Реализация требований о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений

Начальник 2 отдела
Управления ФСТЭК России по Северо-Западному федеральному округу
Нестеренко Олег Дмитриевич
Тел. (812) 312 - 51 - 35

ТРЕБОВАНИЯ О ЗАЩИТЕ ИНФОРМАЦИИ

Федеральным законом от 8 августа 2024 г. № 216-ФЗ внесены изменения статью 14 и часть 5 статьи 16 Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»:

Не допускается передача информации из государственных информационных систем в иные информационные системы, не соответствующие требованиям о защите информации, установленным статьей 16 настоящего Федерального закона

Устанавливается необходимость реализации требований о защите информации в ГИС, а также в иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений

Требования о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений

УТВЕРЖДЕНЫ
приказом ФСТЭК России
от «11» апреля 2025 г. № 117

Требования распространяются на государственные информационные системы, иные информационные системы государственных органов, государственных унитарных предприятий, государственных учреждений

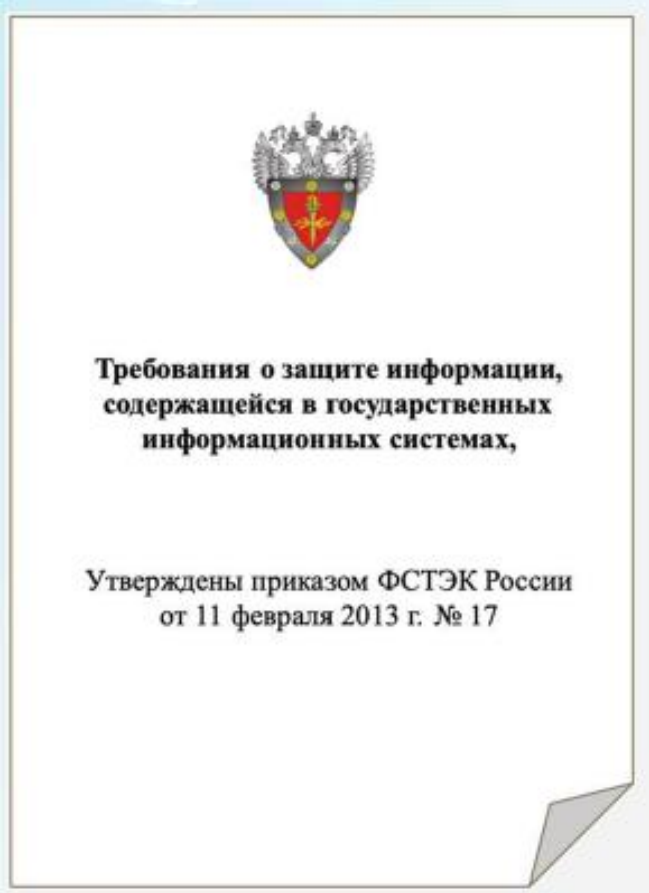
В случае передачи из государственной информационной системы в иные информационные системы информации, доступ к которой ограничен, информационная система, в которую передается информация ограниченного доступа, должна соответствовать Требованиям 149-ФЗ

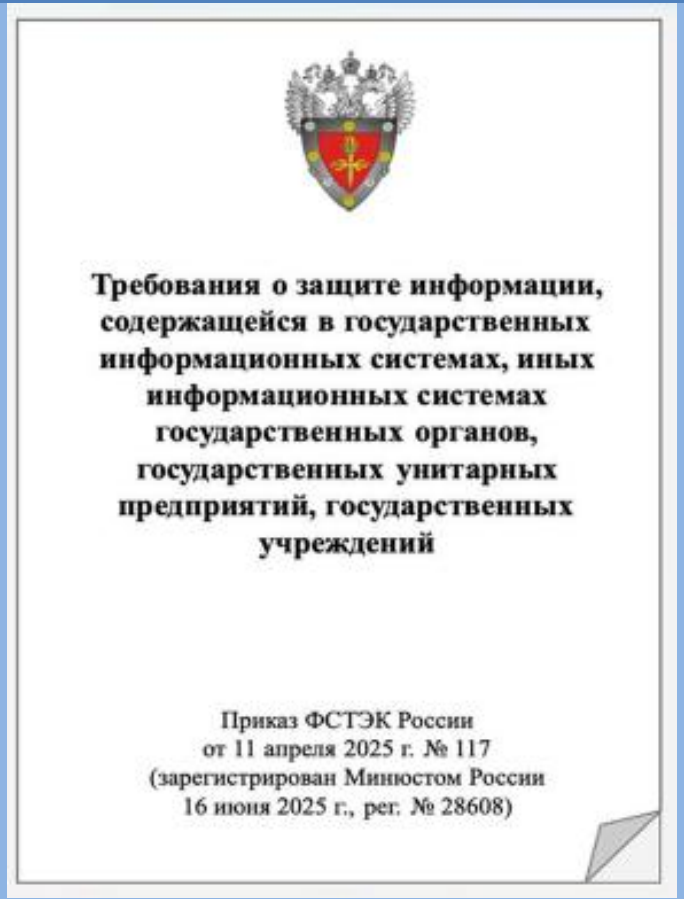
Аттестованные на соответствие Требованиям приказа ФСТЭК России № 17 информационные системы переаттестации не подлежат

Вступили в силу 1 марта 2026 г.

Разработка требований » **Общественное обсуждение** » **Согласование с профильными ведомствами** » **Регистрация в Минюсте России** » **Вступление в силу**

ПЕРЕХОД ТРЕБОВАНИЙ О ЗАЩИТЕ ИНФОРМАЦИИ





- **Спланировать доработку системы защиты информации информационной системы в рамках бюджетных циклов организации**
- **Разработать план перехода на Требования, утвержденные 117 приказом**
- **Провести оценку показателя, характеризующего текущее состояние защиты информации от базового уровня угроз безопасности информации (Кзи)**

ТРЕБОВАНИЯ НА ЭТАПАХ ЖИЗНЕННОГО ЦИКЛА ИНФОРМАЦИОННОЙ СИСТЕМЫ

Государственные информационные системы

Иные информационные системы

Требования к порядку создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации государственных информационных систем и дальнейшего хранения содержащейся в их базах данных информации, утвержденные постановлением Правительства Российской Федерации от 6 июля 2015 г. № 676

ГОСТ Р 51583-2014 «Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения»

ОРГАНИЗАЦИЯ ДЕЯТЕЛЬНОСТИ ПО ЗАЩИТЕ ИНФОРМАЦИИ

Разработка и утверждение политики защиты информации

Определение лиц, ответственных за защиту информации

Применение программных, программно-аппаратных средств, предназначенных для защиты информации

Разработка внутренних стандартов и регламентов по защите информации

Выделение организационных, технических и иных ресурсов, необходимых для защиты информации

РАЗРАБОТКА ПОЛИТИКИ ЗАЩИТЫ ИНФОРМАЦИИ

Область действия политики, включая перечень информации, информационных систем, компонентов информационно-телекоммуникационной инфраструктуры, подлежащих защите

- **определение перечня информационных систем и защищаемой информации**

Определение целей защиты информации

- **исключение утечки информации ограниченного доступа и иной конфиденциальной информации;**
- **предотвращение несанкционированного доступа к информационным системам и содержащейся в них информации и др.**

Категории лиц, участвующих в защите информации, их обязанности (функции) и полномочия (права)

- **руководитель оператора, структурное подразделение, специалисты по защите информации, подрядные организации**

Состав организационной системы управления деятельностью по защите информации и схема взаимодействия ее элементов

Ответственность работников за нарушение требований о защите информации

РАЗРАБОТКА ВНУТРЕННИХ СТАНДАРТОВ И РЕГЛАМЕНТОВ ПО ЗАЩИТЕ ИНФОРМАЦИИ

Внутренние стандарты	
Требования к реализации мер по защите информации	Требования к первичной идентификации лиц, обладающих правами по доступу к информационным системам и (или) содержащейся в них информации и их использованию
	Требования к применяемым моделям доступа пользователей
	Перечень разрешенного и (или) запрещенного для использования программного обеспечения
	Требования к типовым конфигурациям и настройкам программных, программно-аппаратных средств
	Ограничения и запреты действий для пользователей при использовании и обеспечении эксплуатации ими информационных систем

Внутренние регламенты	
Порядок проведения мероприятий или описание реализуемых процессов	Порядок создания, учета, изменения и блокирования, контроля, удаления учетных записей
	Порядок предоставления пользователям удаленного доступа к информационным системам и содержащейся в них информации
	Порядок повышения уровня знаний и информированности пользователей по вопросам защиты информации
	Порядок выявления, оценки и устранения уязвимостей информационных систем
	Порядок разработки безопасного программного обеспечения в случае его самостоятельной разработки оператором (обладателем информации)

СОВЕРШЕНСТВОВАНИЕ МЕТОДИЧЕСКИХ ДОКУМЕНТОВ ПО АТТЕСТАЦИИ

Типовая политика информационной безопасности

Проект

Типовой внутренний стандарт по защите информации

Проект

Типовой внутренний регламент по защите информации

Проект

УПРАВЛЕНИЕ ДЕЯТЕЛЬНОСТЬЮ ПО ЗАЩИТЕ ИНФОРМАЦИИ

Разработка и планирование мероприятий и мер по защите информации

- Определение событий, наступление которых может привести к нарушению целей защиты информации
- Определение информационных систем, ПО И ПАК, несанкционированный доступ к которым и (или) воздействие на которые могут привести к нарушению целей защиты информации
- Выявление и оценка угроз безопасности информации
- Определение состава и сроков проведения мероприятий и принятия мер

Проведение мероприятий и принятие мер по защите информации

- Реализация организационно технических и технических мер по защите информации

Проведение оценки состояния защиты информации

- Показатель текущего состояние защиты информации от базового уровня угроз безопасности информации (показатель защищенности Кзи)
- Показатель, который определяет достаточность и эффективность проведения мероприятий по защите информации (показатель уровня зрелости Пзи)

Совершенствование мероприятий и мер по защите информации

- Планирование мероприятий по защите информации
- Реализация мер по защите информации

ПРОВЕДЕНИЕ ОЦЕНКИ СОСТОЯНИЯ ЗАЩИТЫ ИНФОРМАЦИИ

Показатель, характеризующий текущее состояние защиты информации от базового уровня угроз безопасности информации (показатель защищенности Кзи)

Расчет и оценка показателя защищенности Кзи должны проводиться оператором (обладателем информации) не реже одного раза в шесть месяцев

Методика оценки показателя состояния технической защиты информации и обеспечения безопасности ЗО КИИ РФ, утвержденная ФСТЭК России 11 ноября 2025 г.

Показатель, который определяет достаточность и эффективность проведения мероприятий по защите информации (показатель уровня зрелости Пзи)

Расчет и оценка показателя уровня зрелости Пзи должны проводиться оператором (обладателем информации) не реже одного раза в два года

Методика оценка показателя уровня зрелости (в разработке)

ТРЕБОВАНИЯ К АТТЕСТАЦИИ ИНФОРМАЦИОННЫХ СИСТЕМ И КОНТРОЛЮ УРОВНЯ ЗАЩИЩЕННОСТИ ИНФОРМАЦИИ

Информационная система

До ввода в эксплуатацию

⇩

Аттестация в соответствии с Порядком организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну, утвержденным приказом ФСТЭК России от 29 апреля 2021 г. № 77

В ходе эксплуатации

⇩

Контроль уровня защищенности информации с применением следующих методов:

а) выявление уязвимостей информационных систем с последующей экспертной оценкой;

б) выявление несанкционированных подключений устройств к информационным системам;

в) тестирование информационных систем путем моделирования реализации актуальных угроз;

г) проведение тренировок в соответствии с едиными замыслом и планом

СОВЕРШЕНСТВОВАНИЕ МЕТОДИЧЕСКИХ ДОКУМЕНТОВ ПО АТТЕСТАЦИИ

Для служебного пользования

Методика
испытаний систем защиты информации информационных систем путем тестирования на проникновение

25 июня 2025 г.

Методика
анализа уязвимостей в информационных системах

25 ноября 2025 г.

Методика
испытаний систем защиты информации информационных систем путем осуществления тестирования ее функций безопасности (функционального тестирования)

Проект

<u>Пункт 20 Требований:</u> Не менее 30 % работников структурного подразделения по защите информации должны иметь профессиональное образование по специальности или направлению подготовки в области информационной безопасности или пройти обучение по программе профессиональной переподготовки в области информационной безопасности.

ФСТЭК России

ФЕДЕРАЛЬНАЯ СЛУЖБА ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ

Меню | Главная | Карта сайта | Поиск | Документы | Метки | Ссылки | Обновления | Противодействие коррупции | Версия для слабовидящих | EN

Главная / Документы / Все документы / Перечни / Перечень организаций, осуществляющих образовательную деятельность

Перечень организаций, осуществляющих образовательную деятельность

16 Создано: 14.12.2022 13:57 Обновлено: 19.03.2026 15:47 Просмотры: 128515

Техническая защита информации | Обучение специалистов

PDF Перечень организаций, осуществляющих образовательную деятельность
Размер: 2.13 МБ Скачивания: 13832

ODT Перечень организаций, осуществляющих образовательную деятельность
Размер: 76.02 КБ Скачивания: 7669

Перечень организаций, осуществляющих образовательную деятельность, имеющих дополнительные профессиональные программы в области информационной безопасности, согласованные с Федеральной службой по техническому и экспортному контролю

п/п	Наименование организации, осуществляющей образовательную деятельность	Наименование дополнительной профессиональной программы	Срок освоения, час.	Форма обучения
	Центральный федеральный округ			
1.	Федеральное государственное автономное образовательное учреждение высшего образования "Национальный исследовательский ядерный университет "МИФИ", г. Москва	Программа повышения квалификации "Техническая защита информации. Сертификация средств защиты информации по требованиям безопасности информации"	216	Очная
		Программа повышения квалификации "Техническая защита информации. Способы и средства защиты информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну, от утечки по техническим каналам"	216	Очная
		Программа повышения квалификации "Техническая защита информации. Организация защиты информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну"	216	Очная
		Программа повышения квалификации "Техническая защита информации. Способы и средства защиты информации от несанкционированного доступа"	216	Очная
		Программа повышения квалификации "Обеспечение безопасности персональных данных при их обработке в информационных системах персональных данных"	72	Очная
		Программа профессиональной переподготовки "Криптографические методы и средства защиты информации в информационно-телекоммуникационных системах"	572	Очная
		Программа профессиональной переподготовки "Информационная безопасность. Техническая защита конфиденциальной информации"	504	Очная, очно-заочная

Реализация требований о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений

Начальник 2 отдела
Управления ФСТЭК России по Северо-Западному федеральному округу
Нестеренко Олег Дмитриевич
Тел. (812) 312 - 51 - 35