



Совершенствование требований по технической защите информации

**Начальник управления ФСТЭК России
Шевцов Дмитрий Николаевич**

ИЗМЕНЕНИЯ В ПОЛОЖЕНИЕ О СИСТЕМЕ СЕРТИФИКАЦИИ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ



**Изменения в Положение о
системе сертификации средств
защиты информации,
утвержденное приказом
ФСТЭК России
от 3 апреля 2018 г. № 55**

**утверждены приказом ФСТЭК
России от 5 августа 2021 г.
№ 121**

**вступили в силу
с 7 ноября 2021 г.**

**Особенности сертификации средств
защиты информации иностранного
производства**

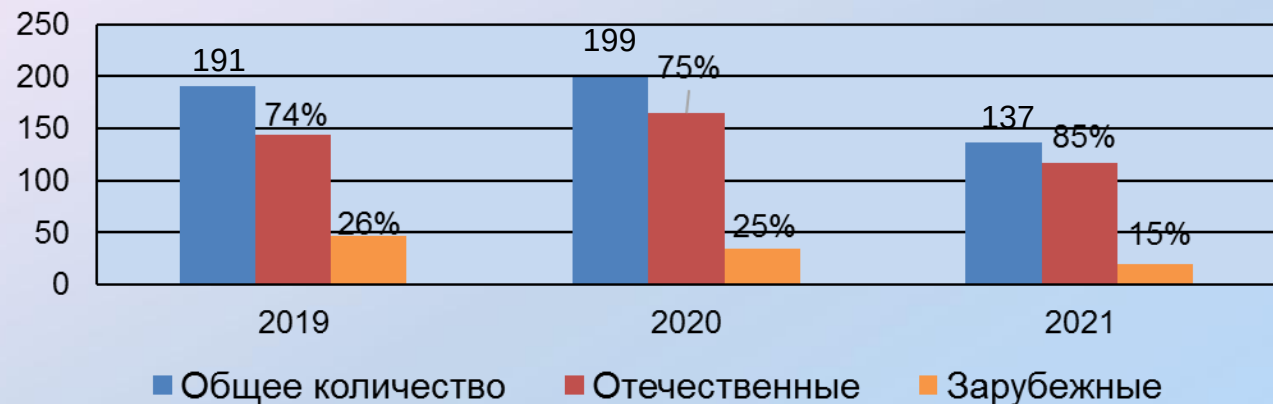
**Новый порядок маркирования средств
защиты информации**

**Изменение порядка отбора образцов
средств защиты информации и
порядка ознакомления с ними
ИЛ и ОС**

**Упрощение порядка продления сроков
действия сертификатов соответствия**

ПОКАЗАТЕЛИ ДЕЯТЕЛЬНОСТИ СИСТЕМЫ СЕРТИФИКАЦИИ СЗИ

Количество выданных сертификатов
соответствия



В настоящее время **производится 411** типов сертифицированных средств защиты информации. Из них **332** – средства защиты информации от несанкционированного доступа и **79** – средства защиты информации от утечки по техническим каналам.

87 % СЗИ отечественного производства.

Ежегодно производится **1000000** экземпляров сертифицированных СЗИ.

Количество основных типов производимых СЗИ НСД

Операционные системы (20 сертификатов)

Системы управления базами данных (9 сертификатов)

Средства виртуализации (9 сертификатов)

Средства доверенной загрузки (11 сертификатов)

Средства контроля и анализа защищенности (12 сертификатов)

Средства антивирусной защиты (21 сертификат)

Системы обнаружения вторжений (28 сертификатов)

Межсетевые экраны (53 сертификата)

Средства контроля съемных машинных носителей информации (4 сертификата)

DLP – системы (5 сертификатов)

Средства защиты от DOS-атак (3 сертификата)

Системы управления событиями безопасности (12 сертификатов)

ПОРЯДОК АТТЕСТАЦИИ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ

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

**утвержден приказом
ФСТЭК России
от 28 сентября 2020 г. № 110**

зарегистрирован Минюстом России, регистрационный № 62451
от 10 февраля 2021 г.

Вступил в силу с 1 июня 2021 г.

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

**утвержден приказом
ФСТЭК России
от 29 апреля 2021 г. № 77**

зарегистрирован Минюстом России, регистрационный № 64589
от 10 августа 2021 г.

Вступил в силу с 1 сентября 2021 г.

Определяют состав и содержание работ по аттестации объектов информатизации,

Устанавливают требования к форме и содержанию документов, разрабатываемых при аттестации

Порядок проведения работ по аттестации объектов информатизации

**Представление ИД
по ОИ в ОА**

Владелец ОИ
представляет в ОА в
электронном виде

**Обследование ОИ в
условиях эксплуатации**

Проводится при
необходимости ОА

**Разработка и
согласование ПИМ АИ**

Разрабатывается ОА,
согласовывается с
владельцем ОИ

**Проведение
АИ ОИ**

Проводятся ОА в
соответствии с п. 18
Порядка

**Оформление
результатов АИ**

Оформляются ОА:
1. Протоколы АИ;
2. Заключение по АИ

**Оформление аттестата
соответствия**

Оформляется ОА в
соответствии с образцом

**Внесение изменений
в ОИ**

Осуществляется по
согласованию с ОА

**Поддержка
безопасности
аттестованного ОИ**

Организуется
владельцем ОИ



КОНТРОЛЬ ЗА КАЧЕСТВОМ ВЫПОЛНЕНИЯ РАБОТ ПО АТТЕСТАЦИИ ОИ

Ведение реестра
аттестованных ОИ

Проведение экспертизы
материалов АИ

Приостановление и
прекращение действия
аттестата соответствия

ПОРЯДОК ПРЕДСТАВЛЕНИЯ ДОКУМЕНТОВ

Владелец ОИ



Орган по аттестации



**ФСТЭК России
(территориальный орган
ФСТЭК России)**

**Техпаспорт ИС
Акт классификации ИС
Модель угроз БИ
Техническое задание
Проектная и эксплуатационная документация
Организационно-распорядительные документы
Документы по результатам анализа уязвимостей**

**Аттестат соответствия ОИ
Технический паспорт на ОИ
Акт классификации (категорирования) ИС
Программу и методики АИ
Протоколы АИ
Заключение по АИ**

Вносит сведения в реестр аттестованных ОИ



ПРОВЕДЕНИЕ ЭКСПЕРТНО-ДОКУМЕНТАЛЬНОЙ ОЦЕНКИ МАТЕРИАЛОВ АТТЕСТАЦИИ



ТРЕБОВАНИЯ ДОВЕРИЯ К СРЕДСТВАМ ЗАЩИТЫ ИНФОРМАЦИИ

**Требования
по безопасности информации,
устанавливающие уровни доверия
к средствам технической защиты
информации и средствам обеспечения
безопасности информационных технологий**

**Приказ
ФСТЭК России
от 2 июня 2020 г. № 76 (зарегистрирован
Минюстом России
11 сентября 2020 г.
№ 59772)**

С 1 января 2022 г. (п.п. 12.2, 12.4):

применение отечественных аппаратных платформ СЗИ (с 5 уровня доверия) и СВТ, являющихся средой функционирования СЗИ (с 3 уровня доверия)

С 1 января 2024 г. (п. 12.3):

применение отечественных процессоров, микросхем, элементов памяти, сетевых карт, графических адаптеров СЗИ (с 4 уровня доверия)

С 1 января 2028 г. (п. 12.5):

применение отечественных процессоров, микросхем, элементов памяти, сетевых карт, графических адаптеров СВТ, являющихся средой функционирования СЗИ (с 2 уровня доверия)

Требования по безопасности информации к средствам контейнеризации



Требования по безопасности информации к средствам контейнеризации

Проект

Функциональные возможности:

формирование среды выполнения контейнеров и обеспечения выполнения их процессов

запуск контейнера и управление данным контейнером

создание образов контейнеров

распространение образов контейнеров

централизованное управление контейнерами и организацией взаимодействия между ними

Функции безопасности:

управление доступом

идентификация и аутентификация пользователей

изоляция контейнеров

выявление уязвимостей в образах контейнеров

проверка корректности конфигурации контейнеров

контроль целостности контейнеров и их образов

централизованное управление образами контейнеров и контейнерами

регистрация событий безопасности



МЕТОДИКА ВЫЯВЛЕНИЯ УЯЗВИМОСТЕЙ И НЕДЕКЛАРИРОВАННЫХ ВОЗМОЖНОСТЕЙ В ПРОГРАММНОМ ОБЕСПЕЧЕНИИ



**Методика выявления
уязвимостей и
недекларированных
возможностей в
программном обеспечении**

**Утверждена
ФСТЭК России
11 февраля 2019 г.**



**Методика выявления уязвимостей
и недекларированных
возможностей в программном
обеспечении**

**Утверждена
ФСТЭК России
25 декабря 2020 г.**

Уточнение (детализация) процедур:

подготовки исследовательского стенда

анализа архитектуры объекта оценки

**статического анализа исходного кода объекта
оценки**

фаззинг-тестирования

экспертизы кода объекта оценки

ПРОГРАММЫ ПОВЫШЕНИЯ КВАЛИФИКАЦИИ ПО ВЫЯВЛЕНИЮ УЯЗВИМОСТЕЙ И НЕДЕКЛАРИРОВАННЫХ ВОЗМОЖНОСТЕЙ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

ПРОВОДЯТСЯ С 2020 ГОДА

Техническая защита информации. Инструментальная и технологическая поддержка методики выявления уязвимостей и недекларированных возможностей в программном обеспечении

Техническая защита информации. Инструментальная и технологическая поддержка фаззинг-тестирования программного обеспечения

ПРОВОДЯТСЯ С 2021 ГОДА

Техническая защита информации. Выявление уязвимостей в программном обеспечении по анализу архитектуры и экспертизе кода в соответствии с Методикой выявления уязвимостей и недекларированных возможностей в программном обеспечении

Техническая защита информации. Выявление уязвимостей в программном обеспечении по статическому анализу в соответствии с Методикой выявления уязвимостей и недекларированных возможностей в программном обеспечении

ВИДЕОЛЕКЦИИ ДЛЯ СПЕЦИАЛИСТОВ

The screenshot shows the website bdu.fstec.ru with the page title "Видеолекции для специалистов в области информационной безопасности". The page contains text about the development of video lectures by the Federal Scientific Center of Information Security (FSTEC Russia) and the Institute of System Programming (ISP RAS). It lists the following topics for the video lectures:

- Особенности фаззинг-тестирования при проведении сертификационных испытаний
- Подходы к фаззинг-тестированию управляемого кода
- Основы динамического символьного выполнения. Поиск ошибок при помощи динамического символьного выполнения
- Инструментальная и технологическая поддержка проведения фаззинг-тестирования программного обеспечения

The video lecture thumbnails show the speaker's name "Дмитрий ПОНОМАРЁВ" and the title "Вводная лекция".

[HTTPS://BDU.FSTEC.RU/EDUCATION#/](https://bdu.fstec.ru/education#/)

t.me/sdl_static

t.me/sdl_dynamic



СТАНДАРТИЗАЦИЯ В ОБЛАСТИ ТЕХНИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

Технический комитет 362

Подкомитет 1 Общеметодологический

Подкомитет 2 Защита информации на объектах информатизации и объектах критической информационной инфраструктуры

Подкомитет 3 Средства и методы защиты информации

Подкомитет 4 Разработка безопасного программного обеспечения

Национальный стандарт Российской Федерации
ГОСТ Р 59547-2021
«Защита информации. Регистрация событий безопасности.
Требования к регистрируемой информации»

Национальный стандарт Российской Федерации
ГОСТ Р ИСО/МЭК 27001-2021
«Информационная технология. Методы и средства обеспечения
безопасности. Система менеджмента информационной безопасности.
Требования»

Национальный стандарт Российской Федерации
ГОСТ Р 59453.1-2021
«Защита информации. Формальная модель управления доступом.
Общие положения»

Национальный стандарт Российской Федерации
ГОСТ Р 59453.2-2021
«Защита информации. Формальная модель управления доступом.
Рекомендации по верификации формальной модели управления
доступом»

Национальный стандарт Российской Федерации
ГОСТ Р 59548-2022
«Защита информации. Мониторинг информационной безопасности.
Общие положения»

Стандарты, утвержденные в 2021 - 2022 годах

ГОСТ Р «Защита информации. Управление компьютерными инцидентами.
Термины и определения»

ГОСТ Р «Защита информации. Управление компьютерными инцидентами.
Общие положения»

ГОСТ Р «Защита информации. Управление компьютерными инцидентами.
Организация деятельности по управлению компьютерными инцидентами»

ГОСТ Р «Защита информации. Управление компьютерными инцидентами.
Руководство по реагированию на компьютерные инциденты»

ГОСТ Р «Защита информации. Идентификация и аутентификация. Уровни
доверия идентификации»

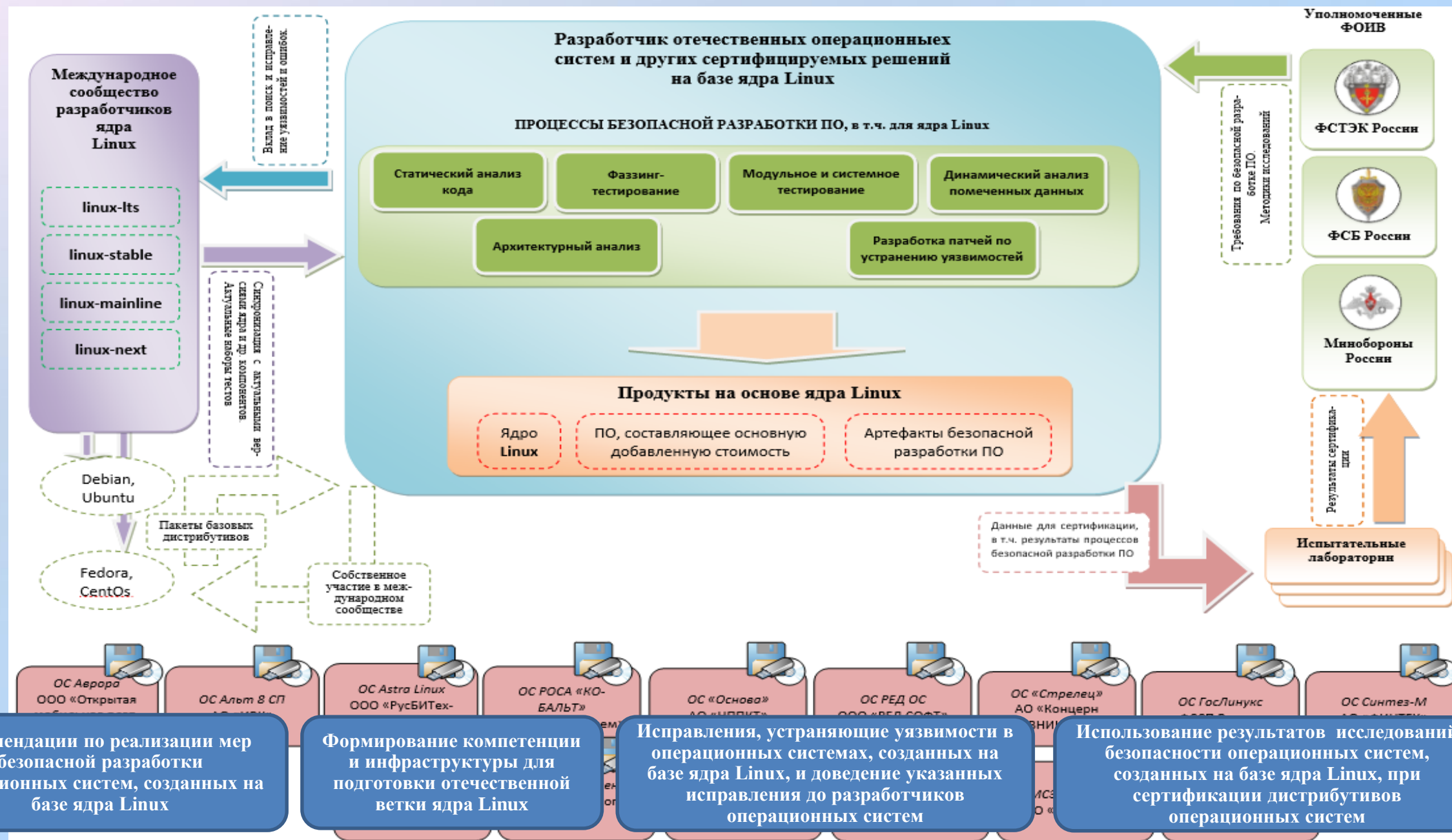
ГОСТ Р «Защита информации. Идентификация и аутентификация. Уровни
доверия аутентификации»

ГОСТ Р «Защита информации. Идентификация и аутентификация. Управление
идентификацией и аутентификацией»

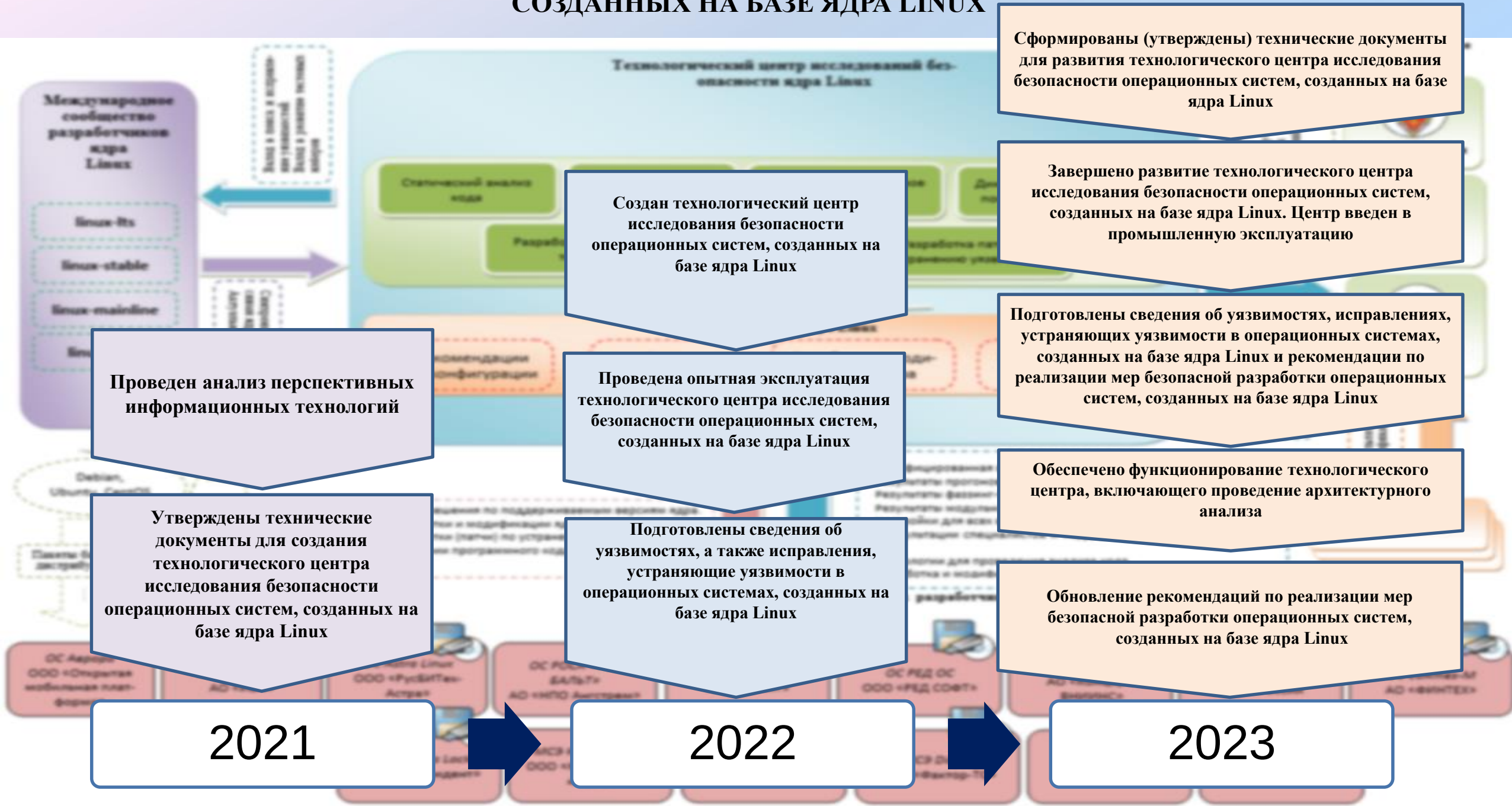
ГОСТ Р «Защита информации от несанкционированного доступа. Термины
и определения»

Планируются на утверждение в 2022 году

Схема организации работ по разработке операционных систем и других сертифицируемых решений на базе ядра Linux

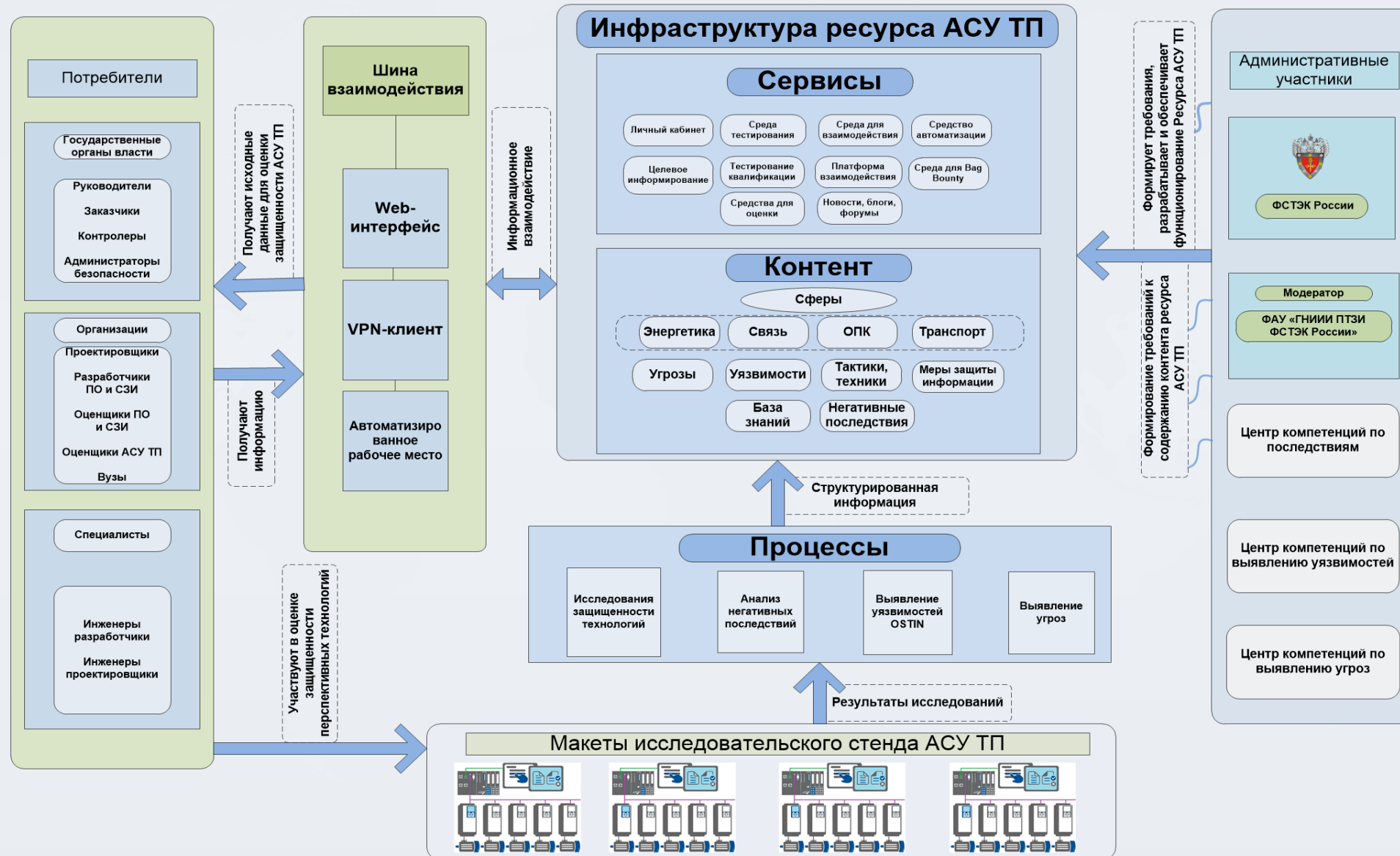


ТЕХНОЛОГИЧЕСКИЙ ЦЕНТР ИССЛЕДОВАНИЯ БЕЗОПАСНОСТИ ОПЕРАЦИОННЫХ СИСТЕМ, СОЗДАННЫХ НА БАЗЕ ЯДРА LINUX



ОТЕЧЕСТВЕННЫЙ РЕСУРС С УЯЗВИМОСТЯМИ УРОВНЯ АВТОМАТИЗИРОВАННЫХ СИСТЕМ УПРАВЛЕНИЯ ТЕХНОЛОГИЧЕСКИМИ ПРОЦЕССАМИ И ПРОМЫШЛЕННОГО ИНТЕРНЕТА ВЕЩЕЙ КРИТИЧЕСКИ ВАЖНЫХ, ПОТЕНЦИАЛЬНО ОПАСНЫХ И ОПАСНЫХ ПРОИЗВОДСТВЕННЫХ ОБЪЕКТОВ В ЦЕЛЯХ ИНФОРМИРОВАНИЯ ОБ УЯЗВИМОСТЯХ ВЛАДЕЛЬЦЕВ ОБЪЕКТОВ

Концепция отечественного ресурса с уязвимостями уровня автоматизированных систем управления технологическими процессами и промышленного интернета вещей критически важных, потенциально опасных и опасных производственных объектов в целях информирования об уязвимостях владельцев объектов



Своевременное выявление уязвимостей автоматизированных систем управления технологическими процессами и промышленного интернета вещей критически важных

Повышение качества программного обеспечения, применяемого в автоматизированных системах управления технологическими процессами и промышленного Интернета вещей критически важных

Повышение квалификации специалистов, занимающихся вопросами контроля за обеспечением уровня защищенности (аудита безопасности) автоматизированных систем управления технологическими процессами и промышленного интернета вещей

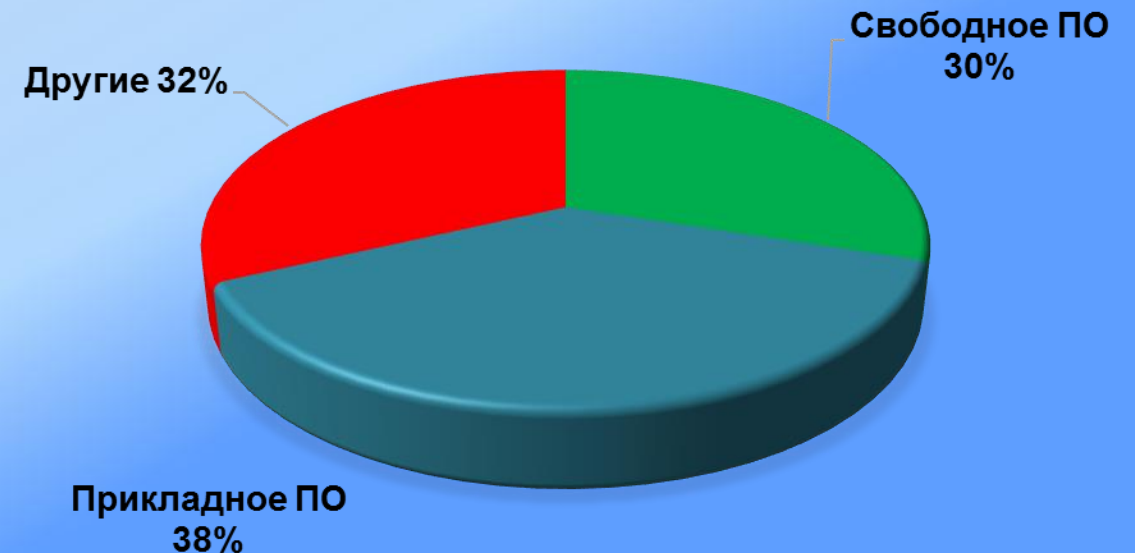
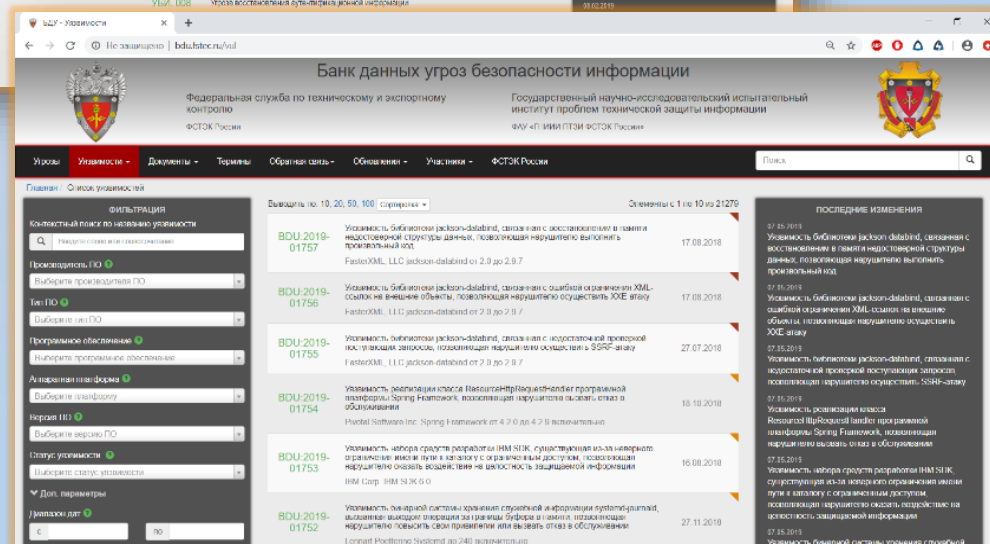
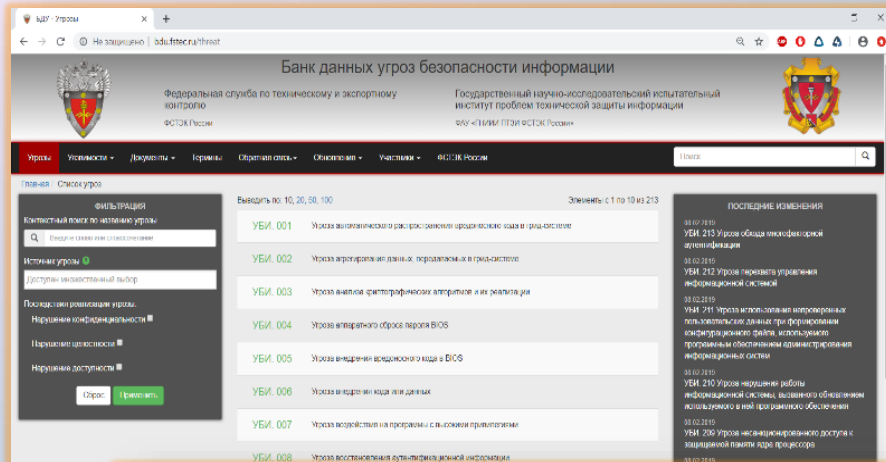
ОТЕЧЕСТВЕННЫЙ РЕСУРС С УЯЗВИМОСТЯМИ УРОВНЯ АВТОМАТИЗИРОВАННЫХ СИСТЕМ УПРАВЛЕНИЯ ТЕХНОЛОГИЧЕСКИМИ ПРОЦЕССАМИ И ПРОМЫШЛЕННОГО ИНТЕРНЕТА ВЕЩЕЙ КРИТИЧЕСКИ ВАЖНЫХ, ПОТЕНЦИАЛЬНО ОПАСНЫХ И ОПАСНЫХ ПРОИЗВОДСТВЕННЫХ ОБЪЕКТОВ В ЦЕЛЯХ ИНФОРМИРОВАНИЯ ОБ УЯЗВИМОСТЯХ ВЛАДЕЛЬЦЕВ ОБЪЕКТОВ



ВЫЯВЛЕНИЕ И УСТРАНЕНИЕ УЯЗВИМОСТЕЙ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ И ОБОРУДОВАНИЯ

По состоянию на январь 2022 г.
Банк данных угроз безопасности информации
содержит:

- сведения о **222** угрозах безопасности информации;
- сведения о более **37 000** уязвимостей программного обеспечения



bdu.fstec.ru

РЕКОМЕНДАЦИИ ПО УСТРАНЕНИЮ УЯЗВИМОСТЕЙ В ГОСУДАРСТВЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ



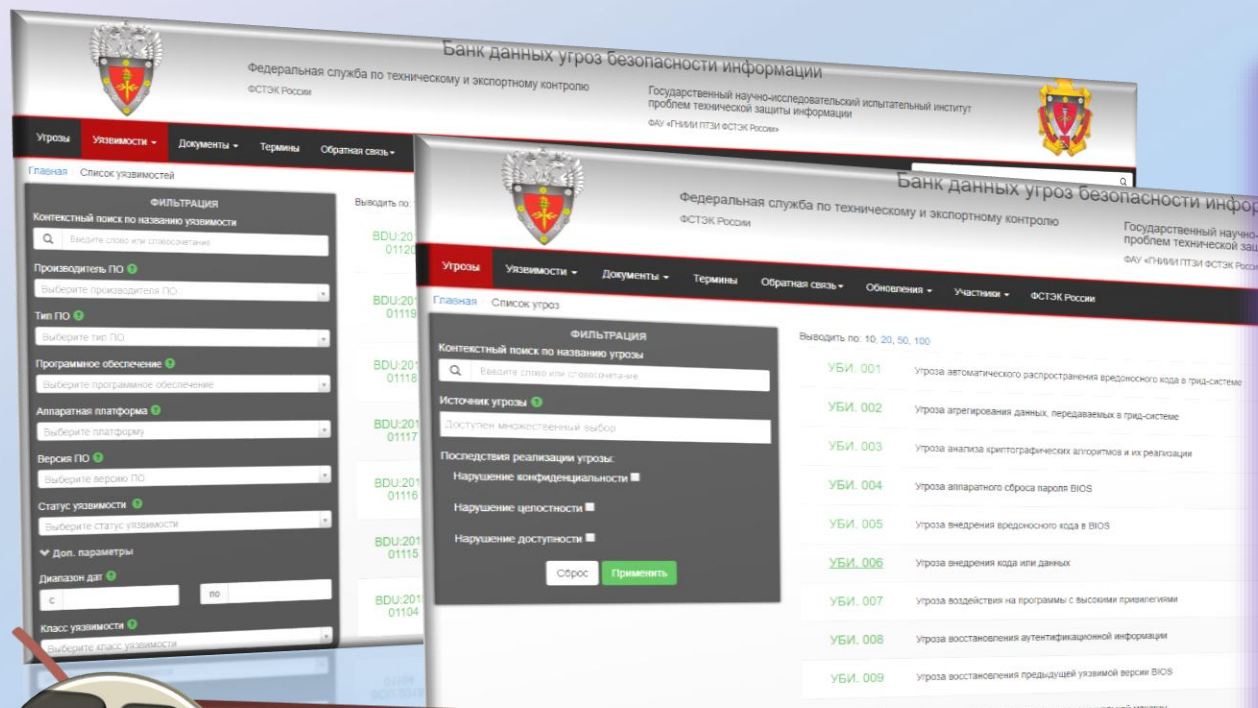
kubernetes



Apache



БАНК ДАННЫХ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ ФСТЭК РОССИИ



Изменения в Методику оценки угроз



Совершенствование банка данных угроз

УТВЕРЖДЕН
ФСТЭК России
5 февраля 2021 г.



ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ТЕХНИЧЕСКОМУ
И ЭКСПОРТНОМУ КОНТРОЛЮ

МЕТОДИЧЕСКИЙ ДОКУМЕНТ

Методика оценки угроз безопасности
информации ФСТЭК России

ОСНОВНЫЕ НАПРАВЛЕНИЯ СОВЕРШЕНСТВОВАНИЯ ДЕЯТЕЛЬНОСТИ ПО ТЕХНИЧЕСКОЙ ЗАЩИТЕ ИНФОРМАЦИИ В 2022, 2023 ГОДАХ

Совершенствование требований по технической защите информации и мер защиты информации

Разработка требований по безопасности информации к средствам защиты информации

Совершенствование качества работ по аттестации объектов информатизации

Совершенствование качества проведения сертификационных испытаний за счет аттестации экспертов органов по сертификации и специалистов испытательных лабораторий

Повышение качества сертифицированных средств защиты информации за счет внедрения и сертификации соответствия систем безопасной разработки

Проведение оценки соответствия систем организации и управления защитой информации операторов центров обработки данных, оказывающих услуги по хранению и обработке информации, обладателями которой являются государственные органы



Совершенствование требований по технической защите информации

**Начальник управления ФСТЭК России
Шевцов Дмитрий Николаевич**