Основные направления системы защиты информации

Заместитель директора
Федеральной службы по техническому
и экспортному контролю

ЛЮТИКОВ Виталий Сергеевич

ПОЛОЖЕНИЕ О ГОСУДАРСТВЕННОЙ СИСТЕМЕ ЗАЩИТЫ ИНФОРМАЦИИ

Проект

Указ Президента Российской Федерации «Об утверждении Положения о государственной системе защиты информации»

- Устанавливает организационные подходы к защите информации ограниченного доступа, а также защите общедоступной информации
- Определяет организационную основу государственной системы защиты информации
- Определяет основные направления деятельности государственной системы защиты информации на федеральном, межрегиональном, региональном, ведомственном и объектовых уровнях

Организационная основа государственной системы защиты информации

- ФСТЭК России
- ФСБ России
- Организации, выполняющие работы по защите информации
- Разработчики средств защиты информации
- Органы по сертификации и испытательные лаборатории
- Научные организации
- Образовательные организации, осуществляющие подготовку кадров области ИБ

ИЗМЕНЕНИЯ В ПОЛОЖЕНИЕ О СИСТЕМЕ СЕРТИФИКАЦИИ

Изменения в Положение о системе сертификации
(приказ ФСТЭК России от 19 сентября 2022 г. № 172 (зарегистрирован Минюстом России 19 октября 2022 г. № 70614))

Сокращение сроков рассмотрения документов по сертификации средств защиты информации и сроков проведения отдельных работ

Разработка и утверждения ПиМ в срок не более 30 к. д. из которых:
- разработка ПиМ ИЛ (до 20 к. д.);
- рассмотрение ПиМ ОС (до 10 к. д.)

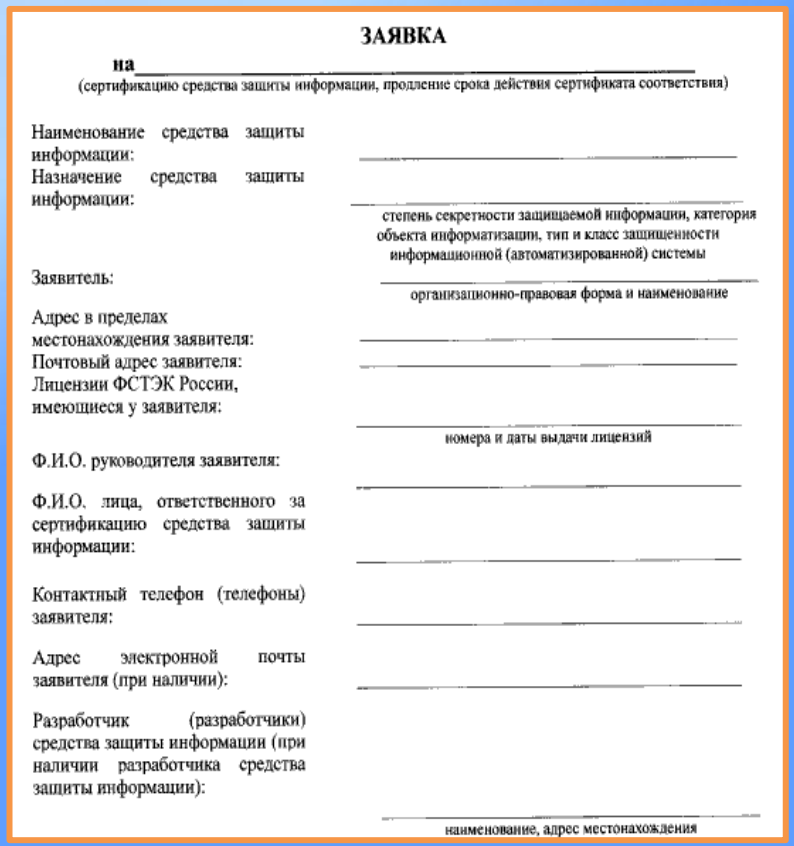
Устранение выявленных в материалах сертификации недостатков ОС, ИЛ, заявителем в срок не более 30 к. д.

Рассмотрение материалов сертификации недостатков ФСТЭК России и ОС в срок не более 15 к. д.

Проведение дополнительных испытаний разработчиком средств защиты информации

Заявитель, являющийся разработчиком средства защиты информации и имеющий **сертификат соответствия процедур безопасной разработки**, в случае внесения изменений, в том числе связанных с функциями безопасности информации,
проводит испытания самостоятельно или с привлечением испытательной лаборатории

Уточнение формы заявки на сертификацию средств защиты информации



ЗАЯВКА

на_____
(сертификацию средства защиты информации, продление срока действия сертификата соответствия)

Наименование средства защиты информации: _____

Назначение средства защиты информации: _____
степень секретности защищаемой информации, категория объекта информатизации, тип и класс защищенности информационной (автоматизированной) системы

Заявитель: _____
организационно-правовая форма и наименование

Адрес в пределах местонахождения заявителя: _____

Почтовый адрес заявителя: _____

Лицензии ФСТЭК России, имеющиеся у заявителя: _____
номера и даты выдачи лицензий

Ф.И.О. руководителя заявителя: _____

Ф.И.О. лица, ответственного за сертификацию средства защиты информации: _____

Контактный телефон (телефоны) заявителя: _____

Адрес электронной почты заявителя (при наличии): _____

Разработчик (разработчики) средства защиты информации (при наличии разработчика средства защиты информации): _____
наименование, адрес местонахождения

СОВЕРШЕНСТВОВАНИЕ БЕЗОПАСНОЙ РАЗРАБОТКИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Проект

Порядок проведения сертификации процессов безопасной разработки программного обеспечения средств защиты информации

Цели:

- Внедрение отечественными разработчиками процедур безопасной разработки
- Совершенствование качества разработки программного обеспечения
- Обеспечение качественной поддержки безопасности программного обеспечения

СОВЕРШЕНСТВОВАНИЕ ПРОЦЕДУР АККРЕДИТАЦИИ

Проект

Порядок аттестации экспертов органов по сертификации и испытательных лабораторий

Цели:

- Повышение уровня знаний и практических навыков у экспертов органов по сертификации и испытательных лабораторий
- Совершенствование процедур аккредитации органов по сертификации и испытательных лабораторий
- Создание условий для профессиональной деятельности и трудоустройства экспертов и специалистов.

Задачи:

- Внести изменения в Порядок аккредитации в части установления требования об аттестации экспертов и специалистов, а также порядка их аттестации.
- Разработать тесты и практические задания для проведения аттестации.

ИЗМЕНЕНИЯ В ТРЕБОВАНИЯ ДОВЕРИЯ

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)

Изменения в Требования доверия
приказ ФСТЭК России от 18 апреля 2022 г. № 68
(зарегистрирован Минюстом России 20 июля 2022 г. № 69318)

с 1 января 2024 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 2026 г. (п. 12.3):
применение отечественных процессоров, микросхем, элементов памяти, сетевых карт, графических адаптеров СЗИ (с 4 уровня доверия)

с 1 января 2030 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

Приказ ФСТЭК России от 4 июля 2022 г. № 118 (зарегистрирован Минюстом России 29 сентября 2022 г., регистрационный № 70275)

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

✓ Разработка требований → ✓ Обсуждение с экспертами → ✓ Оценка регулирующего воздействия → ✓ Регистрация в Минюсте России → ✓ Вступил в силу

ТРЕБОВАНИЯ ПО БЕЗОПАСНОСТИ ИНФОРМАЦИИ К СРЕДСТВАМ ВИРТУАЛИЗАЦИИ

Требования по безопасности информации к средствам виртуализации

Приказ ФСТЭК России от 27 октября 2022 г. № 187

(зарегистрирован Минюстом России 22 декабря 2022 г., регистрационный № 71774)

Функциональные возможности:	Функции безопасности:
создание образов виртуальных машин	доверенная загрузка виртуальных машин средством виртуализации
формирование среды выполнения виртуальных машин	контроль целостности в средстве виртуализации
централизованное управление виртуальными машинами и организацией взаимодействия между ними	регистрация событий безопасности в средстве виртуализации
	управление доступом в средстве виртуализации
	резервное копирование виртуальных машин
	централизованное управление образами виртуальных машин и виртуальными машинами в средстве виртуализации
	идентификация и аутентификация пользователей

✓ Разработка требований → ✓ Обсуждение с экспертами → ✓ Оценка регулирующего воздействия → ✓ Регистрация в Минюсте России → ✓ Вступил в силу

ТРЕБОВАНИЯ ПО БЕЗОПАСНОСТИ ИНФОРМАЦИИ К МНОГОФУНКЦИОНАЛЬНЫМ МЕЖСЕТЕВЫМ ЭКРАНАМ УРОВНЯ СЕТИ

Требования по безопасности информации к многофункциональным межсетевым экранам уровня сети

Многофункциональные межсетевые экраны уровня сети:

программно-аппаратные средства, реализующие контроль за информацией, поступающей в информационную систему и (или) выходящей из информационной системы, и обеспечивающим защиту информационной системы от угроз безопасности информации, связанных с подключением к сетям связи общего пользования

Функции безопасности:

- фильтрация сетевого трафика
- обнаружение и блокирование компьютерных атак
- обнаружение и блокирование вредоносного программного обеспечения
- управление доступом
- идентификация и аутентификация пользователей
- тестирование и контроль целостности
- централизованное управление
- доверенная загрузка межсетевого экрана
- производительность межсетевого экрана
- аппаратная платформа межсетевого экрана
- обеспечение бесперебойного функционирования и восстановления

- ✓ Разработка требований
- ✓ Обсуждение с экспертами
- ✓ Оценка регулирующего воздействия
- Регистрация в Минюсте России
- Вступление в силу

ТРЕБОВАНИЯ ПО БЕЗОПАСНОСТИ ИНФОРМАЦИИ К СИСТЕМАМ УПРАВЛЕНИЯ БАЗАМИ ДАННЫХ

Проект

Требования по безопасности информации к системам управления базами данных

Системы управления базами данных:

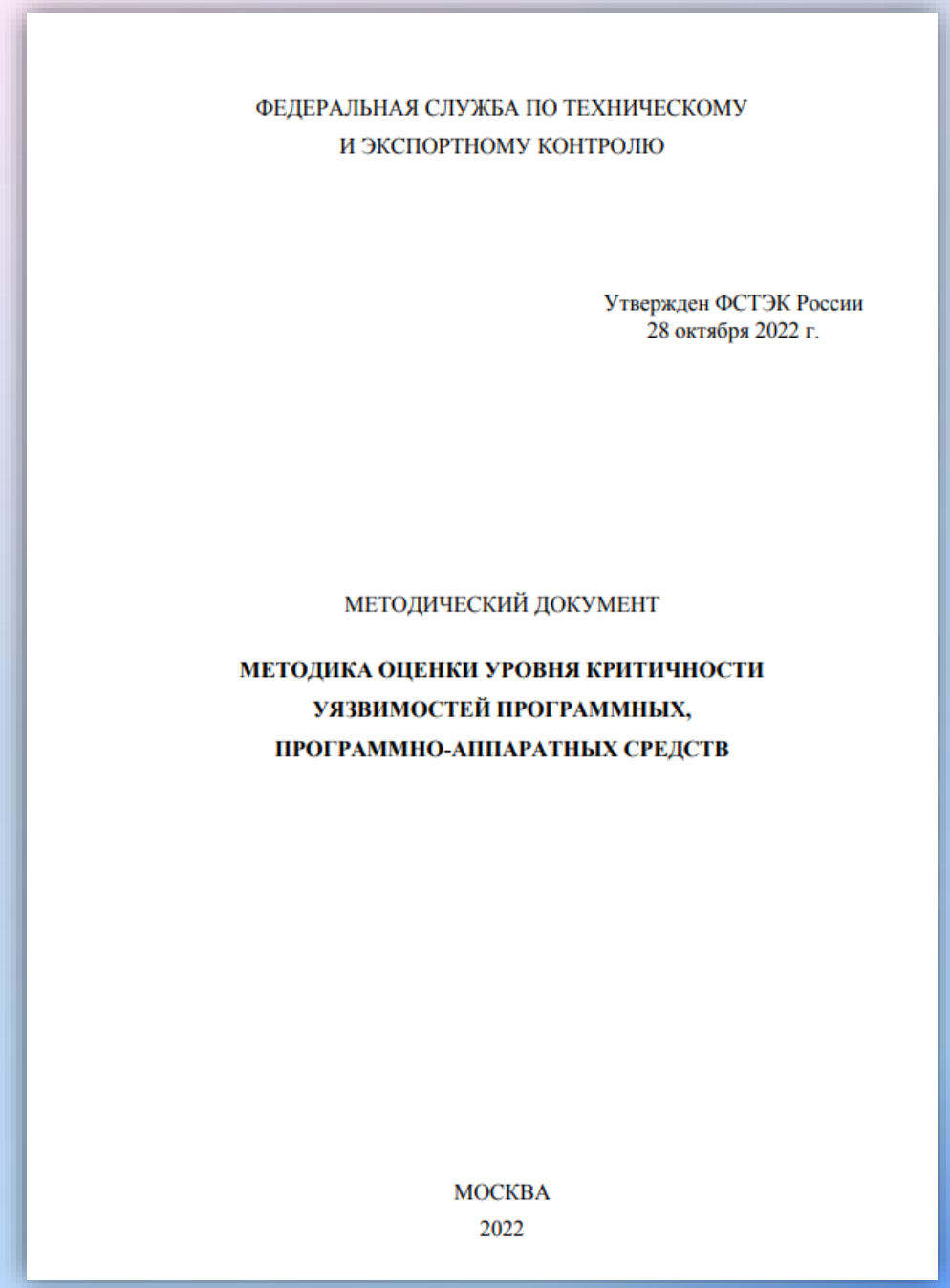
программные средства, обеспечивающие управление доступом субъектов доступа к объектам доступа баз данных, предназначенных для хранения информации, подлежащей защите в информационной (автоматизированной) системе

Функции безопасности:

- управление доступом
- идентификация и аутентификация пользователей
- контроль целостности
- регистрация событий безопасности
- резервное копирование и восстановление
- обеспечение доступности
- очистка памяти
- ограничение программной среды

✓ Разработка требований → ✓ Обсуждение с экспертами → Оценка регулирующего воздействия → Регистрация в Минюсте России → Вступление в силу

МЕТОДИКА ОЦЕНКИ УРОВНЯ КРИТИЧНОСТИ УЯЗВИМОСТЕЙ



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

МОСКВА
2022

Размещена на сайте официальном сайте ФСТЭК России (fstec.ru) и сайте Банка данных угроз безопасности информации (bdu.fstec.ru)

Определяет порядок оценки уровня критичности уязвимостей программных, программно-аппаратных средств

Определяет необходимость принятия мер защиты информации, направленных на устранение уязвимостей

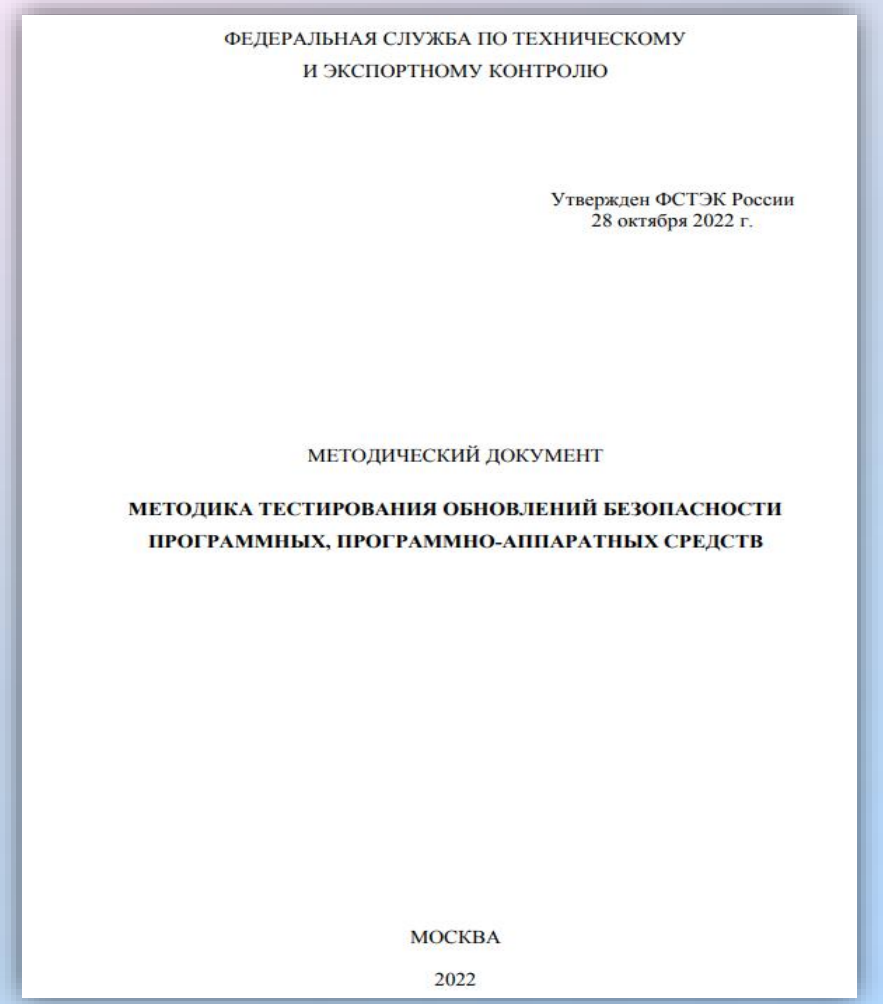
Расчет уровня критичности уязвимости программных, программно-аппаратных средств в информационной системе V осуществляется по следующей формуле:

$$V = I_{cvss} \times I_{infr},$$

где I_{cvss} – показатель, характеризующий уровень опасности уязвимости;

I_{infr} – показатель, характеризующий влияние уязвимости программных, программно-аппаратных средств на функционирование информационной системы

МЕТОДИКА ТЕСТИРОВАНИЯ ОБНОВЛЕНИЙ БЕЗОПАСНОСТИ



ФЕДЕРАЛЬНАЯ СЛУЖБА ПО ТЕХНИЧЕСКОМУ
И ЭКСПОРТНОМУ КОНТРОЛЮ

Утвержден ФСТЭК России
28 октября 2022 г.

МЕТОДИЧЕСКИЙ ДОКУМЕНТ

МЕТОДИКА ТЕСТИРОВАНИЯ ОБНОВЛЕНИЙ БЕЗОПАСНОСТИ ПРОГРАММНЫХ, ПРОГРАММНО-АППАРАТНЫХ СРЕДСТВ

МОСКВА

2022

Размещена на сайте официальном сайте ФСТЭК России (fstec.ru) и сайте Банка данных угроз безопасности информации (bdu.fstec.ru)

Определяет порядок тестирования обновлений безопасности программных, программно-аппаратных средств

Определяет содержание работ по тестированию обновлений безопасности программных, программно-аппаратных средств

Работы по тестированию обновлений безопасности:

- Сверка идентичности обновлений безопасности (Т001)
- Проверка подлинности обновлений безопасности (Т002)
- Антивирусный контроль обновлений безопасности (Т003)
- Поиск опасных конструкций в обновлениях безопасности (Т004)
- Мониторинг активности обновлений безопасности в среде тестирования (Т005)
- Ручной анализ обновлений безопасности (Т006)

СБЕР

ИНТЕР РАО

ДЕПАРТАМЕНТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ ГОРОДА МОСКВЫ

positive technologies

ИСП РАН

Ростелеком Солар

МЕТОДИКА КОНТРОЛЯ (АНАЛИЗА) ЗАЩИЩЕННОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ

Проект

Методика контроля (анализа) защищенности информационных систем

Определяет порядок проведения работ по контролю (анализу) защищенности информационных систем:

а) **определение целей проведения** контроля (анализа) защищенности;

б) **определение области проведения контроля** (анализа) защищенности в информационной системе;

в) **выполнение работ** по контролю (анализу) защищенности;

г) **оформление результатов** контроля (анализа) защищенности.

Работы по контролю (анализу) защищенности

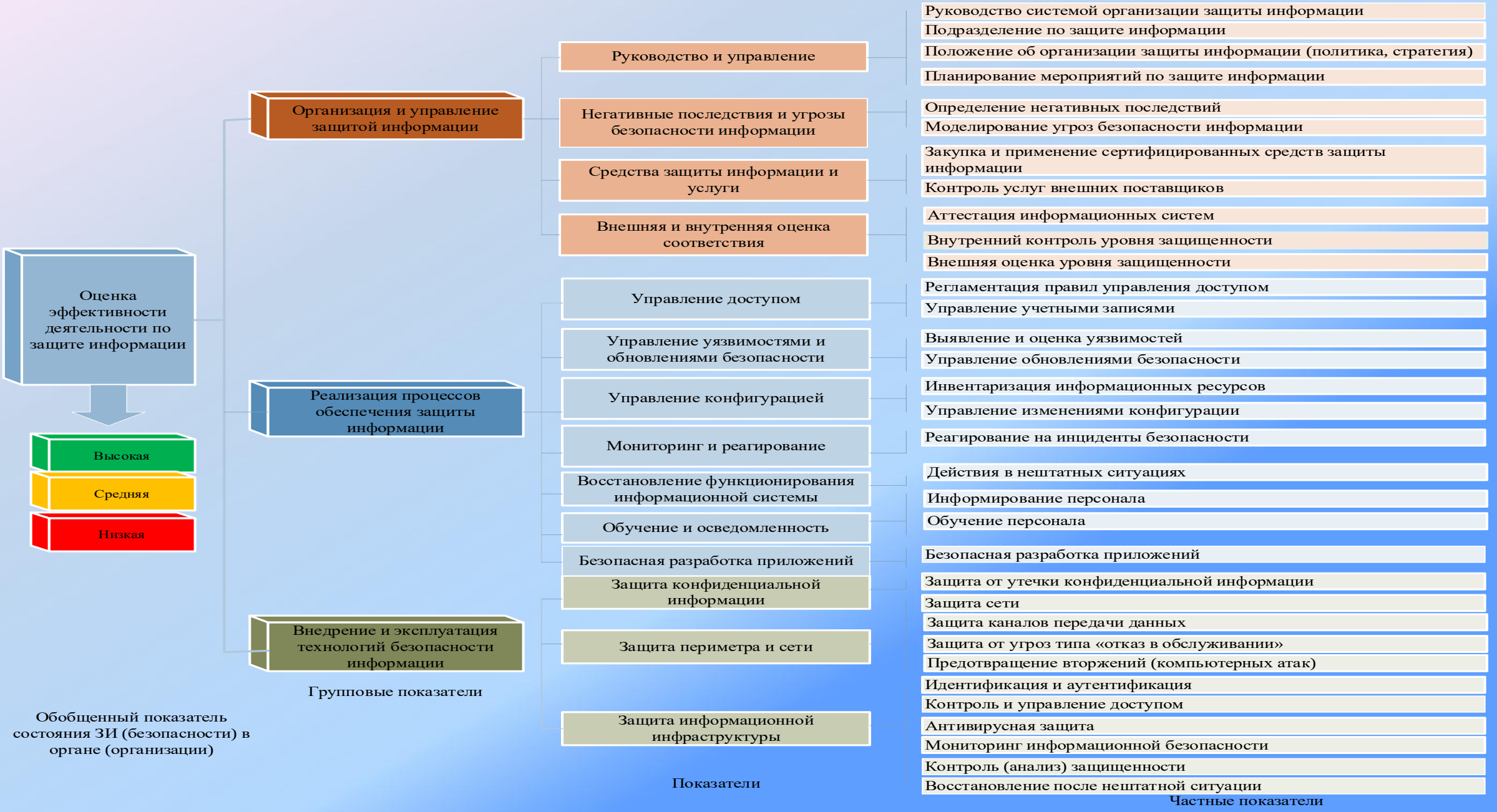
Сбор информации об информационной системе

Анализ уязвимостей информационной системы, включая анализ уязвимостей инфраструктуры, периметра, приложений, беспроводных сетей

Тестирование информационной системы, включая тестирование периметра, внутренней инфраструктуры, беспроводных сетей, социотехническое тестирование

✓Разработка требований → ✓Обсуждение с экспертами → Утверждение ФСТЭК России → Вступление в силу

МЕТОДИКА ОЦЕНКИ СОСТОЯНИЯ ЗАЩИТЫ ИНФОРМАЦИИ (ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ) В ОРГАНЕ (ОРГАНИЗАЦИИ)



МЕТОДИКА УПРАВЛЕНИЯ УЯЗВИМОСТЯМИ В ОРГАНЕ (ОРГАНИЗАЦИИ)

Проект

МЕТОДИЧЕСКИЙ ДОКУМЕНТ
Методика управления уязвимостями в органе (организации)

Управление уязвимостями

- **Мониторинг уязвимостей оценка их применимости**
  - Анализ информации об уязвимостях
  - Анализ релевантности уязвимостей к инфраструктуре
  - Принятие решений на получение дополнительной информации
  - Постановка задачи на сканирование объектов
  - Мониторинг средствами инструментального контроля
  - Оценка защищенности
  - Сканирование объектов
- **Оценка уязвимостей**
  - Получение информации об объектах системы, подверженных уязвимости
  - Определение уровня опасности
  - Определение влияния на систему
  - Расчет критичности
- **Оценка методов и приоритетов устранения уязвимостей**
  - Выбор приоритета устранения уязвимостей
  - Определение методов устранения уязвимостей
  - Принятие решения о срочной установке обновлений
  - Создание задания на установку обновлений
  - Принятие решения о срочной реализации организационных мер
  - Создание задания на реализацию организационных мер
- **Устранение уязвимостей**
  - Согласование с руководством подразделения ИТ
  - Тестирование обновления
  - Установка обновления в тестовом сегменте
  - Принятие решения об установке обновления
  - Установка обновления
  - Применение организационных мер
- **Контроль устранения уязвимостей**
  - Принятие решения о способе контроля
  - Проверка объектов на наличие уязвимостей
  - Оценка защищенности
  - Выявление отклонений и неисполнений
  - Разработка предложений по улучшению процесса управления уязвимостями

НАЦИОНАЛЬНЫЕ СТАНДАРТЫ В ОБЛАСТИ ЗАЩИТЫ ИНФОРМАЦИИ

Утверждены в 2022 году:

- ГОСТ Р 59548-2022 «Защита информации. Регистрация событий безопасности. Требования к регистрируемой информации»
- ГОСТ Р 70262.1-2022 «Защита информации. Идентификация и аутентификация. Уровни доверия идентификации»
- ГОСТ Р 59709-2022 «Защита информации. Управление компьютерными инцидентами. Термины и определения»
- ГОСТ Р 59710-2022 «Защита информации. Управление компьютерными инцидентами. Общие положения»
- ГОСТ Р 59711-2022 «Защита информации. Управление компьютерными инцидентами. Организация деятельности по управлению компьютерными инцидентами»
- ГОСТ Р 59712-2022 «Защита информации. Управление компьютерными инцидентами. Руководство по реагированию на компьютерные инциденты»

Планируются к утверждению в 2023 году:

- Проект национального стандарта ГОСТ Р «Защита информации. Разработка безопасного программного обеспечения. Руководство по оценке безопасности разработки программного обеспечения»
- Проект национального стандарта ГОСТ Р «Защита информации. Разработка безопасного программного обеспечения. Руководство по проведению статического анализа программного обеспечения»
- Проект национального стандарта ГОСТ Р «Защита информации. Разработка безопасного программного обеспечения. Руководство по проведению динамического анализа программного обеспечения»
- Проект национального стандарта ГОСТ Р «Защита информации. Разработка безопасного программного обеспечения. Доверенный компилятор языков Си/Си++. Общие требования»
- Проект национального стандарта ГОСТ Р «Информационная технология. Методология разработки доверенных систем. Конструктивная информационная безопасность. Общие положения»
- Проект национального стандарта ГОСТ Р «Информационная технология. Методология разработки доверенных систем. Конструктивная информационная безопасность. Шаблоны проектирования»
- Проект национального стандарта ГОСТ Р «Информационная технология. Методология разработки доверенных систем. Конструктивная информационная безопасность. Методология разработки»
- Проект национального стандарта ГОСТ Р «Защита информации. Разработка безопасного программного обеспечения. Управление безопасностью программного обеспечения при использовании заимствованных и привлекаемых компонентов»

Основные направления системы защиты информации

Заместитель директора
Федеральной службы по техническому
и экспортному контролю

ЛЮТИКОВ Виталий Сергеевич