Основные направления совершенствования технической защиты информации

Заместитель директора
Федеральной службы по техническому
и экспортному контролю

ЛЮТИКОВ Виталий Сергеевич

Защита информационной инфраструктуры государственных органов (организаций)

Защита информационной инфраструктуры государственных органов (организаций)

Проект Федерального закона «О внесении изменений в статью 16 Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»

Внести в часть 5 статьи 16 изменение, изложив ее в следующей редакции:

"5. Требования о защите информации, обладателями которой являются Российская Федерация, субъект Российской Федерации, муниципальное образование, устанавливаются федеральным органом исполнительной власти в области обеспечения безопасности и федеральным органом исполнительной власти, уполномоченным в области противодействия иностранным техническим разведкам и технической защиты информации, в пределах их полномочий.

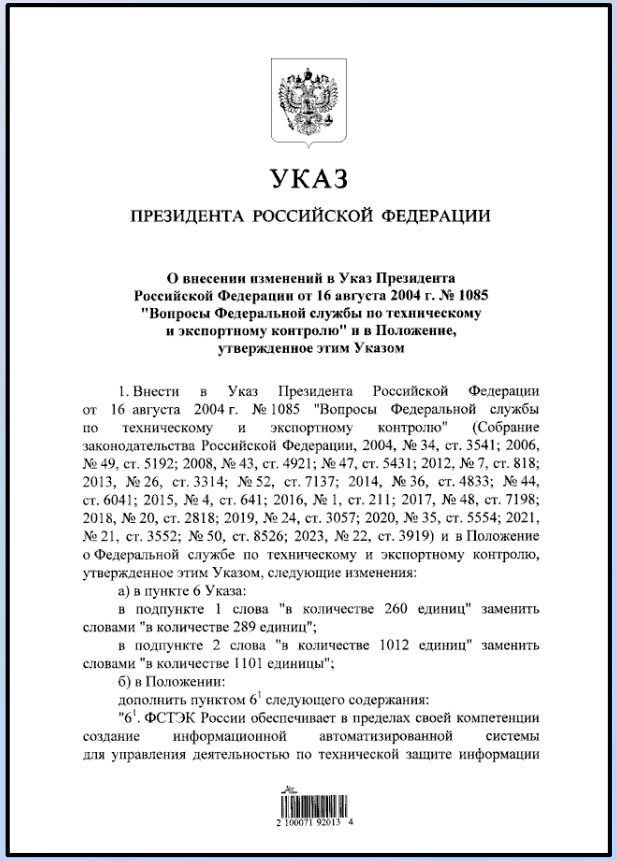
Требования о защите информации, содержащейся в государственных и иных информационных системах, обладателями которой являются Российская Федерация, субъект Российской Федерации, муниципальное образование

Проект

ФСТЭК России поручено до 1 июня 2024 г. разработать требования о защите информации, содержащейся в государственных и иных информационных системах, обладателями которой являются Российская Федерация, субъект Российской Федерации, муниципальное образование.

Оценка состояния защиты информации и обеспечения безопасности объектов КИИ и эффективности деятельности органов государственной власти и организаций

Указ Президента Российской Федерации от 8 ноября 2023 г. № 846 «О внесении изменений в Указ Президента Российской Федерации от 16 августа 2004 г. № 1085 «Вопросы Федеральной службы по техническому и экспортному контролю»



УКАЗ

ПРЕЗИДЕНТА РОССИЙСКОЙ ФЕДЕРАЦИИ

О внесении изменений в Указ Президента Российской Федерации от 16 августа 2004 г. № 1085 "Вопросы Федеральной службы по техническому и экспортному контролю" и в Положение, утвержденное этим Указом

1. Внести в Указ Президента Российской Федерации от 16 августа 2004 г. № 1085 "Вопросы Федеральной службы по техническому и экспортному контролю" (Собрание законодательства Российской Федерации, 2004, № 34, ст. 3541; 2006, № 49, ст. 5192; 2008, № 43, ст. 4921; № 47, ст. 5431; 2012, № 7, ст. 818; 2013, № 26, ст. 3314; № 52, ст. 7137; 2014, № 36, ст. 4833; № 44, ст. 6041; 2015, № 4, ст. 641; 2016, № 1, ст. 211; 2017, № 48, ст. 7198; 2018, № 20, ст. 2818; 2019, № 24, ст. 3057; 2020, № 35, ст. 5554; 2021, № 21, ст. 3552; № 50, ст. 8526; 2023, № 22, ст. 3919) и в Положение о Федеральной службе по техническому и экспортному контролю, утвержденное этим Указом, следующие изменения:

а) в пункте 6 Указа:

в подпункте 1 слова "в количестве 260 единиц" заменить словами "в количестве 289 единиц";

в подпункте 2 слова "в количестве 1012 единиц" заменить словами "в количестве 1101 единицы";

б) в Положении:

дополнить пунктом 6^1 следующего содержания:

"6^1. ФСТЭК России обеспечивает в пределах своей компетенции создание информационной автоматизированной системы для управления деятельностью по технической защите информации

Новые полномочия ФСТЭК России

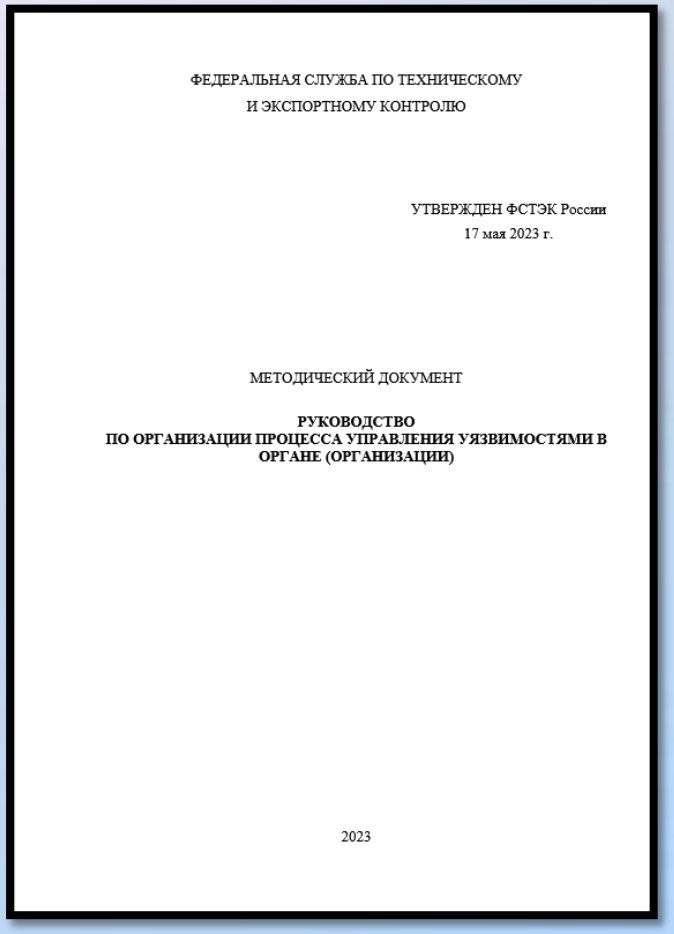
Мониторинг текущего состояния технической защиты информации и обеспечения безопасности значимых объектов критической информационной инфраструктуры

Показатель состояния защиты информации и обеспечения безопасности объектов КИИ в органе государственной власти и (или) организации

Организация и проведение оценки эффективности деятельности ОГВ и организаций по технической защите информации и обеспечению безопасности значимых объектов КИИ

Показатель зрелости деятельности органов государственной власти и организаций по защите информации и обеспечению безопасности объектов КИИ

Выявление угроз безопасности информации и принятие мер по их нейтрализации



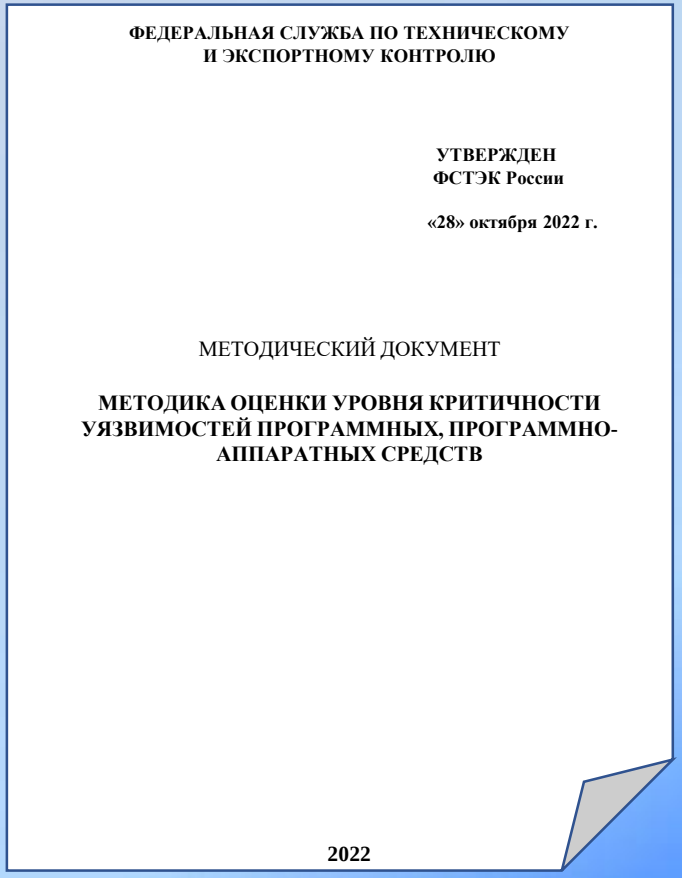
ФЕДЕРАЛЬНАЯ СЛУЖБА ПО ТЕХНИЧЕСКОМУ
И ЭКСПОРТНОМУ КОНТРОЛЮ

УТВЕРЖДЕН ФСТЭК России
17 мая 2023 г.

МЕТОДИЧЕСКИЙ ДОКУМЕНТ

**РУКОВОДСТВО
ПО ОРГАНИЗАЦИИ ПРОЦЕССА УПРАВЛЕНИЯ УЯЗВИМОСТЯМИ В ОРГАНЕ (ОРГАНИЗАЦИИ)**

2023



**ФЕДЕРАЛЬНАЯ СЛУЖБА ПО ТЕХНИЧЕСКОМУ
И ЭКСПОРТНОМУ КОНТРОЛЮ**

**УТВЕРЖДЕН
ФСТЭК России**

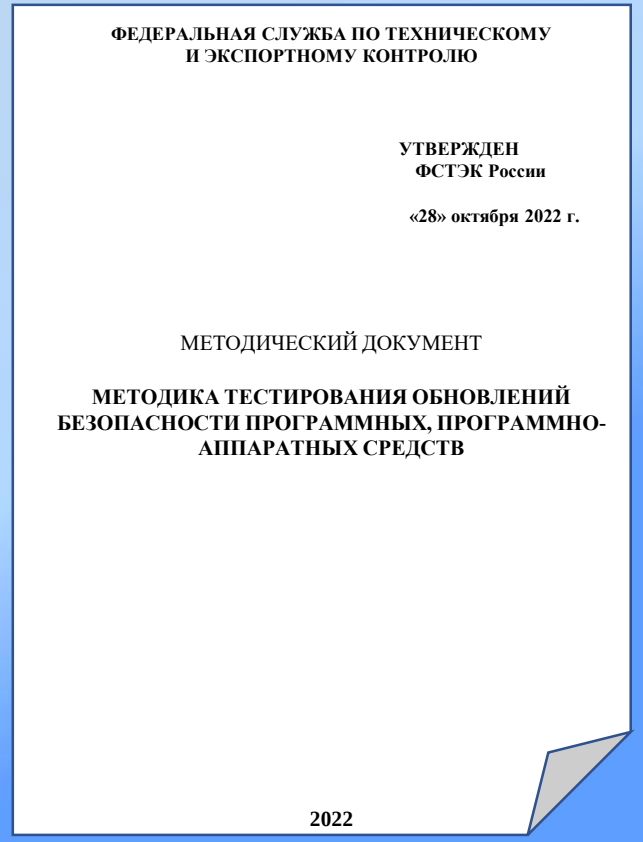
«28» октября 2022 г.

МЕТОДИЧЕСКИЙ ДОКУМЕНТ

МЕТОДИКА ОЦЕНКИ УРОВНЯ КРИТИЧНОСТИ УЯЗВИМОСТЕЙ ПРОГРАММНЫХ, ПРОГРАММНО-АППАРАТНЫХ СРЕДСТВ

2022

Инвентаризация и классификация объектов защиты



**ФЕДЕРАЛЬНАЯ СЛУЖБА ПО ТЕХНИЧЕСКОМУ
И ЭКСПОРТНОМУ КОНТРОЛЮ**

**УТВЕРЖДЕН
ФСТЭК России**

«28» октября 2022 г.

МЕТОДИЧЕСКИЙ ДОКУМЕНТ

МЕТОДИКА ТЕСТИРОВАНИЯ ОБНОВЛЕНИЙ БЕЗОПАСНОСТИ ПРОГРАММНЫХ, ПРОГРАММНО-АППАРАТНЫХ СРЕДСТВ

2022

Раздел Банка данных угроз безопасности информации с результатами тестирования обновлений

https://bdu.fstec.ru/software-section/updates

Протестировано 1015 обновлений

Повышение защищенности от DDoS-атак

Уровни защиты

- РОСКОМНАДЗОР — Национальная система противодействия DDoS-атакам
-  Провайдеры
-  Операторы информационных систем

Меры защиты

- Проведение инвентаризации служб и веб-сервисов, используемых для функционирования официальных сайтов органов государственной власти
- Обеспечение сетевого взаимодействия с применением защищенных актуальных версий протоколов сетевого взаимодействия (HTTPS, SSH и других протоколов)
- Обеспечение фильтрации трафика прикладного уровня с применением средств межсетевого экранирования уровня приложений (WAF)
- Использование хостинга доменных зон у соответствующих провайдеров для защиты службы доменных имён (DNS-служба) или услуги по защите DDoS-атак от специализированного провайдера
- Ограничение количества подключений с каждого IP-адреса (установка на веб-сервере параметра rate-limit)

ФСТЭК России поручено до 1 июня 2024 г. разработать и утвердить требования по обеспечению защищенности государственных информационных систем и значимых объектов критической информационной инфраструктуры Российской Федерации от несанкционированных воздействий типа «отказ в обслуживании».

Повышение качества аттестации объектов информатизации по требованиям безопасности информации

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

Разрабатываемые методические документы

- **Типовая программа и методики аттестационных испытаний**
- **Методика анализа уязвимостей**
- **Методика тестирования функций безопасности**
- **Методика испытания системы защиты информации с использованием средств тестирования**

ТИПОВЫЕ НЕДОСТАТКИ

- применение несертифицированных средств защиты информации;
- отсутствие результатов анализа уязвимостей информационной системы;
- отсутствие сведений об испытаниях системы защиты информации путем осуществления попыток несанкционированного доступа (воздействия) к информационной системе;
- отсутствие мер защиты информации на автоматизированных рабочих местах пользователей и администраторов;
- отсутствие эксплуатационной и организационно-распорядительной документации на систему защиты информации.

По состоянию на февраль 2024 года в реестр ФСТЭК России занесены данные по **12 383 объектам информатизации**:
ГИС – 3 337, ИСУП – 235, ЗП – 753, КИИ – 145, ИСПДн – 7 898, АСУ ТП – 15

Развитие системы сертификации средств защиты информации ФСТЭК России

Совершенствование требований по безопасности информации к СЗИ

Требования по безопасности информации к NGFW

приказ ФСТЭК России от 7.04.22 № 44

Требования по безопасности информации к средствам виртуализации

приказ ФСТЭК России от 27.10.2022 № 187

Требования по безопасности информации к системам управления базами данных

приказ ФСТЭК России от 14.04.2023 № 64

Требования по безопасности информации к средствам контейнеризации

приказ ФСТЭК России от 4.07.2022 № 118

Повышение уровня квалификации экспертов

Порядок аттестации экспертов органов по сертификации и испытательных лабораторий

приказ ФСТЭК России от 27.07.2023 № 147

вступает в силу 1.09.24

Создание инфраструктуры тестирования

Создание Центра компетенций по тестированию производительности, устойчивости функционирования и функциональных возможностей МЭ и иных сетевых устройств

проект

Методика тестирования производительности NGFW

Создание среды тестирования средств защиты информации путем эмуляции действий нарушителей безопасности информации и обеспечения её функционирования

Повышение безопасности системного программного обеспечения

Технологический центр исследования безопасности ядра Linux

Размечено более **17 тыс.** предупреждений
1798 подтверждённых (из них **260** влияющих на безопасность)
275 патчей разработано и принято

Технологический центр исследования безопасности критичных компонентов

Поддерживаемые компоненты: **24**
Размечено более **10 тыс.** предупреждений
Более **700** подтверждённых (из них более **100** влияющих на безопасность)
38 патчей разработано и принято

Центр исследования безопасности системного программного обеспечения

Консорциум участников по поддержке Центра исследования

Мероприятие национального проекта «Экономика данных» (2025-2030 гг.): Обеспечение функционирования Центра исследования безопасности системного программного обеспечения

В Консорциум входят более 30 организаций, разрабатывающих сертифицированные решения на основе ядра:

- АО «Аладдин Р.Д.»
- ООО «Айдеко»
- ООО Фирма «АНКАД»
- ООО «Базальт СПО»
- ООО «БЕЛЛСОФТ»
- ЗАО «ЗЭТ»
- АО «ИВК»
- ООО «Инферит»
- АО «ИнфоТеКС»
- ООО «ИТБ»
- ООО «Код Безопасности»
- ООО «Конфидент»
- АО «МЦСТ»
- АО «НППКТ»
- ООО «Открытая мобильная платформа»
- ООО «ПиЭлСи Технолоджи»
- АО «РАСУ»
- ООО «РЕД СОФТ»
- ООО «НТЦ ИТ РОСА»
- ООО «РусБИТех-Астра»
- АО МВП «Свемел»
- ООО «ТехАргос»
- ООО «Фактор-ТС»
- АО «ФИНТЕХ»
- АО «НПО «Эшелон»
- ООО «Юзергейт»
- ООО «ЯНДЕКС.ОБЛАКО»

Обеспечение защиты информации при внедрении технологий искусственного интеллекта

Мероприятие национального проекта «Экономика данных» (2025-2030 гг.): Обеспечение защиты информации при внедрении технологий искусственного интеллекта. Повышение эффективности средств защиты информации и услуг по защите информации за счет применения технологий искусственного интеллекта

Центр исследований в области обеспечения информационной безопасности при использовании технологий искусственного интеллекта

Задачи:

- Исследование угроз безопасности при применении технологий ИИ в системах защиты информации
- Разработка большой языковой модели для применения в средствах защиты информации.
- Разработка и поддержка в актуальном состоянии информационных ресурсов для информирования о новых угрозах и оценки вероятности атак на системы защиты информации, использующих технологии ИИ
- Разработка эталонных наборов данных для обучения и верификации моделей машинного обучения, а также эталонных базовых моделей машинного обучения для решения задач обеспечения безопасности информации

Внедрение процессов безопасной разработки программного обеспечения

Порядок сертификации процессов разработки безопасного программного обеспечения средств защиты информации

утвержден приказом
ФСТЭК России
от 1 декабря 2023 г. № 240

Методика выявления уязвимостей и недекларированных возможностей в программном обеспечении

Проект

Утвержденные:

ГОСТ Р 56939-2016 «Защита информации.
Разработка безопасного программного обеспечения. Общие требования»

ГОСТ Р 58412-2019 «Защита информации.
Разработка безопасного программного обеспечения. Угрозы безопасности информации при разработке программного обеспечения»

Разрабатываемые:

ГОСТ Р «Защита информации. Разработка безопасного программного обеспечения. Руководство по оценке безопасности разработки программного обеспечения»

ГОСТ Р «Защита информации. Разработка безопасного программного обеспечения. Руководство по проведению статического анализа. Общие требования»

ГОСТ Р «Защита информации. Разработка безопасного программного обеспечения. Руководство по разработке безопасного программного обеспечения»

ГОСТ Р «Защита информации. Разработка безопасного программного обеспечения. Доверенный компилятор языков С/С++. Общие требования»

ГОСТ Р «Защита информации. Разработка безопасного программного обеспечения. Управление безопасностью программного обеспечения при использовании заимствованных и привлекаемых компонентов»

Школа фундаментальных технологий разработки безопасного программного обеспечения в МГТУ им. Н.Э.Баумана

Основные направления совершенствования технической защиты информации

Заместитель директора
Федеральной службы по техническому
и экспортному контролю

ЛЮТИКОВ Виталий Сергеевич