F6

Консалтинг ИБ

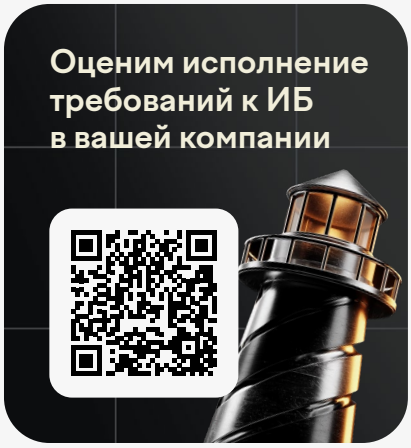
Чек-лист

Приказ ФСТЭК России от 11.04.2025 № 117

Попадает ли ваша информационная система под действия приказа ФСТЭК России от 11.04.2025 № 117?

Приказ № 117 применяется:

- к государственным информационным системам (ГИС);
- к иным ИС государственных органов;
- к ИС государственных учреждений и унитарных предприятий, функционирующих на территории Российской Федерации;
- к муниципальным ИС (если иное не установлено законодательством Российской Федерации);
- к ИС, получающим сведения ограниченного доступа из ГИС.



Приказ № 117 не применяется, если ИС относится:

- к системам Администрации Президента РФ, Совета Безопасности РФ, ФСБ, Правительства РФ;
- к системам Конституционного Суда РФ или Верховного Суда РФ;
- к разведывательным и контрразведывательным системам;
- к системам управления вооружением, военной и специальной техникой;
- к ИС, обрабатывающим сведения, составляющие государственную тайну.

Функционирование ИС, использующих информационно-телекоммуникационную инфраструктуру (ИТКИ), что подразумевает архитектуру ИС на базе центра обработки данных или облачной инфраструктуры, допускается лишь при условии, что сама инфраструктура защищена в соответствии с Приказом № 117.

Чек-лист

Общие положения

- ◯ **При обработке ПДн** в ИС применяются одновременно Постановление Правительства РФ № 1119 и настоящие Требования.
- ◯ **Для значимых объектов КИИ РФ** защита информации обеспечивается по НПА, принятым во исполнение 187-ФЗ, и настоящим Требованиям.
- ◯ **При применении СКЗИ** должны выполняться требования ФСБ России (ч. 5 ст. 16 № 149-ФЗ) и настоящие Требования.
- ◯ Оператор (обладатель информации) **осуществляет защиту** с целью недопущения (снижения возможности) негативных последствий от нарушения конфиденциальности, целостности, доступности информации и от нарушения функционирования ИС.
- ◯ Оператор **определяет цели защиты информации**; негативные последствия определяются на основе банка данных угроз ФСТЭК; задачи защиты должны обеспечивать достижение целей защиты информации.

Документальные меры по защите информации

- ◯ **Разработана и утверждена политика защиты информации**, учитывающая все ИС оператора и, при наличии, ИТКИ; в политике определены область действия, перечни информации, ИС и элементов ИТКИ, цели и задачи, принципы защиты информации, объекты защиты и обязанности лиц; политика утверждена руководителем (ответственным лицом) и обязательна для всех подразделений и работников.
- ◯ **Разработаны и утверждены внутренние стандарты, регламенты по защите информации**, устанавливающие требования к идентификации и использованию учётных записей, моделям доступа, перечням разрешённого и запрещённого ПО, типовым конфигурациям и настройкам средств, а также описывающие процессы защиты информации с учётом особенностей деятельности и ИС; документы утверждены руководителем (ответственным лицом), для них определена область действия.
- ◯ Подрядные организации, которым предоставляется доступ к ИС/информации или передаётся информация, **ознакомлены с политикой ЗИ** в части, их касающейся; **обязанность** её выполнения **закреплена** в договорах/документах.
- ◯ Внутренние стандарты и регламенты **доведены до пользователей и подрядчиков** (в части, их касающейся); пользователи обязаны их исполнять; исполнение подрядчиками закреплено в документах.

- ◯ **Оператор определяет** показатели: состояние защищённости от базового уровня угроз и уровень зрелости процессов ЗИ; расчёт по методическим документам ФСТЭК (Указ Президента РФ от 16.08.2004 № 1085, пп. 4 п. 8, 5 Положения).
- ◯ Состояние защищённости рассчитывается не реже **1 раза в 6 месяцев**, уровень зрелости – не реже **1 раза в 2 года**; при несоответствии нормируемым значениям руководитель информируется в течение **3 календарных дней**; значения направляются в ФСТЭК не позднее **5 рабочих дней** после расчёта.
- ◯ При необходимости **разрабатывается и реализуется** план мероприятий по совершенствованию ЗИ (с мероприятиями, сроками, ответственными), обеспечивающий достижение нормированных значений состояния защищённости и уровня зрелости; план доводится до подразделений.

Организационные меры по защите информации

- ◯ Оператор (обладатель информации) **организует деятельность по защите информации** в ИС и **управляет ею на всех стадиях жизненного цикла** (создание, развитие, эксплуатация, вывод из эксплуатации) в соответствии с Требованиями.
- ◯ Руководитель оператора **организует защиту информации** или **назначает ответственное лицо**; **определены** лица, ответственные за защиту информации.
- ◯ **Оператор выделяет** организационные, технические и иные ресурсы, необходимые для защиты информации.
- ◯ Обязанности и полномочия ответственного лица по организации, управлению и контролю защиты информации **включены в его должностные обязанности**; их **объём достаточен** для реализации Требований.
- ◯ **Создано структурное подразделение по ЗИ** или назначены специалисты по ЗИ; их функции и полномочия определены локальными актами; объём обязанностей достаточен для выполнения мероприятий и мер по ЗИ. Возможно возложение функций на уже существующее подразделение ИБ.
- ◯ Работники подразделения по ЗИ **обладают необходимыми компетенциями**; не менее **30%** имеют **профильное образование/профпереподготовку** по ИБ.
- ◯ Подразделение по ЗИ **обеспечивает** ЗИ при взаимодействии с подразделениями-пользователями ИС и подразделениями эксплуатации.

- ◯ Подразделения-пользователи ИС и подразделения эксплуатации **участвуют** в мероприятиях и мерах по ЗИ в объёме, установленном внутренними стандартами/регламентами.
- ◯ По решению оператора **привлекаются** лицензированные специализированные **организации по ТЗКИ**; их функции и используемые средства **определяются оператором**; работники подразделения по ЗИ **участвуют в приёмке** результатов.
- ◯ Подразделение по ЗИ **готовит обоснованные предложения** по необходимым ресурсам (организационным, материально-техническим и др.) с указанием целей ЗИ и прогнозируемых негативных последствий при их отсутствии; руководитель/ответственное лицо обеспечивает выделение ресурсов.
- ◯ **Функционирует** организационная система управления деятельностью по ЗИ, возглавляемая руководителем/ответственным лицом; включает планирование, реализацию, оценку состояния ЗИ и совершенствование мер.
- ◯ При планировании мероприятий и мер по ЗИ **определяются**: события в ИС, ведущие к нарушению целей ЗИ; ИС и компоненты, критичные с точки зрения ЗИ; актуальные угрозы; состав, сроки и ресурсы мероприятий и мер.
- ◯ Мероприятия и меры по ЗИ **направлены на блокирование** (нейтрализацию) **актуальных угроз**. (Подробнее в Приказе ФСТЭК №117 п. 30 Требований).

Технические меры по защите информации

- ◯ Подразделение по ЗИ **использует ПО и ПАК**, **обеспечивающие**: выявление угроз и вторжений, контроль уровня защищённости, мониторинг ИБ, выявление уязвимостей, контроль настроек и конфигураций, автоматизацию ЗИ. **Состав средств определён** во внутренних документах.

Проведение мероприятий по оценке защиты информации

- ◯ Достаточность и эффективность мероприятий (процессов) по ЗИ **оцениваются по показателю уровня зрелости**.

Выявление и оценка угроз

- ◯ При создании ИС **определены актуальные угрозы**, **для ГИС разработана модель угроз** в соответствии с ПП РФ № 676; в эксплуатации **обеспечивается** своевременное выявление актуальных угроз, их приоритизация, оповещение подразделений, принятие мер по блокированию/нейтрализации при наличии признаков реализации.

Управление конфигурациями, уязвимостями и обновлениями

- ◯ **Организован контроль конфигураций ИС**, исключающий несанкционированное изменение состава ПО/ПАК, настроек и конфигураций, предусмотренных внутренними стандартами; обеспечивается обнаружение фактов несанкционированных изменений и причин; используется учёт ИТ-активов и/или системы инвентаризации, к которым подразделение ЗИ имеет доступ.
- ◯ **Реализовано управление уязвимостями**: выявление уязвимостей, оценка критичности, определение методов и приоритетов устранения, контроль устранения; уязвимости критического уровня устраняются или компенсируются не более **24 часов**, высокого уровня не более **7 календарных дней**; сроки по средним/низким уровням определены во внутренних регламентах; при выявлении «новых» уязвимостей информация о них в течение **5 рабочих дней** направляется в ФСТЭК для включения в БДУ.
- ◯ **Реализовано управление обновлениями**: проверка подлинности и целостности обновлений; тестирование до применения в промышленном контуре; выдача разрешений на установку с учётом безопасных настроек; бесконтрольная установка обновлений не допускается; сроки применения обновлений, устраняющих уязвимости, установлены во внутренних регламентах с учётом уровней опасности и рисков.

Управление доступом

- ◯ **Организована защита при обработке, хранении и обращении с информацией ограниченного доступа**. (Подробнее в Приказе ФСТЭК №117 п. 40 Требований).
- ◯ **Обеспечена защита информации при применении конечных устройств**. (Подробнее в Приказе ФСТЭК №117 п. 41 Требований).
- ◯ **Обеспечена защита при использовании мобильных устройств для доступа к ИС**: исключён НСД/воздействие через каналы мобильной связи, сервисы, интерфейсы и порты; обеспечена защита каналов передачи данных; используется строгая аутентификация; пользователи обязаны исключить НСД к своим мобильным устройствам.

- ◯ Использование личных мобильных устройств для доступа к ИС допускается только при **соответствии Требованиям** и наличии у оператора технической и организационной **возможности контроля** такого использования.
- ◯ Контроль использования мобильных устройств (служебных и личных, применяемых для доступа к ИС) **организован** в соответствии с внутренними стандартами и регламентами по ЗИ.
- ◯ При использовании мобильных устройств для доступа к ИС вне служебных обязанностей (в т. ч. к общедоступной информации) **оператор принимает меры по защите ИС** и при необходимости обеспечивает защиту каналов передачи данных.
- ◯ **Организована защита при удалённом доступе**: исключён НСД через каналы и интерфейсы, каналы связи и средства защищены; служебный доступ осуществляется с использованием выделенных и сертифицированных средств в сетях РФ с СЗИ и строгой аутентификацией, контроль ведётся по внутренним документам. (Подробнее в Приказе ФСТЭК №117 п. 46 Требований).
- ◯ **Обеспечена защита при беспроводном доступе**: исключён НСД через подключение к точкам доступа или подмену средств; каналы и средства защищены, точки доступа идентифицированы и размещены в установленных местах, служебные сети изолированы от общедоступных. (Подробнее в Приказе ФСТЭК №117 п. 47 Требований).
- ◯ **Обеспечена защита при предоставлении привилегированного доступа**: исключено получение и злоупотребление правами, применяются персонифицированные учётные записи с минимальными правами и строгой (многофакторной) аутентификацией; роли не совмещаются, неиспользуемые записи блокируются, все действия контролируются. (Подробнее в Приказе ФСТЭК №117 п. 48 Требований).

Мониторинг событий информационной безопасности

- ◯ **Организован мониторинг ИБ**: сбор, обработка и анализ событий безопасности; выявление признаков реализации угроз и нарушений внутренних требований; мониторинг проводится для всех ИС, кроме локальных/изолированных (в них обеспечивается контроль журналов); мониторинг ведётся согласно ГОСТ Р 59547-2021; допускается использование доверенных технологий ИИ; периодически формируется отчёт о результатах мониторинга с типами событий и инцидентами, рекомендациями; итоговый отчёт за год направляется в ФСТЭК.
- ◯ **Осуществляется взаимодействие с ГосСОПКА**: Обеспечено непрерывное взаимодействие с ГосСОПКА (подробнее в Приказе ФСТЭК №117 п. 59 Требований)

Безопасная разработка программного обеспечения

- ◯ При самостоятельной разработке ПО оператором **проводятся мероприятия по разработке безопасного ПО** в соответствии с ГОСТ Р 56939-2024 (разделы 4 и 5); при привлечении подрядчика в ТЗ могут устанавливаться требования по безопасной разработке по ГОСТ.

Физическая защита ИС

- ◯ **Обеспечена физическая защита ИС**: исключён несанкционированный физический доступ к средствам обработки и хранения информации, доступ предоставляется только при служебной необходимости; съёмные носители учитываются, контролируются и выдаются оператором, использование посторонних носителей запрещено. (Подробнее в Приказе ФСТЭК №117 п. 51 Требований).

Обеспечение непрерывности функционирования и резервного копирования

- ◯ **Обеспечена непрерывность функционирования ИС при нештатных ситуациях**: предусмотрена возможность восстановления выполнения значимых функций в пределах установленных интервалов времени.
- ◯ Оператор **устанавливает интервалы восстановления** значимых функций в зависимости от класса защищённости и значимости: для К1 не более **24 часов**, К2 не более **7 календарных дней**, К3 не более **4 недель**; интервалы отражаются во внутренних документах и актах создания/эксплуатации ИС или требованиях обладателя информации.
- ◯ Средства, обеспечивающие выполнение значимых функций, **развернуты** в отказоустойчивой конфигурации, гарантирующей восстановление в установленный интервал.
- ◯ **Организовано резервное копирование**: создаются и хранятся резервные копии ПО, ПАК, конфигураций и информации для значимых функций на защищённых носителях; периодичность, параметры резервирования и проверки восстановления определены во внутренних документах, проводятся регулярные тренировки по восстановлению. (Подробнее в Приказе ФСТЭК №117 п. 55 Требований).

Обучение пользователей

- ◯ **Организованы мероприятия по повышению уровня знаний и информированности пользователей по вопросам ЗИ**: доведение памяток/баннеров/буклетов; проведение лекций, семинаров, обучающих игр; имитационные рассылки писем для оценки устойчивости к социальной инженерии; тренировки по практической отработке мероприятий ЗИ.
- ◯ Способы обучения, периодичность и формы оценки знаний **определены** во внутренних регламентах; оценка проводится не реже **1 раза в 3 года** или **после компьютерного инцидента**; для пользователей с недостаточным уровнем знаний организуется повторное обучение.

Взаимодействие с подрядчиками

- ◯ **При взаимодействии с подрядчиками обеспечена ЗИ**: исключён НСД через средства и каналы подрядчиков, установлены требования к защите информации для подрядчиков, копирование информации допускается только при документальном закреплении; обработка данных у подрядчика ведётся с мерами ЗИ, определёнными оператором, разработки и тестирование подрядчика выполняются на изолированных стендах с контролируемым доступом. (Подробнее в Приказе ФСТЭК №117 п. 58 Требований).

Защита от DDoS и использование искусственного интеллекта

- ◯ **Обеспечена защита от DDoS-атак**: предотвращается блокировка доступа авторизованных пользователей, применяются меры фильтрации трафика с провайдерами, средства защиты размещены в РФ. (Подробнее в Приказе ФСТЭК №117 п. 59 Требований).
- ◯ **При использовании ИИ для функционирования ИС обеспечена защита от НСД** и воздействия через наборы данных, модели ИИ и их параметры, процессы и сервисы обработки и поиска решений; исключена передача разработчику модели ИИ информации ограниченного доступа из ИС, в том числе для улучшения модели.
- ◯ **При взаимодействии пользователей с сервисами на основе ИИ (запрос-ответ) определены и контролируются** шаблоны или допустимые тематики и форматы ответов, разрабатываются и применяются критерии выявления недостоверных ответов, предусмотрено реагирование на них; исключено нерегламентированное влияние ИИ на модель и ИС, используются доверенные технологии ИИ. (Подробнее в Приказе ФСТЭК №117 п. 61 Требований).

Реализация мер защиты ИС, контроль уровня защищённости и применение СЗИ

- ◯ **Реализация мер ЗИ в ИС** включает: реализацию базовых мер ЗИ по классам защищённости; адаптацию базовых мер к архитектуре и технологиям ИС; верификацию адаптированных мер с учётом актуальных угроз и возможностей нарушителей, их дополнение/усиление.
- ◯ Для ГИС до начала обработки/хранения информации **проводится аттестация** на соответствие Требованиям, аттестация осуществляется в соответствии с приказом ФСТЭК № 77; решение об аттестации иных ИС госорганов/ГУПов/госучреждений принимает руководитель/ответственное лицо.
- ◯ Контроль уровня защищённости информации **включает** оценку возможностей нарушения безопасности и функционирования ИС внутренними и внешними нарушителями; осуществляется методами: выявление уязвимостей и экспертная оценка их использования; выявление несанкционированных подключений устройств; тестирование ИС с моделированием угроз (в т. ч. на повышение привилегий); проведение тренировок по действиям при реализации угроз.
- ◯ Контроль уровня защищённости проводится не реже **1 раза в 3 года** или **после компьютерного инцидента**; методы и периодичность определены во внутреннем регламенте; по результатам составляется отчёт, подписываемый исполнителями, в течение **3 рабочих дней** направляемый руководителю/ответственному лицу; отчёт направляется в ФСТЭК в течение **5 рабочих дней** после завершения контроля.
- ◯ Мероприятия и меры по ЗИ **реализуются оператором** с использованием методических документов ФСТЭК России (Указ Президента РФ от 16.08.2004 № 1085, пп. 4 п. 8, 5 Положения).
- ◯ При невозможности реализации отдельных мероприятий/мер по ЗИ **разрабатываются и внедряются** компенсирующие меры, обеспечивающие блокирование актуальных угроз; их применение обосновывается на этапе создания ИС, а эффективность подтверждается при аттестации.
- ◯ Технические меры ЗИ **принимаются** на аппаратном, системном, прикладном уровнях и в ИТКИ; на аппаратном/системном уровнях используются встроенные средства ЗИ; на прикладном/сетевом — встроенные и/или наложенные и сетевые средства ЗИ.
- ◯ Для защиты **используются** сертифицированные СЗИ в соответствии с эксплуатационной документацией; разработчик обеспечивает поддержку безопасности (обновления для устранения уязвимостей/дефектов) на территории РФ; СЗИ применяются с учётом запретов, установленных Указом Президента РФ № 250 (п. 6).
- ◯ Классы и уровни доверия сертифицированных **СЗИ соответствуют**: для К1 не ниже **4 класса** защиты и уровня доверия; для К2 не ниже **5 класса**; для К3 **6 класс** защиты и уровень доверия.
- ◯ На стадиях жизненного цикла ГИС меры ЗИ **принимаются** в соответствии с ПП РФ № 676; для иных ИС в соответствии с ГОСТ Р 51583-2014 (раздел 5).

Требования к определению класса защищённости ИС

- ◯ **Определены виды информации**, обрабатываемой в ИС, и для каждого **вида установлены уровни значимости информации** (УЗ1–УЗ3) по конфиденциальности, целостности, доступности и функционированию ИС с указанием возможного ущерба.
- ◯ **Определён масштаб ИС** (федеральный, региональный или объектовый) с описанием территории/объектов, на которые распространяется функционирование ИС.
- ◯ **Присвоен класс защищённости ИС** (К1, К2 или К3) в соответствии с сочетанием уровня значимости информации и масштаба ИС.
- ◯ Для ИС, функционирующих на базе ИТКИ, **подтверждено**, что класс защищённости ИС не превышает класс защищённости ИТКИ.
- ◯ При необходимости **выделены отдельные сегменты** ИС с различающимися классами защищённости и определены классы защищённости для каждого сегмента.
- ◯ Результаты классификации **оформлены актом**, содержащим наименование ИС и (при наличии) сегментов, установленный уровень значимости информации, масштаб и присвоенные классы защищённости; акт утверждён оператором (обладателем информации).
- ◯ **Установлен порядок пересмотра классов защищённости** ИС/сегментов при изменении масштаба ИС или значимости информации.

F6

Технологии для борьбы с киберугрозами

info@f6.ru +7 495 984-33-64 f6.ru