Основные направления совершенствования технической защиты информации

Первый заместитель директора
Федеральной службы по техническому
и экспортному контролю

ЛЮТИКОВ Виталий Сергеевич

Совершенствования требований по безопасности информации

Федеральным законом от **8 августа 2024 г. № 216-ФЗ** внесены изменения **статью 14 и часть 5 статьи 16** Федерального закона от **27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»:**

Не допускается передача информации из государственных информационных систем в иные информационные системы, не соответствующие требованиям о защите информации, установленным статьей 16 настоящего Федерального закона

Устанавливается необходимость реализации требований о защите информации в государственных информационных системах, а также в иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений

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

Проект

Проектом Требований устанавливаются:

- требования к организации деятельности по защите информации и управлению данной деятельностью;
- требования к проведению мероприятий и принятию мер по защите информации.

Управление деятельностью по защите информации должно включать:

- разработку 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.

Вступают в силу с 1 марта 2026 г., за исключением пункта 54 Требований, который вступает в силу с 1 сентября 2027 г.

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

Внесение изменений в Кодекс Российской Федерации об административных правонарушениях

Статья 13.12 КоАП РФ	Действующая редакция	Новая 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.**

Предлагается увеличить 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.**

Совершенствование требований к средствам защиты информации

Требования по безопасности информации к средствам обнаружения и реагирования уровня узла (EDR)

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

Требования по безопасности информации к межсетевым экранам (новая редакция)

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

Требования по безопасности информации к средствам контроля за действиями привилегированных учетных записей

Результаты оценки качества проведения работ по аттестации объектов информатизации

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

Результаты рассмотрения аттестационных материалов за 2024 год	
Количество объектов информатизации	11110
Рассмотрено материалов	более 2600
Возвращено на доработку	более 550
Приостановлено аттестатов	2

Порядок организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации, содержащий сведения, составляющие государственную тайну утвержден приказом ФСТЭК России от 28 сентября 2020 г. № 110

Результаты рассмотрения аттестационных материалов за 2024 год	
Количество объектов информатизации	12177
Рассмотрено материалов	более 2700
Возвращено на доработку	более 550
Приостановлено лицензий	5

Типовые недостатки по рассмотрению аттестационных материалов на объекты информатизации

- Не проводятся мероприятия по анализу уязвимостей
- Не проводятся мероприятия по функциональному тестированию
- Не проводятся мероприятия по тестированию системы в обход ее системы защиты информации
- Отсутствие результатов оценки защищенности информации в режиме обработки и воспроизведения акустических речевых сигналов
- Отсутствие результатов испытаний по каналам акустоэлектромагнитных преобразований, высокочастотного облучения, навязывания и прокачки
- Применение несертифицированных в системе сертификации ФСТЭК России средств защиты информации (Интернет-АРМов, IP-телефонов)
- Проведение оценки виброзоны с нарушением положений утвержденной Методики

Оценка состояния технической защиты информации и обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ

Утвержден
ФСТЭК России
2 мая 2024 г.

МЕТОДИЧЕСКИЙ ДОКУМЕНТ

Методика
оценки показателя состояния защиты информации и обеспечения безопасности объектов критической информационной инфраструктуры Российской Федерации

2024

Типовые недостатки

- Не реализована многофакторная аутентификация учетных записей привилегированных пользователей
- Наличие неустраненных критических уязвимостей на периметре и внутри информационной инфраструктуры
- Не утвержден документ, определяющий порядок реагирования на компьютерные инциденты
- Не реализован централизованный сбор событий безопасности
- Полномочия ответственного лица по обеспечению информационной безопасности не возложены на заместителя руководителя органа (организации)

Проведена оценка 170 организаций

Критический – 47 %

Низкий – 40 %

Минимальный базовый – 13 %

Повышение защищенности информационной инфраструктуры Российской Федерации

Постановление Правительства Российской Федерации от 13 мая 2022 г. № 860 «О проведении эксперимента по повышению уровня защищенности государственных информационных систем федеральных органов исполнительной власти и подведомственных им учреждений»

Минцифры России с участием ФСБ России и ФСТЭК России

Проведена оценка защищенности 100 государственных информационных систем

Выявлено более 1250 недостатков (уязвимостей)

- 37 критический уровень
- 472 высокий уровень
- 322 средний уровень
- 421 низкий уровень

Большинство недостатков (уязвимостей) связано с прикладным ППО ГИС

Перечни мер по устранению выявленных недостатков в ГИС согласованы с ФСТЭК России

Совершенствование методических документов по аттестации на соответствие требованиям о защите информации

Методика испытаний систем защиты информации информационных систем путем осуществления тестирования ее функций безопасности (функционального тестирования)

Проект

Методика анализа уязвимостей в информационных системах

Проект

Методика испытаний систем защиты информации информационных систем путем тестирования на проникновение

Проект

Центр исследования безопасности системного программного обеспечения

Технологический центр тестирования ядра Linux

Технологический центр исследования безопасности критичных компонентов

Центр исследования безопасности системного программного обеспечения

В основную ветку ядра Linux принято более 475 патчей

24 поддерживаемых компонента

Более 150 специалистов работают над тестированием ядра Linux и критичных компонентов

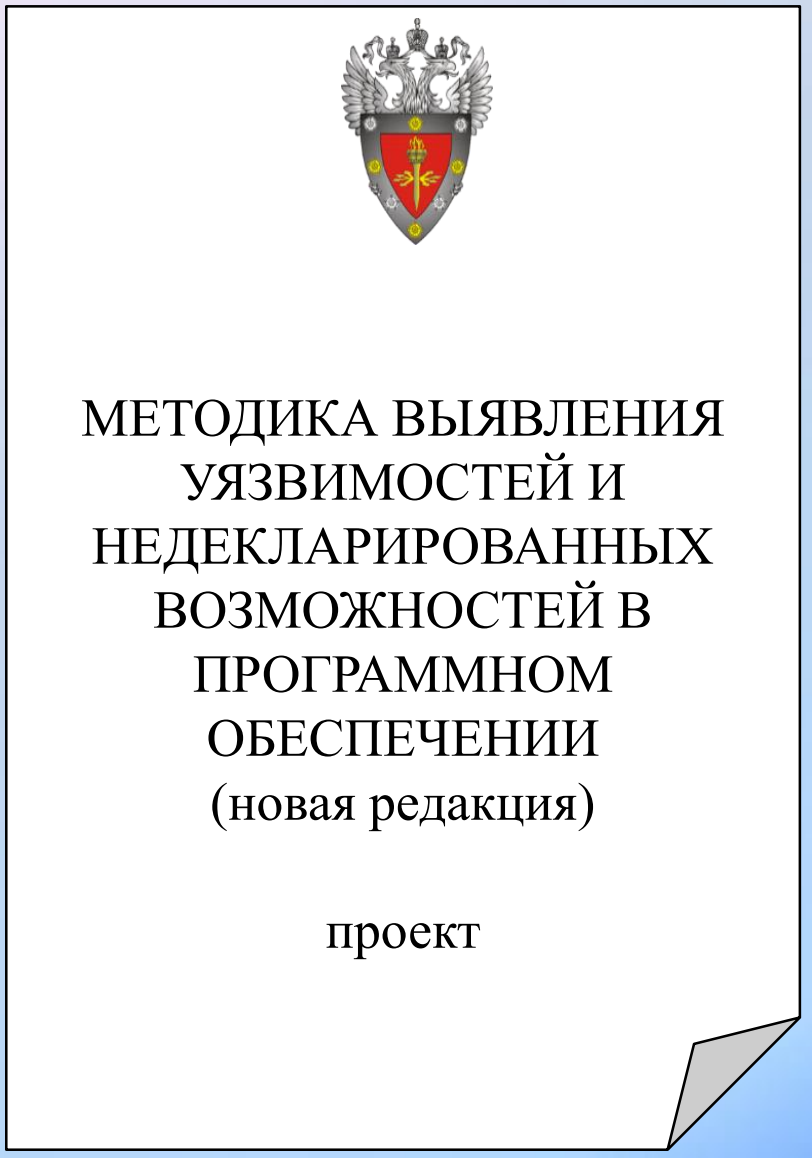
Более 30 000 размеченных предупреждений

Более 15 000 размеченных предупреждений

Выявлено 134 уязвимости в ядре Linux

146 патчей разработано и принято

Методика выявления уязвимостей и недекларированных возможностей в программном обеспечении



При проведении исследований учитываются результаты реализации у разработчиков процессов разработки безопасного программного обеспечения в соответствии ГОСТ Р 56939

Определен порядок использования результатов работы Центра исследований безопасности системного программного обеспечения для сертификации объекта оценки

Введено требование о предоставлении исходного кода объекта оценки с 6 уровня контроля

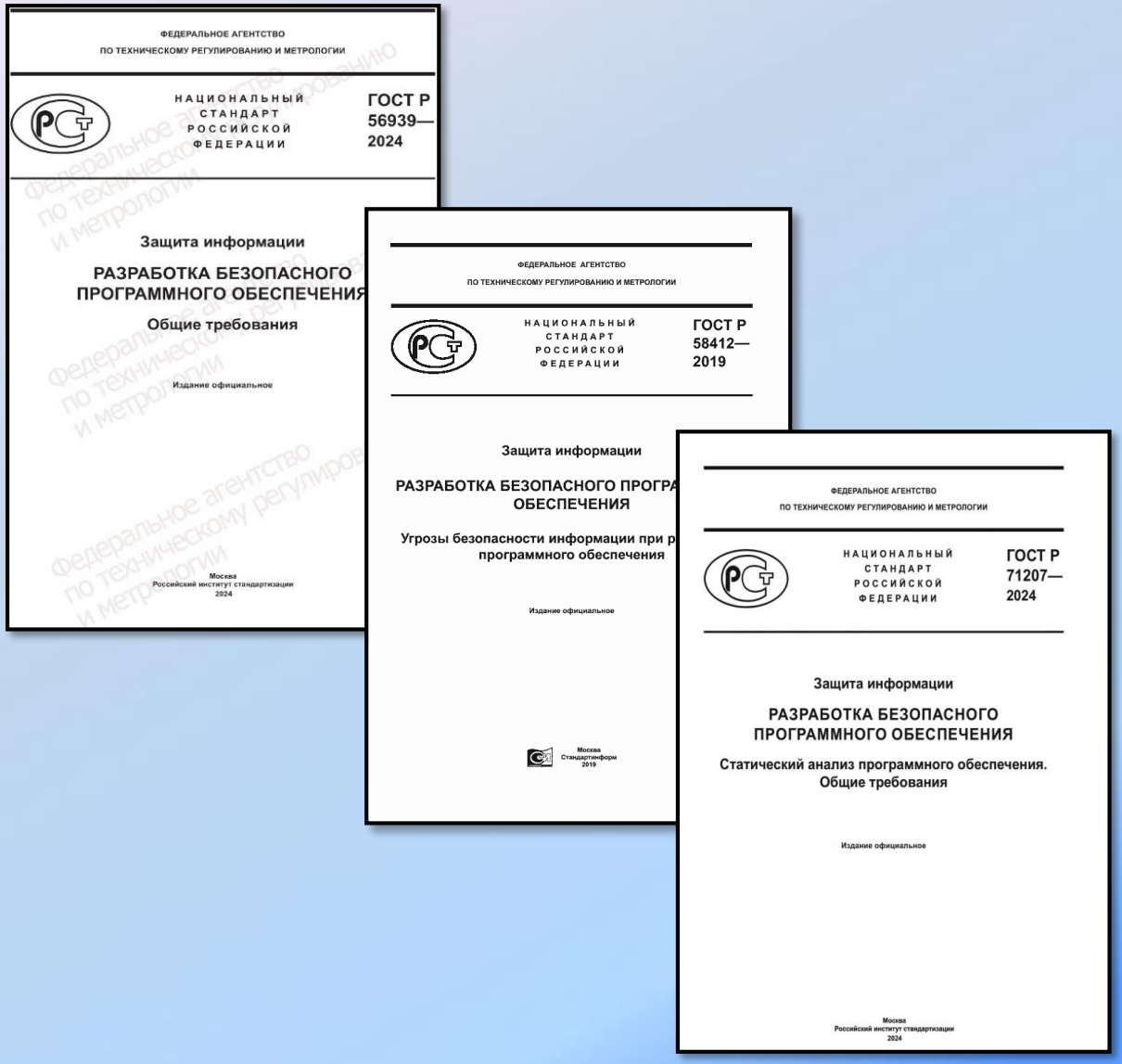
Уточнена методология определения поверхности атаки объекта оценки

Введено требования о представлении информации о сторонних программных компонентах объекта оценки и проведении в их отношении композиционного анализа

Уточнены требования к проведению анализа архитектуры, статического, динамического анализа и оформлению результатов

Национальные стандарты в области разработки безопасного программного обеспечения

Технический комитет 362 «Защита информации»



ГОСТ Р «Защита информации. Разработка безопасного программного обеспечения. Динамический анализ программного обеспечения»
ГОСТ Р «Защита информации. Разработка безопасного программного обеспечения. Композиционный анализ программного обеспечения. Общие требования»
ГОСТ Р «Защита информации. Разработка безопасного программного обеспечения. Методика оценки уровня внедрения процессов разработки безопасного программного обеспечения»
ГОСТ Р «Защита информации. Разработка безопасного программного обеспечения. Термины и определения»
ГОСТ Р «Защита информации. Системы с конструктивной информационной безопасностью. Методология разработки»
ГОСТ Р «Защита информации. Доверенная среда исполнения. Общие требования»

Порядок сертификации 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»

Критерии оценки разработки безопасного программного обеспечения средств защиты информации

Проверка наличия у изготовителя средств разработки программного обеспечения и средств проведения статического и динамического анализа программного обеспечения

Проверка выполнения требований к обучению специалистов изготовителя

Оценка соответствия руководства требованиям по безопасной разработке

Проверка реализации изготовителем процедур поддержки безопасности программного обеспечения

Проверка реализации изготовителем процессов безопасной разработки, приведенных в руководстве и в документации

Количество заявок на сертификацию: 10

Количество решений: 7

Количество сертификатов: 3

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

Аттестация экспертов проводится

В форме тестирования (100 вопросов по каждой области аккредитации)

В форме решения практических задач (2 задачи по каждой области аккредитации)

Время тестирования по каждой области – **90 минут**

Время решения практических задач по каждой области – **120 минут**

- Статический анализ
- Ресерс-инжиниринг
- Динамический анализ
- Веб-пентест

Количество заявок на аттестацию 104 экспертов

Принято решение о допуске 71 эксперта

Запланирована аттестация 47 экспертов

Аттестовано 14 экспертов

Не прошли аттестацию 10 экспертов

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

Проведение испытаний средств статического анализа исходного кода

Национальный стандарт Российской Федерации ГОСТ Р 71207-2024 «Защита информации. Разработка безопасного программного обеспечения. Статический анализ программного обеспечения. Общие требования»

1 этап
- Формирование перечня участников
- Формирование жюри
- Формирование критериев оценки
- Формирование площадки испытаний

2 этап
- Согласование жюри комплектов тестов
- Запуск этапа «домашнее задание»
- Подведение предварительных итогов «домашнего задания»

3 этап
- Подготовка площадки испытаний
- Запуск, проведение испытаний, разметка полученных результатов

4 этап
- Оценка жюри результатов испытаний
- Опубликование результатов испытаний

Отечественные разработчики ПО и экспертные организации, принявшие участие в испытании средств статического анализа

ИСП РАН, Эшелон комплексная безопасность, positive technologies, SBER TECH, KASPERSKY lab, Ростелеком Солар, Base ALT, Фобос-НТ, РусБИТех-Астра, PVS-Studio

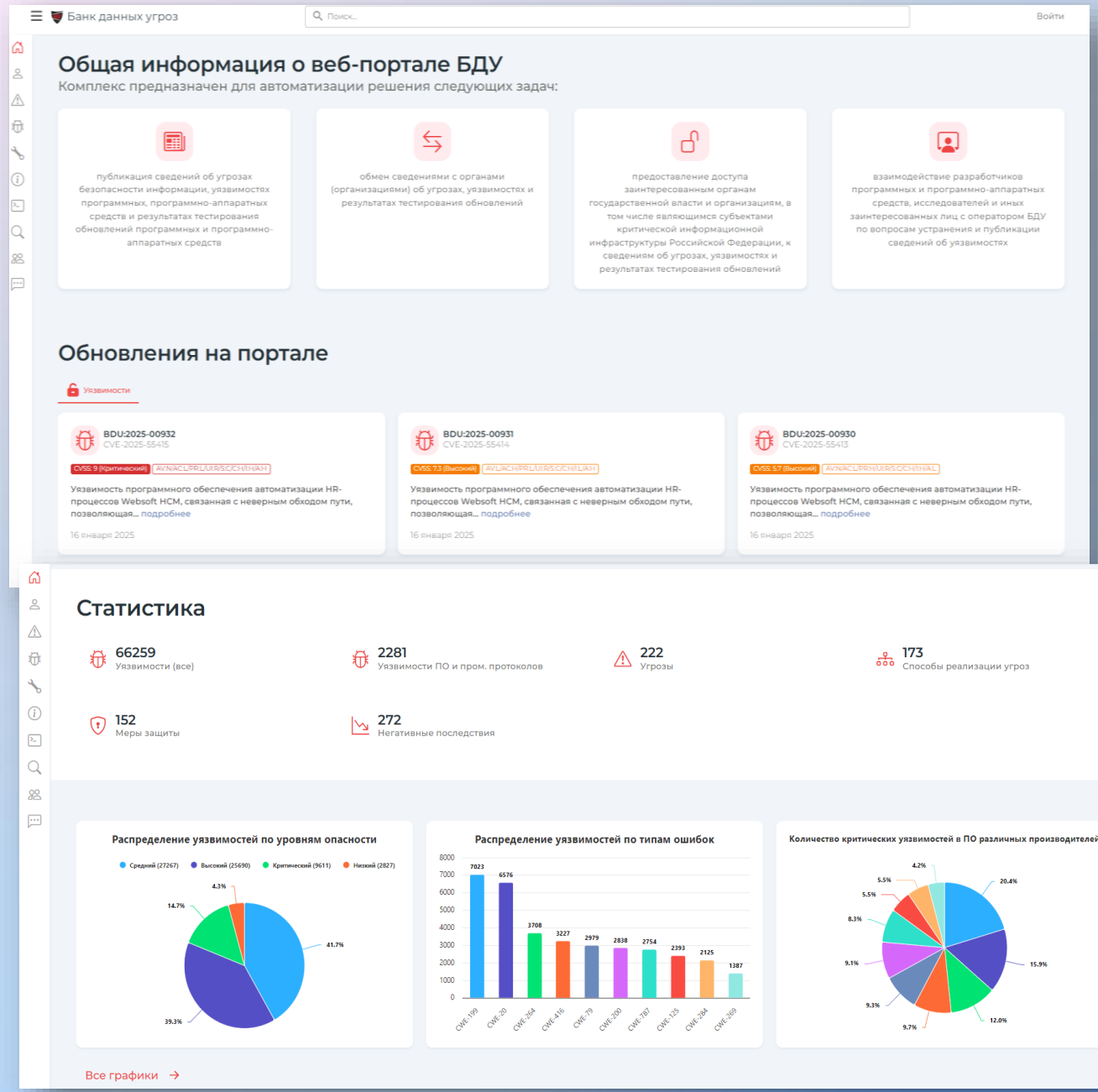
При информационной поддержки ООО «Медиа Группа «Авангард»

Авангард медиа группа

Проведение тестирование на базе МГТУ им. Н.Э.Баумана

МГТУ 1830

Развитие банка данных угроз безопасности информации



Основные обновления:

- Предоставление авторизованного доступа разработчикам СЗИ и ПО, а также исследователям УБИ
- Получение информации об уязвимостях ПО посредством API-взаимодействия
- Возможность публикации сведений об уязвимостях ПО экспертным сообществом
- Непрерывная публикация сведений об уязвимостях ПО
- Возможность обмена информацией в реальном времени посредством чата

II квартал 2026 г.

Основные направления совершенствования технической защиты информации

Первый заместитель директора
Федеральной службы по техническому
и экспортному контролю

ЛЮТИКОВ Виталий Сергеевич