КРОСС
ТЕХНОЛОДЖИС



Регуляторный патч

Дайджест изменений законодательства
в сфере ИБ за 3 квартал

2025

Вступительное слово



Катерина Сашенко

Руководитель департамента аудита,
консалтинга и оценки соответствия

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.

Содержание

- ФСТЭК утвердила методику проведения пентеста в госорганизациях
- Субъектам КИИ дали еще 2 года на обновление порядка подключения к ГосСОПКА
- Перевод значимых объектов КИИ на отечественное ПО получит новые дедлайны и наполнение

ФСТЭК утвердила методику проведения пентеста в госорганизациях

Информационное сообщение ФСТЭК России от 08.09.2025 № 240/24/4734

Открыть документ

Для кого актуально

Для госорганов, ГУП и любых других госучреждений, у которых на балансе есть ГИС 1, 2 классов защищенности, имеющие выход в интернет или связи с другими информационными системами.

Исключение сделано для взаимодействий, организованных с применением сертифицированных СКЗИ.



Анастасия Мельникова
руководитель департамента оценки защищенности

Решение ФСТЭК о введении методики пентеста показывает, что регулятор идёт в сторону практической защищённости, а не формального соответствия.

Ценность пентеста определяется не только фактом его проведения, но и качеством исполнения.

Напрямую на результат влияют корректно заданные границы тестирования, реалистичные сценарии атак и квалификация исполнителей.

Ключевые ошибки — выбор формального подхода и недооценивание специфики ГИС, тогда уязвимости остаются незамеченными, а риски — неуправляемыми.

Детали

Госорганам понадобятся дополнительные бюджеты на ИБ для проведения пентеста.

Сейчас, если говорить о регулярных проверках, закон обязывает их проводить функциональное тестирование систем защиты информации и анализ уязвимостей с использованием сканеров, пентест станет третьим направлением проверки.

Рекомендуемые шаги

- Определить состав информационных систем, для которых требуется провести процедуры аттестации или контроля защищенности в отчетный период (1 год).
- Для выбранных систем определить перечень сервисов, имеющих выход в Интернет, белых IP и т.д.
- Указать полученные сведения при формировании технических заданий на проведение аттестационных испытаний или контроля защищенности. Это поможет получить объективную оценку стоимости работ.

Рекомендуем проводить регулярные пентесты до аттестации систем, чтобы успеть исправить уязвимости до начала аттестации. Хорошая периодичность – не реже раза в год.

Субъектам КИИ дали еще 2 года на обновление порядка подключения к ГосСОПКА

Приказ ФСБ РФ
от 21.07.2025 № 282

Открыть документ

Детали

Ранее предполагалось, что к 2025 году субъекты КИИ перейдут на отечественные решения для предоставления сведений в ГосСОПКА.

Теперь срок продлили до 13 декабря 2027 года. У организаций, которые еще не выполнили требование, два пути:

01.

Создание и аккредитация собственного центра ГосСОПКА с использованием отечественных продуктов

02.

Заключение соглашений со сторонним уже существующим аккредитованным центром

Рекомендуемые шаги

- Оценить текущий порядок взаимодействия с НКЦКИ и его соответствия требованиям.
- Провести оценку ресурсов для реализации одного из вариантов правомерного представления сведений в ГосСОПКА.
- Выбрать оптимальный вариант и осуществить его реализацию до 13 декабря 2027 года.



Михаил Назаров
директор по сервису компании «ЕСА ПРО» (входит в ГК «Кросс технолоджис»)

При выборе подхода важно учесть, что создание своего центра – трудоёмкий процесс. Компании предстоит построить центр мониторинга инцидентов (SOC) или перевести существующий на российские решения, разработать нормативные документы, описать процессы, собрать команду специалистов для уровней L1-L3. Кроме того, для центров регламентируются сроки реагирования и уведомления НКЦКИ об инцидентах.

С учётом перечисленных факторов даже крупные компании сегодня выбирают подключение к сторонним аккредитованным центрам — это позволяет сэкономить ресурсы, повысив защищённость. В ЕСА ПРО функционирует такой центр, и мы фиксируем рост спроса на его услуги ввиду последних законодательных изменений.

Самостоятельное подключение к НКЦКИ может быть применимо для компаний, у которых есть свой in-house SOC, но даже в этом случае экономические преимущества не очевидны

Перевод значимых объектов КИИ на отечественное ПО получит новые дедлайны и наполнение

Проект постановления вынесен на обсуждение

Открыть документ

Детали

Помимо обязательных для всех субъектов КИИ требований по переходу на доверенные ПАК (с 1 апреля 2026 года), значимые объекты КИИ (ЗОКИИ) предлагается перевести на российское ПО, зарегистрированное в соответствующем реестре (РПО или реестровое ПО). Сроки перехода — не позднее 1 января 2028 г. (в отдельных случаях предусмотрен срок до 2030 г.)



Катерина Сашенко
Руководитель департамента аудита, консалтинга и оценки соответствия

Рекомендуем субъектам КИИ заблаговременно оценить долю РПО на принадлежащих значимых объектах КИИ, а также принять активное участие в обсуждении настоящего проекта на Федеральном портале проектов нормативно правовых актов

Рекомендуемые шаги

- Дождаться отраслевого плана по переходу на РПО.
- В течение 1-2 месяцев после получения отраслевого плана провести инвентаризацию ИТ-активов значимых объектов КИИ. Если понадобится переход на РПО — оценить затраты и предельные сроки, чтобы составить и утвердить план для вашей организации.
- По результатам перехода на РПО в срок до 1 января 2028 года предоставить отчетность.

Если для существующего ПО в реестре нет аналога по функциональным, техническим и эксплуатационным характеристики, нужно будет до 1 августа 2026 г. уведомить об этом отраслевые уполномоченные органы.

Тогда срок перехода может быть сдвинут, но не далее, чем на 1 декабря 2030 г.

КРОСС
ТЕХНОЛОДЖИС

Поможем подготовиться к изменениям

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

Написать