КРОСС
ТЕХНОЛОДЖИС

Регуляторный патч

Дайджест изменений законодательства
в сфере ИБ за 4 квартал 2025 года

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 опубликовала методику анализа защищенности* информационных систем

Методический документ от 25 ноября 2025 г.

Открыть документ

Методика смещает акцент

с формального выявления недостатков на оценку реальной возможности их эксплуатации с учетом особенностей архитектуры системы, сценариев атак и модели угроз. Она формирует понятную основу для выстраивания зрелого процесса управления уязвимостями — от технического анализа до приоритизации устранения и повторной проверки

Для кого актуально

Переводя с юридического языка на деловой, для владельцев государственных информационных систем, а также ИСПДн, объектов КИИ, АСУ ТП, аттестованных или подлежащих аттестации на соответствие требованиям по защите информации

Детали

- Раньше анализ был сфокусирован на проведении внутреннего сканирования информационных систем. Теперь, сверх этого, методика требует проведения внешнего сканирования – в периметр попадают все серверы и системы, которые имеют выход за пределы сети организации или «общаются» с ней из Интернета. В методике прописаны границы (проверяемые объекты) сканирования и выполняемые работы
- В методике закрепляется возможность применения дополнительных инструментальных средств анализа уязвимостей, включая несертифицированные и собственные разработки, что при обоснованном использовании позволяет существенно повысить глубину и качество обследования. Это особенно важно для проверки внешнего периметра, которую трудно провести сертифицированными средствами
- Облегчена проверка типовых рабочих мест. Если в компании существуют места с одинаковой архитектурой и настройками ПО, например корпоративные ноутбуки, можно проверить только 30%, а не все 100, как было раньше
- Прописаны требования к анализу уязвимостей ПО с моделями машинного обучения (ML)
- Определены требования к конфиденциальности результатов анализа уязвимостей. Что особенно важно – указана необходимость передачи данных по защищенным каналам
- Представлена структура отчетного документа по результатам анализа уязвимостей

* Под анализом защищенности понимается не пентест, а процесс выявления уязвимостей в программном обеспечении, сетевом и серверном оборудовании, а также недостатков их конфигурации и других аспектов, связанных с требованиями информационной безопасности, которые изложены в методике.

Ашраф Садыхбеков

Ведущий аудитор департамента консалтинга,
аудита и оценки соответствия

Анализ уязвимостей перестает быть разовой процедурой «для отчета» и становится инструментом оценки реальных рисков. Прежде всего, мы прогнозируем, что с принятием методики возрастет роль инвентаризации, корректного определения границ анализа и последующего устранения уязвимостей с обязательной повторной проверкой.

Организациям с высоким уровнем зрелости ИБ методика гарантирует более прогнозируемый и управляемый результат, менее зрелым — выявление системных пробелов в управлении уязвимостями.

В краткосрочной перспективе у части организаций возможен рост затрат — за счет расширения глубины анализа, вовлечения внутренних команд и устранения накопленных уязвимостей.

В среднесрочной перспективе методика, напротив, позволит оптимизировать бюджеты: допускается сокращение объемов типового сканирования (например, по АРМ), а приоритизация уязвимостей строится от реальных рисков, а не «количества находок». Это сокращает количество избыточных работ и фокусирует ресурсы на действительно критичных проблемах

Рекомендуемые шаги

- Продолжать регулярно проводить сканирование уязвимостей инфраструктуры и устранять проблемы. Если вы еще этого не делали, то начать проводить проверки
- Определить во внутренних стандартах и регламентах возможность (или невозможность) применения дополнительных инструментов для проведения анализа уязвимостей, помимо сертифицированных ФСТЭК. Чтобы расширить перечень инструментов, можно ссылаться на методику

С чего начать анализ защищенности информационных систем

01.

Провести инвентаризацию ИС и инфраструктуры

02.

Пересмотреть границы анализа и модели угроз

03.

Закрепить процесс устранения уязвимостей и повторной проверки

04.

Актуализировать внутренние регламенты управления уязвимостями

При необходимости к процессу можно привлечь проверенного интегратора. Наша команда на регулярной основе проводит подобные тесты для заказчиков различного масштаба. Будем рады вам помочь

ФСБ предлагает изменить требования к центрам ГосСОПКА и порядок получения аккредитации

Проект приказа ФСБ РФ

Открыть документ

В ноябре была опубликована третья версия проекта соответствующего приказа ФСБ России: она ужесточает требования к численности и образованию сотрудников. В перспективе это позволит повысить защищенность организаций на фоне растущего количества кибератак. Обратная сторона медали – усиление дефицита кадров и рост затрат на услуги корпоративных центров ГосСОПКА

Сергей Козлов

Руководитель центра кибербезопасности
Кросс технолоджис

Новый приказ потребует увеличения численности штата центров ГосСОПКА примерно в 2 раза, поскольку устанавливается запрет на совмещение должностей (за исключением роли замруководителя).

В случае с полным функционалом центр ГосСОПКА потребует минимум 17 человек, что может привести к росту ФОТ и увеличению сроков закрытия вакансий. Компаниям будет сложнее получить аккредитацию на внутренний центр ГосСОПКА, а подключение к внешнему станет дороже

Для кого актуально

Для тех, кто планирует создать свой центр, а также для владельцев центров ГосСОПКА, уже имеющих заключенные с НКЦКИ соглашения о сотрудничестве

Детали

- Определены процедура аккредитации и порядок ее приостановления
- Представлены формы заявления на аккредитацию и декларации о соответствии организаций требованиям к центрам ГосСОПКА
- Представлены требования к центрам, в том числе по обеспечению информационной безопасности их ресурсов. Среди обязательных: применение средств антивирусной защиты информации, межсетевого экранирования и обнаружения вторжений, имеющих сертификаты соответствия ФСБ России
- Подробно указаны требования к компетенциям работников
- Определен срок действия аттестата аккредитации – 5 лет

Ждем финальную версию документа. Как только она появится, оповестим вас о ключевых особенностях

Рекомендуемые шаги

01.

Необходимо еще до утверждения приказа провести оценку кадрового состава и технической оснащенности центра ГосСОПКА, а также соответствия иным требованиям

02.

В случае выявления недостаточной реализации отдельных требований определить план работ в переходный период для успешного прохождения аккредитации: бюджетирование закупок, открытие дополнительных вакансий и т.п.

03.

Отслеживать появление новых версий проекта приказа, чтобы быть готовыми к переменам

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