоматизированные системы управления, информационно-телекоммуникационные сети и системы обработки персональных данных (далее – ПДн). Методика разработана в соответствии с требованиями [приказа ФСТЭК России от 29.04.2021 № 77](#) «Об утверждении порядка организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну» и предназначена для использования в ходе аттестации объектов информатизации, контроля защищенности информации и оценки соответствия установленным требованиям.

Параллельно ФСТЭК России утвердила новый обязательный [методический документ](#) – методику для самооценки и контроля уровня защиты информации информационных ресурсов и объектов КИИ, предусматривающую расчет показателя защищенности (КЗИ) по шкале от 0 до 1. Данная методика заменила ранее действовавший документ аналогичного назначения и определила порядок расчета КЗИ для государственных органов, субъектов КИИ и иных организаций, подпадающих под требования ФСТЭК России.

В совокупности с изменениями, внесенными осенью 2025 года в [порядок сертификации процессов разработки безопасного ПО](#) (далее – РБПО), включая обновление нормативных ссылок, уточнение требований к руководству по безопасной разработке, корректировку оформления документации и пересмотр срока действия сертификата, формируется единая логика оценки защищенности информационных систем. В рамках обновлённой процедуры сертификация теперь проводится на материально-технической базе изготовителя на территории РФ с обеспечением доступа сертифицирующего органа к средам разработки и сборки, а сама проверка была расширена за счёт оценки руководства по безопасной разработке, артефактов процессов, применяемых инструментов анализа программного обеспечения, инструментального контроля и проверки компетентности персонала. Сертификат выдается на срок, указанный в заявке, но не более 5 лет, и в пределах области действия, определённой в руководстве по безопасной разработке.

Для организаций такие изменения в регулировании РБПО и оценки защищенности означают необходимость перехода от эпизодических проверок к постоянным процессам. Наличие отчета о пентесте или результатов сканирования уязвимостей само по себе больше не гарантирует соответствие требованиям. Критичным становится умение показать, каким образом результаты таких мероприятий используются для принятия управленческих решений, корректировки архитектуры и повышения уровня защищенности в динамике.

Персональные данные

Изменения регулирования обработки ПДн в 2025 году носили точечный характер и были сосредоточены преимущественно на вопросах обезличивания информации. В развитие соответствующих законодательных поправок были приняты [постановление Правительства РФ № 1154](#) «Об утверждении требований к обезличиванию персональных данных, методов обезличивания персональных данных и Правил обезличивания персональных данных», устанавливающее обязательные требования к процессам обезличивания ПДн, а также [приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций \(далее – Роскомнадзор\) от 19.06.2025 № 140](#) «Об утверждении требований к обезличиванию ПДн и методов обезличивания персональных данных, за исключением случаев, указанных в пункте 9.1 части 1 статьи 6 Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных» (далее – 152-ФЗ)». Приказ Роскомнадзора отменяет ранее действовавший документ ([приказ Роскомнадзора от 05.09.2013 № 996](#)).

Одним из ключевых событий стало расширение полномочий Роскомнадзора по установлению требований к обезличиванию ПДн, оформленное в 2025 году. Если ранее регулирование в этой сфере во многом опиралось на методические рекомендации и допускало широкий диапазон интерпретаций, то новые полномочия фактически переводят обезличивание в режим нормируемого процесса. Это означает, что выбор методов, глубина обезличивания и оценка рисков повторной идентификации перестают быть исключительно зоной усмотрения оператора и становятся предметом надзорного контроля.

Практическим следствием данных изменений становится рост требований к методической и технической проработке процессов обезличивания. Формальный подход, при котором обезличивание рассматривалось как разовая процедура для вывода данных из-под действия законодательства о ПДн, становится неустойчивым. Операторы вынуждены документировать выбранные методы, обосновывать их достаточность и обеспечивать воспроизводимость результатов, в том числе в рамках проверок и разбирательств.

Дополнительно в [152-ФЗ](#) были внесены [изменения](#), предусматривающие обязанность оформлять согласие субъекта ПДн в виде отдельного документа, не включённого в иные договоры, соглашения или пользовательские условия, что усиливает требования к юридическому оформлению процессов обработки ПДн.

Дополняющим элементом трансформации регулирования стал [Федеральный закон от 01.04.2025 № 41-ФЗ](#) «О создании государственной информационной системы противодействия правонарушениям, совершаемым с использованием информационных и коммуникационных технологий, и о внесении изменений в отдельные законодательные акты Российской Федерации» (далее – 41-ФЗ). Закон существенно расширил обязанности операторов и владельцев информационных систем в части выявления и предотвращения правонарушений, совершаемых с использованием информационных и коммуникационных технологий, включая мошеннические действия и иные формы противоправной активности в цифровой среде. Важной особенностью документа является смещение фокуса с последствий инцидентов на превентивные меры и постоянный мониторинг аномалий и подозрительной активности. Помимо расширения обязанностей операторов и владельцев информационных систем в части выявления и предотвращения инцидентов, статья 15 указанного закона установила запрет на использование иностранных мессенджеров и иных систем обмена сообщениями при информировании граждан РФ, а также ввела специальные

требования для сервисов размещения объявлений и иных цифровых платформ, включая реализацию возможности по использованию механизмов идентификации через Единую биометрическую систему.

В совокупности изменения в регулировании ПДн и меры по борьбе с кибермошенничеством формируют единый контур требований, в котором защита данных рассматривается не изолированно, а как элемент общей системы управления рисками. Для организаций это означает необходимость пересмотра моделей обработки данных, интеграции процессов защиты персональных данных с инцидент-менеджментом и более тесного взаимодействия между юридическими, ИБ-подразделениями.

Недопустимые события и реагирование

Развитие нормативных подходов к понятию недопустимых событий и организации реагирования на инциденты является логическим продолжением реформирования системы обеспечения безопасности критических и государственных информационных ресурсов. **Методические рекомендации**, разработанные в целях оказания методологической помощи операторам информационных систем, за исключением информационных систем критически важных объектов и объектов КИИ.

Методические рекомендации закрепляют понятийный аппарат, включая определения недопустимого события, вектора компьютерной атаки и критериев реализации недопустимых событий, а также ориентированы на формирование перечней событий, способных привести к прерыванию операционной деятельности организаций.

Принципиальным элементом документа является смещение акцента на обеспечение непрерывности операционной деятельности, а не исключительно на технические аспекты защиты информации. В рекомендациях предусмотрено формирование постоянно действующих рабочих групп с участием подразделений по управлению рисками, ИТ-функции и ИБ, применение сценарного моделирования с имитацией компьютерных атак, а также использование критериев реализации недопустимых событий, связанных с получением доступа к операционным системам, прикладному ПО, сетевым сегментам и документам.

Документ носит рекомендательный характер, не вводит самостоятельных юридических обязанностей и прямо указывает, что не распространяется на объекты КИИ, а также не подменяет требования нормативных правовых актов в области защиты информации, оставляя выбор конкретных защитных мер за организацией.

Заключение

Итоги 2025 года в сфере нормативного регулирования ИБ свидетельствуют о системном уплотнении требований, охватывающих защиту КИИ, ГИС, обработку ПДн, РБПО, управление уязвимостями и функционирование механизмов реагирования на компьютерные атаки и инциденты. В течение года происходила не просто актуализация отдельных нормативных правовых актов, а последовательное выстраивание взаимосвязей между федеральными законами, постановлениями Правительства РФ и ведомственными документами, формирующими единый контур регулирования.

Центральную роль в этой трансформации сыграли изменения в 187-ФЗ и 149-ФЗ. Закрепление в 187-ФЗ требований по переходу на доверенные программно-аппаратные комплексы и ориентации на использование отечественного ПО, развитие механизмов ГосСОПКА, институционализация отраслевых перечней объектов КИИ и особенностей их категорирования, а также корректировка правил категорирования через подзаконные акты Правительства РФ сформировали более структурированную модель управления рисками в сфере КИИ. Параллельно уточнение правового режима ГИС и принятие приказа ФСТЭК России № 117 расширили круг систем государственных органов и организаций, в отношении которых обязательны меры защиты информации и применение сертифицированных СрЗИ, при сохранении аттестации как обязательной процедуры исключительно для ГИС.

Отдельным направлением консолидации требований стало развитие регулирования в области импортозамещения и допустимости использования программных продуктов. Повышение административной ответственности за применение несертифицированных СрЗИ, появление законодательных предпосылок для ведения реестра доверенного ПО и подготовки отдельного регулирования в отношении разработанного для собственных нужд ПО, а также ожидаемые подзаконные акты в сфере перехода на отечественные решения на значимых объектах КИИ указывают на формирование устойчивой связки между происхождением программных продуктов, их правовым статусом и возможностью эксплуатации в критичных и государственных системах.

В сфере управления уязвимостями и оценки защищённости наблюдается закрепление процессного подхода. Методики ФСТЭК России по оценке критичности уязвимостей, анализу защищённости, расчёту показателей защищённости, а также обновление порядка сертификации процессов РБПО формируют модель, в которой внимание смещается от разовых мероприятий к воспроизводимым циклам выявления рисков, их обработки и подтверждения эффективности реализованных мер.

Изменения в регулировании обработки ПДн носили более узкий, но содержательный характер. Введение обязательных требований к обезличиванию через постановление Правительства РФ и приказы Роскомнадзора, корректировка правил получения согласия субъектов ПДн, а также 41-ФЗ о противодействии киберпреступлениям и ограничении использования иностранных коммуникационных сервисов при взаимодействии с гражданами дополнили общую архитектуру требований в части защиты информации и предотвращения злоупотреблений.

Методические рекомендации Минцифры России по формированию перечней недопустимых событий дополнили данный контур, задав ориентиры для государственных организаций в части обеспечения непрерывности операционной деятельности и сценарного анализа рисков, при этом сохранив рекомендательный характер и разграничение с обязательными режимами регулирования в сфере КИИ.

Для организаций совокупность изменений 2025 года означает необходимость перехода от фрагментарного соблюдения отдельных требований к комплексному управлению соответствием. Возрастает значение инвентаризации информационных систем и используемого ПО, синхронизации программ импортозамещения с требованиями по защите информации, выстраивания процессов реагирования на инциденты и управления уязвимостями, а также документирования архитектурных решений и управленческих процедур.

В более широком контексте 2025 год можно рассматривать как этап институционального закрепления риск-ориентированной и процессной модели обеспечения ИБ, в которой норматив-

ные требования всё в большей степени ориентируют организации на устойчивость, управляемость и проверяемость систем защиты, а не на формальное наличие отдельных документов или сертификатов. Именно эта логика, по-видимому, будет определять дальнейшее развитие регулирования в последующие периоды.

**Наталья Лабынцева**

Автор отчета, ведущий консультант по информационной безопасности «КИТ»

**Евгений Баклушин**

Редактор отчета, директор «КИТ», автор блога **BESSEC**

«КИТ» — поставщик профессиональных сервисов в области кибербезопасности, цифровой трансформации и ИИ



Мы обеспечиваем независимость бизнеса в цифровой среде через безопасность — от аудита текущего состояния до комплексного внедрения решений.

Консалтинг ИБ

- Категорирование объектов КИИ
- Аудит информационной безопасности
- Консалтинг по защите персональных данных
- Разработка концепции / стратегии развития ИБ
- Сопровождение по получению лицензий в области ИБ
- Разработка организационно-распорядительной документации

Архитектура ИБ

- Проектирование архитектуры системы ИБ и ее подсистем
- Внедрение средств и систем ИБ
- Консалтинг по импортозамещению
- Аттестация объектов информатизации

Тестирование на проникновение

- Оценка возможности реализации недопустимых событий
- Тестирование на проникновение
- Тестирование безопасности веб-приложений и сайтов
- Аттестация объектов информатизации

Цифровая трансформация

- Оценка готовности и внедрение ИИ
- Оценка кибербезопасности ИИ
- Разработка стратегии цифровой трансформации
- Анализ производственных данных
- Построение киберполигонов