Требования 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

СОВЕРШЕНСТВОВАНИЕ ТРЕБОВАНИЙ О ЗАЩИТЕ ИНФОРМАЦИИ

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

Проект

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 настоящим Требованиям

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

Вступают в силу с 1 марта 2026 г.

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

ПОРЯДОК ПРИМЕНЕНИЯ ТРЕБОВАНИЙ В ИНФОРМАЦИОННЫХ СИСТЕМАХ

ТРЕБОВАНИЯ О ЗАЩИТЕ ИНФОРМАЦИИ НА ЭТАПАХ ЖИЗНЕННОГО ЦИКЛА ИНФОРМАЦИОННОЙ 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 РФ от 6 июля 2015 г. № 676

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

Разработка модели угроз и технического задания

Выделение ресурсов для защиты информации

Разработка и утверждение политики защиты информации

Формирование требований к системе

Разработка (проектирование) системы

Внедрение системы

Аттестация ИС

Эксплуатация ИС

Применение программных и аппаратных СЗИ

Определение лиц, ответственных за защиту информации

Разработка внутренних стандартов и регламентов по ЗИ

Разработка и планирование мероприятий и мер по защите информации

Проведение мероприятий и принятие мер по защите информации

Проведение оценки состояния защиты информации

Совершенствование мероприятий и мер по защите информации

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 схему взаимодействия ее элементов

Ответственность работников за нарушение требований о защите информации

ОРГАНИЗАЦИЯ И УПРАВЛЕНИЕ ДЕЯТЕЛЬНОСТЬЮ ПО 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)

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

ТРЕБОВАНИЯ К ПРОВЕДЕНИЮ МЕРОПРИЯТИЙ И ПРИНЯТИЮ МЕР ПО ЗАЩИТЕ ИНФОРМАЦИИ

- выявление и оценка угроз безопасности информации
- контроль конфигураций информационных систем
- управление уязвимостями
- управление обновлениями
- обеспечение защиты информации при использовании конечных устройств
- обеспечение защиты информации при обработке, хранении и обращении с информацией ограниченного доступа
- обеспечение защиты информации при использовании мобильных устройств
- обеспечение защиты информации при удаленном доступе пользователей к информационным системам
- обеспечение защиты информации при беспроводном доступе пользователей к информационным системам
- обеспечение мониторинга информационной безопасности
- обеспечение разработки безопасного программного обеспечения
- обеспечение непрерывности функционирования информационных систем при возникновении нештатных ситуаций
- обеспечение доверия при взаимодействии в информационных системах субъектов и объектов доступа
- повышение уровня знаний и информированности пользователей по вопросам защиты информации
- обеспечение защиты информации при взаимодействии с подрядными организациями
- обеспечение защиты информации при использовании искусственного интеллекта

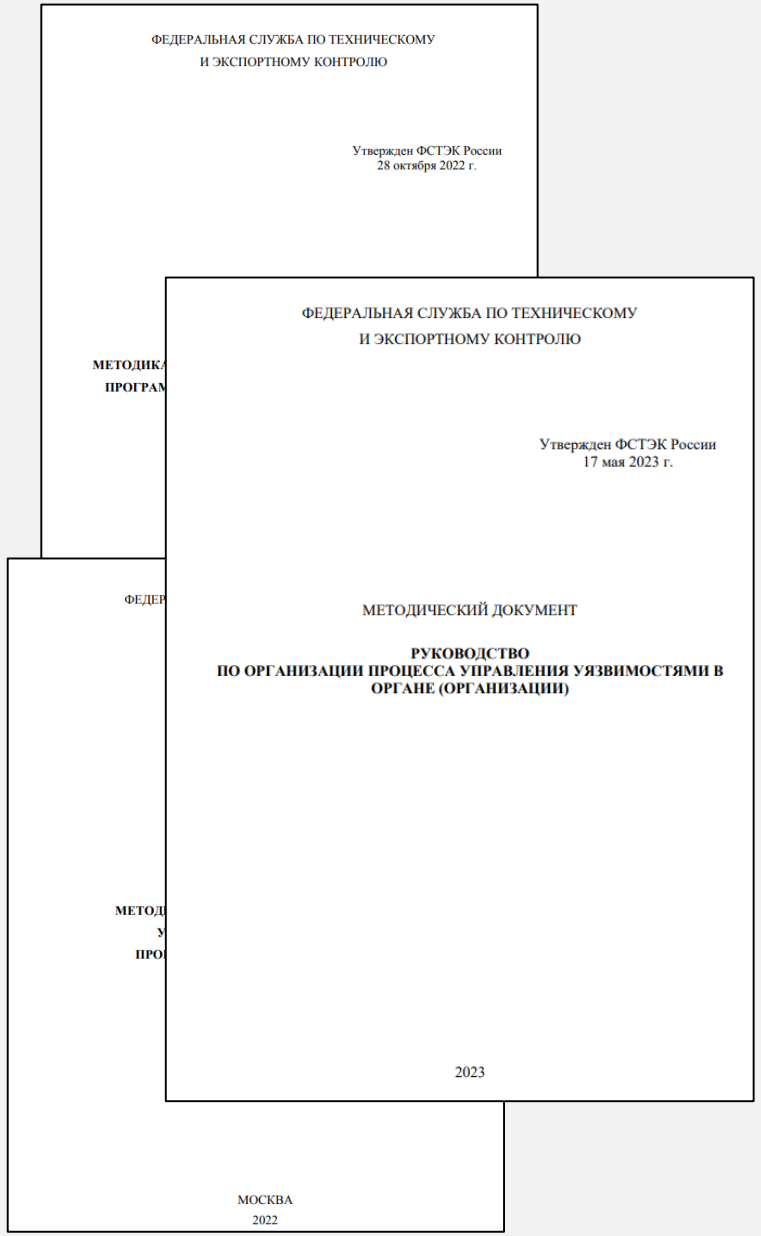
ВЫЯВЛЕНИЕ И ОЦЕНКА УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

Модель угроз безопасности информации информационной системы

На этапе формирования требований и проектирования системы	На этапе развития (модернизации) системы	В ходе эксплуатации системы
исходные данные для: **разработки и внедрения мер** по защите информации; **выбора средств защиты информации** и их функциональных возможностей в ходе создания (развития) подсистем защиты информации информационных систем		Предназначена для: **поиска данных и признаков**, идентифицирующих наличие актуальных угроз; **приоритизации выявленных угроз;** **принятия мер** по блокированию актуальных угроз; **оповещения** подразделений (работников) об актуальных угрозах.

Решение о необходимости разработки модели угроз безопасности информации в ходе создания **негосударственных** информационных систем принимается руководителем оператора (обладателя информации)

МЕРОПРИЯТИЯ ПО УПРАВЛЕНИЮ УЯЗВИМОСТЯМИ



Оценка критичности уязвимостей

Определение методов и приоритетов устранения уязвимостей

Контроль за устранением уязвимостей

Устранение уязвимостей

Критические	Высокие	Средние и низкие
не более 24 часов	не более 7 календарных дней	сроки определяют в регламенте

При выявлении неизвестных уязвимостей оператор в срок **не более 5 рабочих дней** передает информацию в Банк данных угроз безопасности информации ФСТЭК России

ОСОБЕННОСТИ РЕАЛИЗАЦИИ ОТДЕЛЬНЫХ МЕРОПРИЯТИЙ ПО ЗАЩИТЕ ИНФОРМАЦИИ

Управление обновлениями	Проведение проверки подлинности и целостности обновлений программных, программно-аппаратных средств, тестирование обновлений до их применения в контурах промышленной эксплуатации
Защита информации при применении мобильных устройств	Личные мобильные устройства допускаются при их соответствии Требованиям и наличия у оператора возможности контроля использования мобильных устройств
Мероприятия по обеспечению ЗИ при удаленном доступе	Применение личных устройств допускается при условии применения сертифицированных средств обеспечения безопасной дистанционной работы, средств антивирусной защиты и др.
Мероприятия по обеспечению ЗИ при беспроводном доступе	Конфигурация и настройки, уровни сигналов точек беспроводного доступа должны исключать возможность подключения к ним посторонних лиц. Указанные точки беспроводного доступа должны быть однозначно идентифицированы в информационных системах, а также определены места их размещения
Мероприятия по обеспечению ЗИ при предоставлении привилегированного доступа	Привилегированные учетные записи должны быть закреплены за соответствующими ролями пользователей. Удаленный привилегированный доступ с применением строгой аутентификации, а в случае технической невозможности ее применения — с использованием усиленной многофакторной аутентификации

МЕРОПРИЯТИЯ ПО РАЗРАБОТКЕ БЕЗОПАСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Самостоятельная разработка оператором (обладателем информации) программного обеспечения

Национальный стандарт
ГОСТ Р 56939-2024

Защита информации

РАЗРАБОТКА БЕЗОПАСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Общие требования

СЭД

Кадровые системы

ПО автоматизации деятельности

Выявление и устранение уязвимостей в разрабатываемом оператором (обладателем информации) программном обеспечении

Реализация мер, предусмотренные разделами 4 и 5 ГОСТ Р 56939-2024

В ТЗ на разработку программного обеспечения могут быть включены требования по разработке безопасного программного обеспечения в соответствии с ГОСТ Р 56939-2024

Подтверждением выполнения подрядной организацией мер по разработке безопасного программного обеспечения является наличие у нее сертификата соответствия, выданного ФСТЭК России в соответствии с приказом ФСТЭК России от 1 декабря 2023 г. № 240.

МЕРОПРИЯТИЯ ПО ЗАЩИТЕ ИНФОРМАЦИИ ПРИ ВЗАИМОДЕЙСТВИИ ОПЕРАТОРА (ОБЛАДАТЕЛЯ ИНФОРМАЦИИ) С ПОДРЯДНЫМИ ОРГАНИЗАЦИЯМИ

Подрядная организация - организация, которой на основании договора или иного документа передается информация, предоставляется доступ к информационным системам оператора (обладателя информации) и (или) содержащейся в них информации 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.

В договорах должны быть установлены обязанности подрядных организаций по обеспечению защиты информации, к которой получен доступ, а также ответственность за невыполнение этой обязанности.

Не допускается копирование подрядными организациями информации, к которой им предоставлен доступ, если такое копирование не предусмотрено в договорах или иных документах

В информационных системах, отдельных программно-аппаратных средствах подрядных организаций, в которых осуществляются обработка и хранение полученной в результате предоставленного доступа информации, должны быть приняты меры по защите информации

Разработка (развитие) и (или) тестирование программного обеспечения подрядными организациями непосредственно в контуре промышленной эксплуатации информационных систем оператора (обладателя информации) не допускается

МЕРОПРИЯТИЯ ПО ОБЕСПЕЧЕНИЮ ЗАЩИТЫ ИНФОРМАЦИИ ПРИ ИСПОЛЬЗОВАНИИ ДЛЯ ФУНКЦИОНИРОВАНИЯ ИНФОРМАЦИОННЫХ СИСТЕМ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

Атаки на модели машинного обучени	Угроза отравления обучающей выборки	Угроза утечки данных из модел	Угроза отравления обучающей выборки

При взаимодействии в формате строго заданных шаблонов запросов и ответов:

- определены шаблоны запросов пользователей, направляемых в искусственный интеллект, и обеспечен контроль соответствия запросов установленным шаблонам;
- определены шаблоны ответов искусственного интеллекта и обеспечен контроль соответствия ответов установленным шаблонам.

При взаимодействии в формате свободной текстовой формы запросов и ответов:

- определены для направляемых в искусственный интеллект запросов пользователей допустимые тематики и обеспечен контроль соответствия запросов допустимым тематикам;
- определены форматы ответов искусственного интеллекта в соответствии с допустимыми тематиками и обеспечен контроль соответствия ответов установленным форматам и допустимым тематикам

Разработаны статистические критерии для выявления недостоверных ответов искусственного интеллекта для последующего сбора и анализа недостоверных ответов

Обеспечено реагирование на недостоверные ответы искусственного интеллекта

МЕРОПРИЯТИЯ ПО ОБЕСПЕЧЕНИЮ ДОВЕРИЯ ПРИ ВЗАИМОДЕЙСТВИИ СУБЪЕКТОВ И ОБЪЕКТОВ ДОСТУПА В РАСПРЕДЕЛЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ

МЕРОПРИЯТИЯ ПО РЕАЛИЗАЦИИ В ИНФОРМАЦИОННЫХ СИСТЕМАХ МЕР ПО ИХ ЗАЩИТЕ И СОДЕРЖАЩЕЙСЯ В НИХ ИНФОРМАЦИИ

- идентификация и аутентификация
- управление доступом
- регистрация событий безопасности
- защита виртуализации и облачных вычислений
- защита технологий контейнерных сред и их оркестрации
- защита веб-технологий
- защита программных интерфейсов взаимодействия приложений
- защита конечных устройств

17 мер защиты информационных систем и содержащейся в них инфомации

Реализация базового набора мер

Адаптация базового набора мер

Верификация адаптированного базового набора мер

1 класс	• от нарушителей с высоким уровнем возможностей
2 класс	• от нарушителей с повышенным уровнем возможностей
3 класс	• от нарушителей с базовым уровнем возможностей

Класс защищенности (К) = [уровень значимости информации; масштаб системы].

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 в соответствии с едиными замыслом и планом тренировок.

Требования 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