Направления совершенствования технической защиты информации

Начальник управления ФСТЭК России

Шевцов Дмитрий Николаевич

Совершенствование требований по технической защите информации в информационных системах

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

Приказ ФСТЭК России № 117 от 11 апреля 2025 г.

Мероприятия и меры по защите информации, содержащейся в информационных системах

Методический документ ФСТЭК России

Проект

ГОСТ Р 51583

Порядок создания автоматизированных систем в защищенном исполнении. Общие положения.

Национальный стандарт Российской Федерации

Разработанные документы по вопросам защиты информации в 2025 году

Методика испытаний систем защиты информации информационных систем методами тестирования на проникновение, утвержденная ФСТЭК России 25 июня 2025 г.

Методика анализа защищенности информационных систем, утвержденная ФСТЭК России 25 ноября 2025 г.

Приказ ФСТЭК России от 11 июня 2025 г. № 205 «О внесении изменений в Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам безопасности информационных технологий»

Приказ ФСТЭК России от 20 января 2026 г. № 9 «О внесении изменений в Положение о системе сертификации средств защиты информации»

Проект приказа ФСТЭК России « О внесении изменений в Порядок организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну…»

Планы по разработке документов в 2026 году

Требования по безопасности информации, устанавливающих уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий (новая редакция)

Требования по безопасности информации к средствам антивирусной защиты (новая редакция)

Методика тестирования производительности многофункциональных межсетевых экранов уровня сети

Методика выявления уязвимостей и недекларированных возможностей в программном обеспечении (новая редакция)

Методика по осуществлению тестирования функций безопасности информационных систем (функциональное тестирование)

Совершенствование подходов по определению трудозатрат на техническую защиту информации

Минтрудом России совместно с Минцифры России, ФСТЭК России и ФСБ России разработан проект **типовых межотраслевых норм труда (норм времени) на работы по обеспечению защиты информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений**

№ п/п	Наименование работ	Единица измерения - одна типовая информационная система (объект), государственный орган (организация) или документ	Норма времени в человеко-часах[2] (Нтип)
1	Организация и контроль деятельности по защите информации в подведомственных государственных органах (организациях) в течение года	1 орган (организация)	60
2	Разработка и утверждение политики защиты информации	1 орган (организация)	120
3	Разработка и утверждение внутренних стандартов по защите информации	1 орган (организация)	120
4	Разработка и утверждение внутренних регламентов по защите информации	1 орган (организация)	80
5	Определение лиц, ответственных за защиту информации	1 орган (организация)	10
6	Выделение организационных, технических и иных ресурсов, необходимых для защиты информации	1 орган (организация)	20
	…		

Повышение административной ответственности за нарушение требований по технической защите информации

Федеральный закон от 23 марта 2025 г. № 104-ФЗ «О внесении изменений в статьи 4.5 и 13.12 Кодекса Российской Федерации об административных правонарушениях и статью 1 Федерального закона «О внесении изменений в Кодекс Российской Федерации об административных правонарушениях»

Статья 13.12 КоАП РФ	Предыдущая редакция	Действующая редакция
Часть 2. Использование несертифицированных информационных систем, баз и банков данных, а также несертифицированных средств защиты информации, если они подлежат обязательной сертификации (за исключением средств защиты информации, составляющей государственную тайну)	граждане - от 1,5 до 2,5 тыс. р. должностные лица - от 2,5 до 3 тыс. р. юридические лица - от 20 до 25 тыс. р.	граждане - **от 5 до 10 тыс. р.** должностные лица - **от 10 до 50 тыс. р.** юридические лица - **от 50 до 100 тыс. р.**
Часть 4. Использование несертифицированных средств, предназначенных для защиты информации, составляющей государственную тайну	должностные лица – от 3 до 4 тыс. р. юридические лица - от 20 до 30 тыс. р.	должностные лица - **от 20 до 50 тыс. р.** юридические лица - **от 50 до 100 тыс. р.**
Часть 6. Нарушение требований о защите информации (за исключением информации, составляющей государственную тайну), установленных федеральными законами и принятыми в соответствии с ними иными нормативными правовыми актами Российской Федерации	граждане - 0,5 до 1 тыс. р. должностные лица - от 1 до 2 тыс. р. юридические лица - от 10 до 15 тыс. р.	граждане - **от 5 до 10 тыс. р.** должностные лица - **от 10 до 50 тыс. р.** юридические лица - **от 50 до 100 тыс. р.**
Часть 7. Нарушение требований о защите информации, составляющей государственную тайну, установленных федеральными законами и принятыми в соответствии с ними иными нормативными правовыми актами Российской Федерации	граждане - от 1 до 2 тыс. р. должностные лица - от 3 до 4 тыс. р. юридические лица - от 15 до 20 тыс. р.	граждане - **от 10 до 20 тыс. р.** должностные лица - **от 20 до 50 тыс. р.** юридические лица - **от 50 до 100 тыс. р.**

Увеличен установленный частью 1 статьи 4.5 КоАП РФ срок давности привлечения к ответственности за административные правонарушения, предусмотренные статьей 13.12 КоАП РФ, до 1 года.

Повышение качества аттестации информационных систем

Порядок организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну

приказ ФСТЭК России
от 29 апреля 2021 г. № 77

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

Основные нарушения:

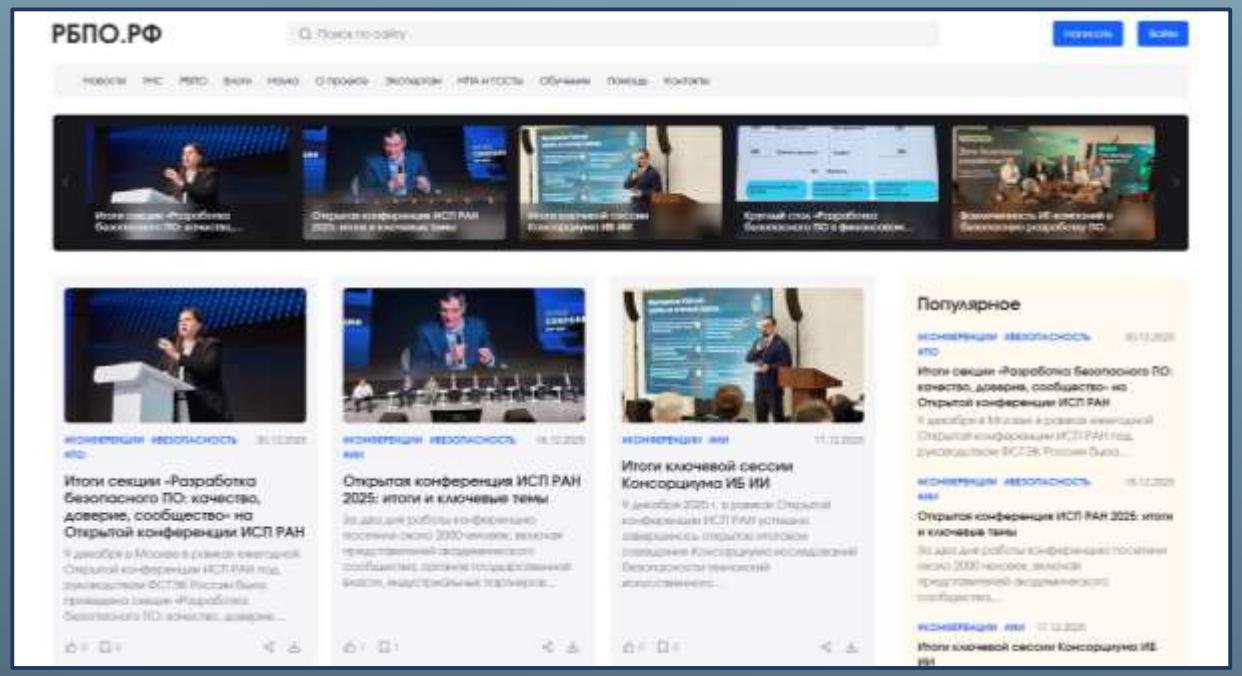
Отсутствие результатов проведения испытаний системы защиты информации путём осуществления тестирования её функций безопасности (функциональное тестирование)

Отсутствие результатов проведения испытаний системы защиты информации путём осуществления попыток несанкционированного доступа (воздействия) в обход системы защиты информации с использованием средств защиты информации

Отсутствие результатов проведения анализа уязвимостей с использованием средств контроля эффективности защиты информации от несанкционированного доступа

В 90% рассмотренных материалов выявляются указанные недостатки

Внедрение практик разработки безопасного программного обеспечения



РБПО.РФ

В 2025 году в рамках создания отечественного ресурса Унифицированная среда разработки безопасного отечественного ПО были достигнуты следующие результаты:

Разработана методология проведения композиционного анализа

Проводится апробация предоставления доступа пользователей к личным кабинетам, методическим материалам

Разработана методология проведения статического анализа

Проводится разработка методологии по иным процессам

Сертификация процессов разработки безопасного программного обеспечения средств защиты информации

Порядок сертификации процессов разработки безопасного программного обеспечения средств защиты информации

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

Национальный стандарт ГОСТ Р 56939-2024 «Защита информации. Разработка безопасного программного обеспечения. Общие требования»

Органы по сертификации

ИСП РАН

АТОМЗАЩИТАИНФОРМ
РОСАТОМ

Организации имеющие сертификат:

ОТКРЫТАЯ МОБИЛЬНАЯ ПЛАТФОРМА

SBER TECH

РусБИТех-Астра

PostgresPro

kaspersky

positive technologies

infotecs

Количество заявок на сертификацию: 22

Количество решений: 15

Количество сертификатов: 7

Повышение уровня безопасности средств защиты информации за счет проверки целостности и подлинности ПО и его обновлений на основе сертификатов безопасности

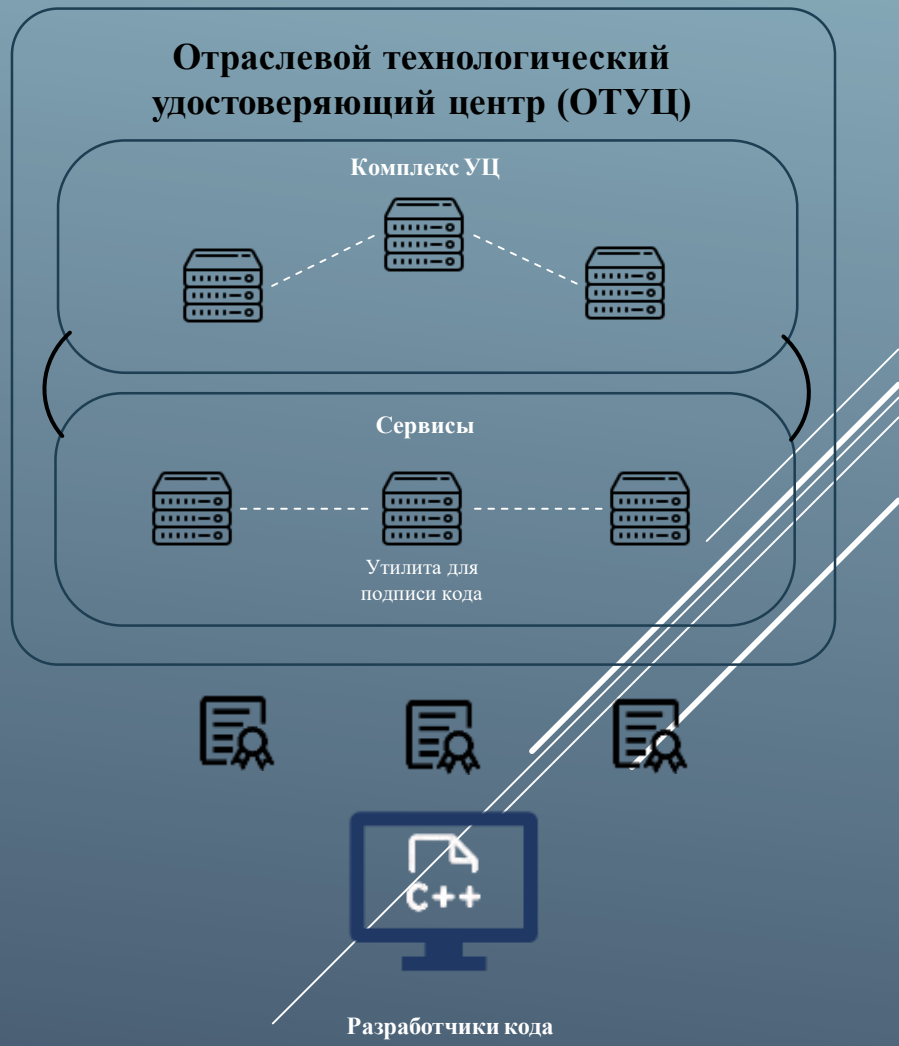
Цель:
Разработка и регламентация системного подхода по подтверждению целостности и авторства программного обеспечения средств защиты информации

Проблематика:
Отсутствие массовой практики подтверждения целостности и авторства ПО с поддержкой ГОСТ

Задачи:
Обеспечение целостности ПО;
Обеспечение совместимости ПО;
Обеспечение аутентичности ПО;
Инвентаризация ПО.

Реализован выпуск сертификатов

- ✓ сертификаты меток доверенного программного кода (формирование и проверка цифровой подписи российского ПО)



Контроль за устранением уязвимостей в сертифицированных средствах защиты информации

Порядок испытаний и поддержки безопасности средств защиты информации, в состав которых входят заимствованные программные компоненты с открытым исходным кодом

письмо ФСТЭК России
от 26 сентября 2024 г. № 240/24/4436

Более 90% (более 380)сертифицированных средств защиты информации созданы с использованием заимствованных программных компонентов

Часто используемые заимствованные программные компоненты при разработке СЗИ:

- Nginx
- Libvirt
- OpenSSL
- Qemu
- NodeJS

Сведения о SBOM представила **141** организация (69%)

Сведения о SBOM **НЕ** представили **83** организации (31%)

Выдано более **90** планов испытаний на средства защиты информации

Выдано **17** планов поддержки на средства защиты информации

Средства защиты информации, в состав которых включены заимствованные программные компоненты с открытым исходным кодом

Количество заимствованных программных компонентов в СЗИ

- В операционных системах свыше 1900 заимствованных программных компонентов
- В средствах виртуализации свыше 750 заимствованных программных компонентов
- В средстве контейнеризации свыше 840 заимствованных программных компонентов
- В системах управления базами данных свыше 580 заимствованных программных компонентов

Автоматизированная инвентаризация заимствованных программных компонентов

trivy | OWASP dep-scan | bin-tool | CodeScoring

Выявление директивных и транзитивных компонентов, входящих в состав СЗИ

Отсутствие возможности исключения «нежелательных» компонентов, входящих с состав СЗИ

Выявление уязвимостей в заимствованных программных компонентах, входящих в состав СЗИ

Выполнение на регулярной основе проверки заимствованных программных компонентов

Проблематика:

- Разработчики средств защиты информации не обладают сведениями о полном перечне программных компонентов
- Не проводится анализ уязвимостей заимствованных программных компонентов
- Не автоматизирован процесс формирования перечня заимствованных программных компонентов и анализа их уязвимостей

Аттестация работников органов по сертификации и испытательных лабораторий

Порядок аттестации работников органов по сертификации и испытательных лабораторий, выполняющих работы по оценке (подтверждению) соответствия в отношении продукции (работ, услуг), используемой в целях защиты сведений, составляющих государственную тайну или относимых к охраняемой в соответствии с законодательством Российской Федерации иной информации ограниченного доступа

утвержден приказом ФСТЭК России от 27 июля 2023 г. № 147

Количество заявок от 39 организаций на аттестацию 263 экспертов

Не прошли первичный отбор 15 экспертов

Принято решение о допуске 248 экспертов, из которых

Аттестовано **160 (65%)** экспертов

Запланирована аттестация 24 эксперта

Не прошли аттестацию 64 (26%) эксперта

Аттестация экспертов осуществляется на материально-технической базе МГТУ им. Н.Э.Баумана

Только 30% экспертов сдают теоретическую часть с первого раза
Только 5% экспертов решают практическую часть с первого раза

Эксперты отвечают правильно на **48%** вопросов в части Требований по безопасности информации к СЗИ

Эксперты отвечают правильно на **70%** вопросов в части Положения о системе сертификации

Эксперты отвечают правильно на **78%** вопросов в части Требований по безопасности информации, устанавливающих уровни доверия

Направления совершенствования технической защиты информации

Начальник управления ФСТЭК России

Шевцов Дмитрий Николаевич