Особенности реализации Требований о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений

Заместитель начальника 2 управления ФСТЭК России

Гефнер Ирина Сергеевна

РЕАЛИЗАЦИЯ МЕР И МЕРОПРИЯТИЙ ПО ЗАЩИТЕ ИНФОРМАЦИИ

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

Приказ ФСТЭК России
от 11 апреля 2025 г. № 117
(зарегистрирован Минюстом России
16 июня 2025 г., рег. № 28608)

МЕТОДИЧЕСКИЙ ДОКУМЕНТ

МЕРОПРИЯТИЯ И МЕРЫ ПО ЗАЩИТЕ ИНФОРМАЦИИ, СОДЕРЖАЩЕЙСЯ В ИНФОРМАЦИОННЫХ СИСТЕМАХ

ПРОЕКТ

2026

Размещен на сайте ФСТЭК России

Для достижения целей защиты информации должно проводиться **21 мероприятие по защите информации**, а также в информационных системах должно быть реализовано **17 групп мер защиты информации**

ОРГАНИЗАЦИИ, ПРИНИМАЮЩИЕ УЧАСТИЕ В АПРОБАЦИИ МЕТОДИЧЕСКОГО ДОКУМЕНТА

Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации
Федеральное Казначейство
Департамент информационных технологий города Москвы
ФАУ «ГНИИИ ПТЗИ ФСТЭК России»
ФКУ «Государственные Технологии»
Институт Системного программирования им. В.П. Иванникова Российской Академии Наук
ООО «Центр Безопасности Информации»
ООО «Безопасная Информационная Зона»
ПАО «Ростелеком»
АО «Лаборатория Касперского»
АО «Позитивные Технологии»
ООО НТЦ «Фобос-НТ»
ООО «Юзергейт»
ООО «Айдеко»
ООО «Научно-Испытательный Институт Систем обеспечения комплексной безопасности»
АО «Аладдин Р.Д.»
АО «Инфовотч»
ООО «Открытая Мобильная Платформа»
ПАО «Сбербанк»
ООО «Яндекс»
ООО «Конфидент»
АО «Национальный Инновационный Центр»
АО «ИНФОТЕКС»

23 организации
принимают участие в апробации
методического документа

СТРУКТУРА МЕТОДИЧЕСКОГО ДОКУМЕНТА

1. ОБЩИЕ ПОЛОЖЕНИЯ	Область применения (ГИС, иные системы госорганов и организаций, объекты КИИ, ИСПДн) Предназначен для операторов и подрядчиков Применяется при создании систем, а также при оценке эффективности реализации мер
2. ФАКТОРЫ, ВЛИЯЮЩИЕ НА СОСТОЯНИЕ ЗАЩИТЫ ИНФОРМАЦИИ, СОДЕРЖАЩЕЙСЯ В ИНФОРМАЦИОННЫХ СИСТЕМАХ	Реализация мероприятий (процессов) по защите информации в органе (организации) Оценка достаточности и эффективности проведения мероприятий по защите информации
3.МЕРОПРИЯТИЯ (ПРОЦЕССЫ) ПО ЗАЩИТЕ ИНФОРМАЦИИ	Представлено описание 19 мероприятий по защите информации
4. МЕРЫ ПО ЗАЩИТЕ ИНФОРМАЦИОННЫХ СИСТЕМ И СОДЕРЖАЩЕЙСЯ В НИХ ИНФОРМАЦИИ	Представлено описание 18 мер по защите информации
Приложение 1.Термины и определения **Приложение 2. Содержание базовых мер защиты информации**	

СТРУКТУРА ОПИСАНИЯ МЕРОПРИЯТИЙ ПО ЗАЩИТЕ ИНФОРМАЦИИ

На примере описания мероприятия по **контролю конфигураций информационных систем**

Цель реализации	Требования к реализации	Требования к документированию	Требования к усилению*
Исключение несанкционированного изменения состава программных, программно-аппаратных средств информационных систем	Контроль конфигураций информационных систем должен предусматривать: определение объектов инвентаризации, сбор, учет и хранение данных об объектах инвентаризации; контроль состава объектов определение конфигураций объектов	Внутренние стандарты с типовыми конфигурациями и настройками программных, программно-аппаратных средств должны содержать: перечень информационных систем и (или) отдельных типов (классов) программных, программно-аппаратных средств; описание настройки и конфигурации	Контроль конфигураций информационных систем осуществляется на основе данных автоматизированных систем сбора и хранения данных об объектах инвентаризации и их конфигурациях (CMDB-системы).

*Усиления мероприятий (процессов) применяются по решению оператора (для повышения эффективности реализации мероприятий по защите информации и повышения уровня защищенности информационных систем и содержащейся в них информации

СТРУКТУРА ОПИСАНИЯ МЕР ЗАЩИТЫ ИНФОРМАЦИИ

На примере описания меры по **идентификации пользователей**

Цель реализации

Исключение доступа к информационной системе лиц, не являющихся пользователями информационной системы

Требования к реализации

В информационной системе должна осуществляться идентификация внешних и внутренних пользователей

Требования к первичной и вторичной идентификации

Требования к управлению идентификаторами

Требования к документированию

В эксплуатационной документации на информационную систему должны быть определены:

перечень типов пользователей;

состав идентификационных данных;

порядок идентификации

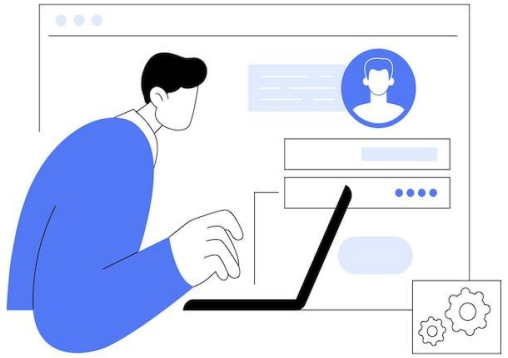
Требования к усилению*

В информационной системе должно быть реализовано централизованное управление идентификаторами

*Усиления мер по защите информации являются обязательными в зависимости от класса защищенности информационной системы

ОСОБЕННОСТИ РЕАЛИЗАЦИИ ИДЕНТИФИКАЦИИ И АУТЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЕЙ

Внутренние пользователи



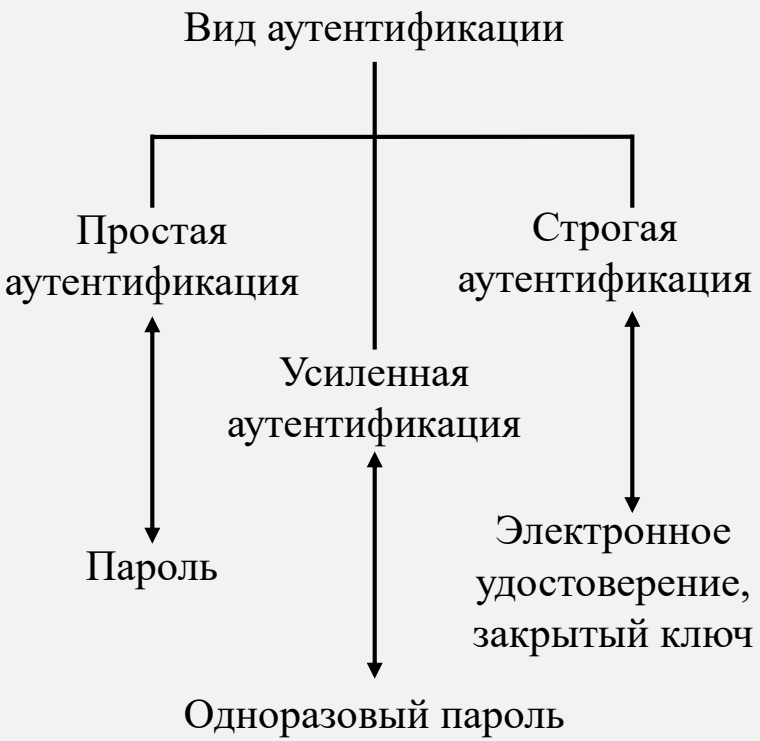
1) **работники оператора (обладателя информации), заказчика информационной системы, а также подведомственных ему государственных органов и организаций** при их наличии, выполняющие свои обязанности (функции) с использованием информации, информационных технологий и средств вычислительной техники информационной системы и которым в информационной системе присвоены учетные записи

2) **работники подрядных организаций**, привлекаемые на договорной основе для оказания услуг, проведения работ по обработке, хранению информации, созданию (развитию), обеспечению эксплуатации информационных систем, а также для выполнения работ, оказания услуг по защите информации

Внешние пользователи

пользователи, получающие доступ к информационной системе со средств вычислительной техники**, не входящих в состав информационной системы или** для которых оператором информационной системы **не могут устанавливаться и контролироваться требования о защите информации**

ТРЕБОВАНИЯ К АУТЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЕЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ



ГОСТ Р 58833—2020

Тип пользователя	Тип доступа	Права доступа	Вид аутентификации		
			К3	К2	К1
Внутренний пользователь	Локальный	Непривилегированный	П	У	У
	Удалённый	Непривилегированный	У	У	С
Внутренний пользователь	Локальный	Привилегированный	У	У	С
	Удалённый	Привилегированный	С	С	С
Внутренний пользователь с мобильного устройства	Удаленный	Непривилегированный	У	С	С
Внешний пользователь	Удалённый	Непривилегированный	П	У	У

Принятые обозначения:

П – простая (парольная) аутентификация;

У – усиленная (двухфакторная) аутентификация;

С – строгая аутентификация (двухфакторная, с использованием закрытого ключа, криптографических методов и протоколов, сертификатов безопасности).

МЕРОПРИЯТИЯ И МЕРЫ ПО ЗАЩИТЕ КОНЕЧНЫХ И МОБИЛЬНЫХ УСТРОЙСТВ

Конечные устройства

физические и виртуальные устройства информационных систем, имеющие постоянный доступ к сети «Интернет»

- Реализация мер по защите конечных устройств (ЗКУ)
- Мониторинг и анализа процессов и событий
- Предупреждение пользователя

Мобильные устройства

смартфоны и планшетные компьютеры под управлением мобильных операционных систем, обеспечивающих представление мобильных сервисов и беспроводных технологий связи (Wi-Fi, Bluetooth, сотовой связи)

- Реализация мер по защите мобильных устройств (ЗМУ)
- Управление и контроль использования мобильных устройств
- Контроль приложений

ЗАЩИТА ИНФОРМАЦИИ ПРИ ВЗАИМОДЕЙСТВИИ С ПОДРЯДНЫМИ ОРГАНИЗАЦИЯМИ

Оператор (заказчик)

В договорах или иных документах устанавливает:

- обязанность подрядчика по обеспечению защиты информации, к которой получен доступ
- требования к реализации мер, в том числе к аттестации (при необходимости)
- ответственность за нарушения требований оператора

- ❑ Создание для подрядчиков отдельных учетных записей
- ❑ Мониторинг и регистрация действий учетных записей
- ❑ Защита каналов передачи данных

Подрядные организации

оказание услуг, проведение работ по:

- обработке, хранению информации,
- созданию (развитию) систем,
- обеспечению эксплуатации систем,
- выполнению работ, оказания услуг по защите информации

Реализация мероприятий и мер защиты информации, установленных методическим документом и оператором (заказчиком)

ОБЕСПЕЧЕНИЕ ЗАЩИТЫ ИНФОРМАЦИИ ПРИ ИСПОЛЬЗОВАНИИ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

- **программное обеспечение, обеспечивающее реализацию системы искусственного интеллекта**
- **выходная модель машинного обучения и ее параметры (веса)**

Оценка угроз безопасности информации системы искусственного интеллекта

Реализация мер защиты информации (ЗИИ.1)

Реализация процессов разработки безопасного программного обеспечения в соответствии с ГОСТ Р 56939-2024

В отношении программного обеспечения, обеспечивающего реализацию системы искусственного интеллекта, должны быть проведены анализ уязвимостей и проверки на отсутствие недекларированных возможностей

ОБЕСПЕЧЕНИЕ ЗАЩИТЫ ИНФОРМАЦИИ ПРИ ИСПОЛЬЗОВАНИИ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

Инфраструктура оператора

ПО, обеспечивающее реализацию системы искусственного интеллекта

Выходная модель машинного обучения, LoRA, RAG

API-интерфейсы, агенты, системы цензуры

Входит в состав системы оператора

Предоставляется как сервис

Реализация мер по защите информации (ЗИИ.2)

Реализация мер по защите информации (ЗИИ.2)

В инфраструктуре подрядчика должны реализованы меры по классу защищенности не ниже класса защищенности системы оператора

СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ, ПРИМЕНЯЕМЫЕ ДЛЯ РЕАЛИЗАЦИИ МЕР

Общий перечень СЗИ, необходимых для реализации приказов ФСТЭК России № 17 и № 117

- Операционные системы
- Межсетевые экраны
- Средства контроля защищенности
- Средства защиты среды виртуализации
- Средства резервного копирования и восстановления
- Средства защиты мобильных устройств (MDM)
- Средства обнаружения вторжений (IDS/IPS)
- Средства доверенной загрузки
- Средства регистрации событий безопасности
- Средства защиты контейнеризации
- Средства антивирусной защиты
- Средства защиты от DDoS-атак

Требованиями приказа ФСТЭК России № 117 **дополнительно** определена необходимость применения указанных средств в зависимости от класса защищенности системы

- Средства управления идентификацией и аутентификацией (IDM/IAM, PAM и др.)
- Средства обнаружения и реагирования на уровне узла (EDR)
- Средства мониторинга информационной безопасности (SIEM)

Особенности реализации Требований о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений

Заместитель начальника 2 управления ФСТЭК России

Гефнер Ирина Сергеевна