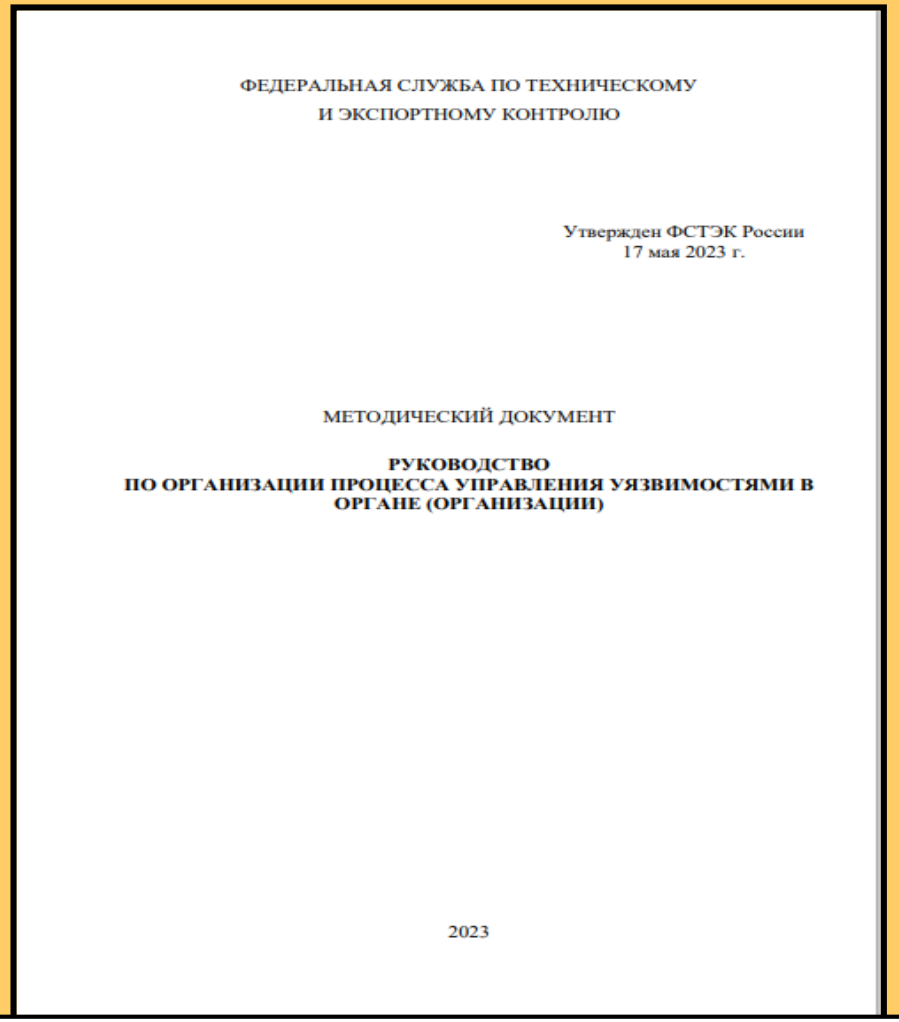
Выступление
начальника отдела Управления ФСТЭК России по Приволжскому федеральному округу
Сажина Сергея Владимировича

Организация процесса управления уязвимостями в ВУЗах

Требования по управлению уязвимостями

Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденные приказом ФСТЭК России от 11 февраля 2013 г. № 17	18.7. В ходе контроля за обеспечением уровня защищенности информации, содержащейся в информационной системе, осуществляются анализ и оценка функционирования информационной системы и ее системы защиты информации, включая анализ и устранение уязвимостей и иных недостатков в функционировании системы защиты информации информационной системы
Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденные приказом ФСТЭК России от 18 февраля 2013 г. № 21	АН3.1 Выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей
Требования к обеспечению защиты информации в АСУ производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды, утвержденные приказом ФСТЭК России от 14 марта 2014 г. № 31	16.4. В ходе анализа угроз безопасности информации в автоматизированной системе управления и возможных рисков от их реализации осуществляются периодический анализ уязвимостей автоматизированной системы управления, возникающих в ходе ее эксплуатации
Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации, утвержденные приказом ФСТЭК России от 25 декабря 2017 г. № 239	13.2. В ходе анализа угроз безопасности информации в значимом объекте и возможных последствий их реализации осуществляются анализ уязвимостей значимого объекта, возникающих в ходе его эксплуатации

Руководство по организации процесса управления уязвимостями



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)**

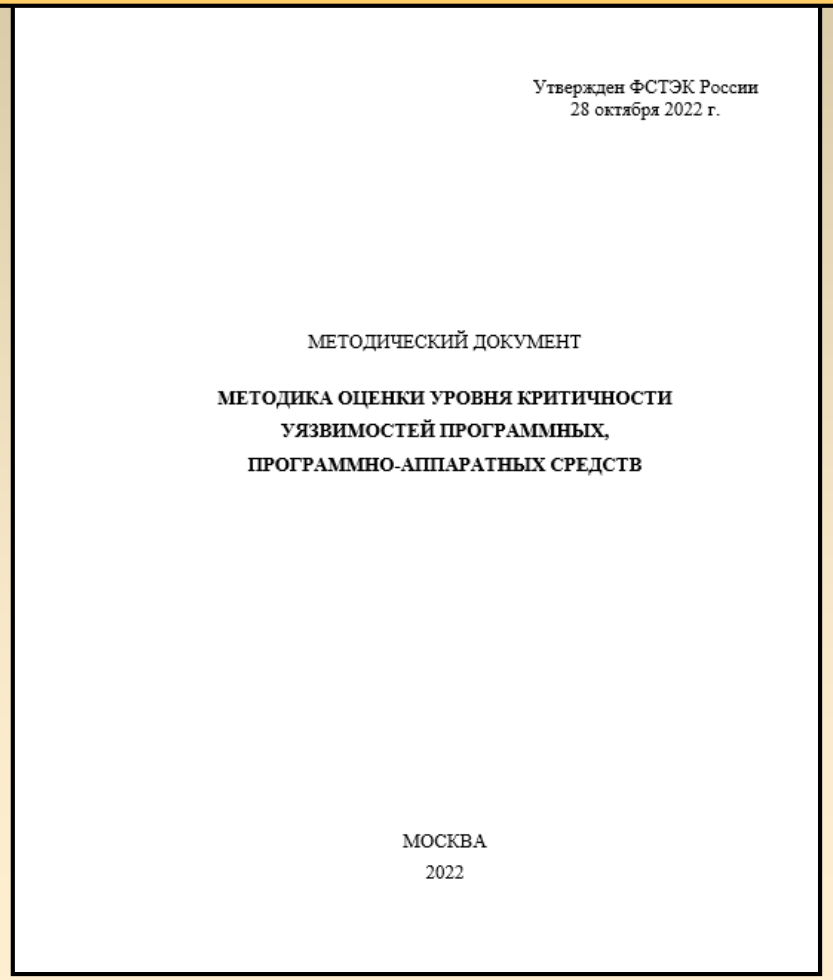
2023

Процесс управления уязвимостями включает пять основных этапов

Задачами Руководства являются создание основы для разработки детальных регламентов и стандартов по управлению уязвимостями с учетом особенностей функционирования органов (организаций) и организация взаимодействия между структурными подразделениями органов (организаций) по вопросам устранения уязвимостей

Обеспечение безопасности значимого объекта в ходе его эксплуатации

28 октября 2022 г. ФСТЭК России утверждены:
Методика оценки уровня критичности уязвимостей программных, программно-аппаратных средств;
Методика тестирования обновлений безопасности программных, программно-аппаратных средств

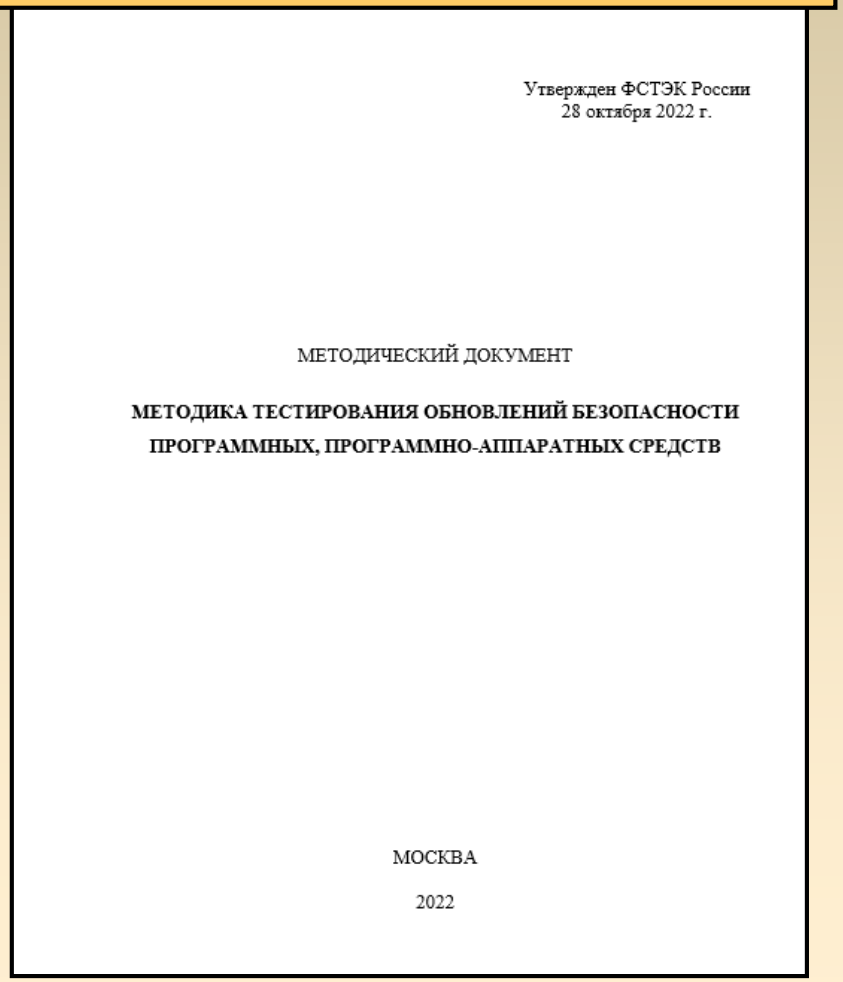


Утвержден ФСТЭК России
28 октября 2022 г.

МЕТОДИЧЕСКИЙ ДОКУМЕНТ

МЕТОДИКА ОЦЕНКИ УРОВНЯ КРИТИЧНОСТИ УЯЗВИМОСТЕЙ ПРОГРАММНЫХ, ПРОГРАММНО-АППАРАТНЫХ СРЕДСТВ

МОСКВА
2022



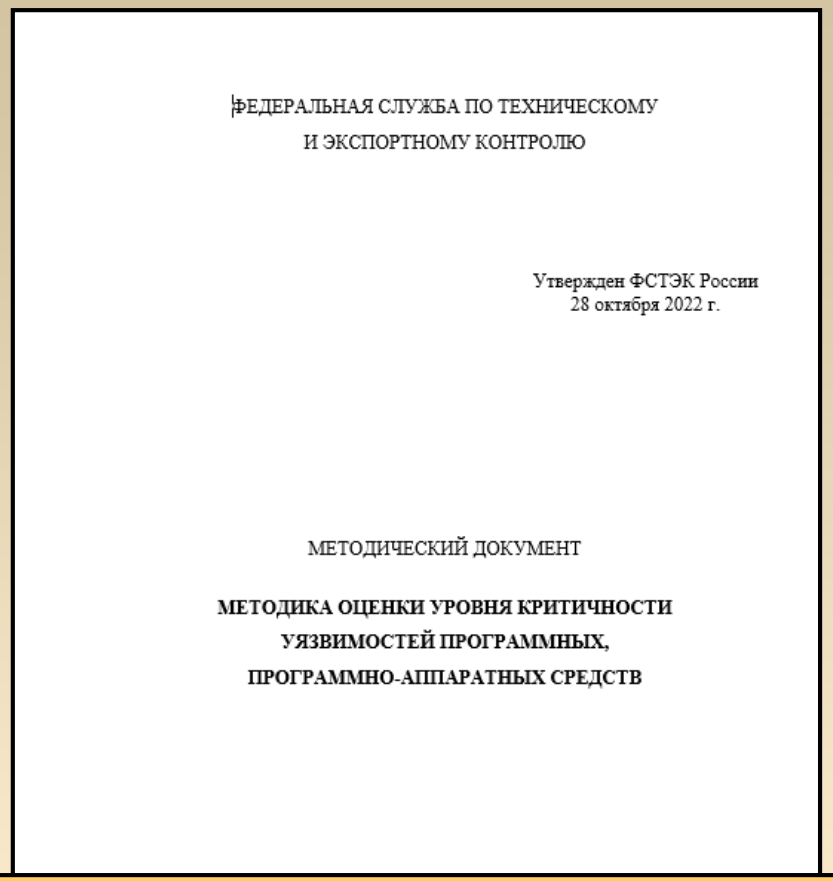
Утвержден ФСТЭК России
28 октября 2022 г.

МЕТОДИЧЕСКИЙ ДОКУМЕНТ

МЕТОДИКА ТЕСТИРОВАНИЯ ОБНОВЛЕНИЙ БЕЗОПАСНОСТИ ПРОГРАММНЫХ, ПРОГРАММНО-АППАРАТНЫХ СРЕДСТВ

МОСКВА
2022

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

В отношении уязвимостей, которым присвоен **критический** уровень опасности, принимаются меры по их устранению в течении часов (до 24 часов)

В отношении уязвимостей, которым присвоен **высокий** уровень опасности, принимаются меры по их устранению в течении часов (до 7 дней)

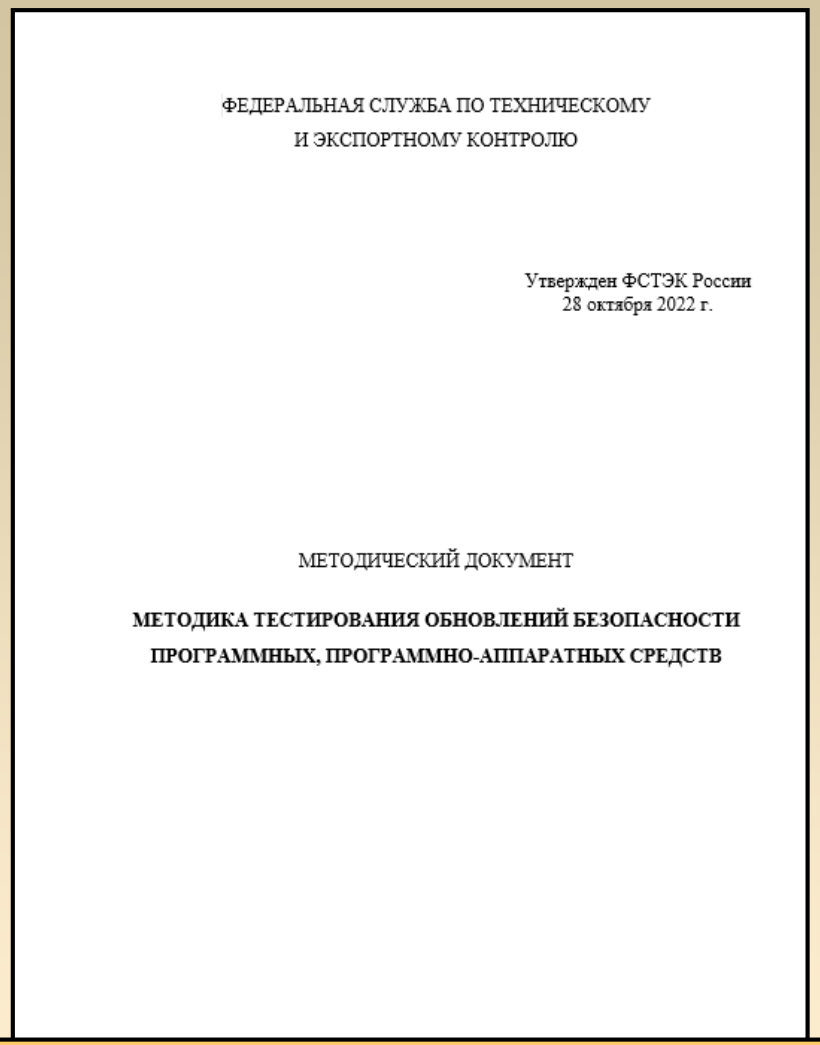
В отношении уязвимостей, которым присвоен **средний** уровень опасности, принимаются меры по их устранению в течении часов (до 4 недель)

В отношении уязвимостей, которым присвоен **низкий** уровень опасности, принимаются меры по их устранению в течении часов (до 4 месяцев)

Уязвимости могут быть устранены путем установки обновлений программного обеспечения, программно-аппаратного средства или принятия компенсирующих организационных и технических мер защиты информации

Устранение уязвимостей в сертифицированных средствах защиты информации обеспечивается в приоритетном порядке и осуществляется в соответствии с эксплуатационной документацией

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

В ходе проведения тестирования обновлений безопасности должны выполняться следующие тесты:

а) сверка идентичности

Сверка идентичности обновлений безопасности, полученных из различных источников путем расчета и сравнения их контрольных сумм

б) проверка подлинности

Проверка подлинности обновлений безопасности путем их сравнения с предоставленными разработчиками обновления средств проверки

в) антивирусный контроль обновлений безопасности

г) поиск опасных конструкций

Поиск конструкций с применением индикаторов компрометации, YARA-правил, контекстный поиск баннеров, лозунгов и другой противоправной информации

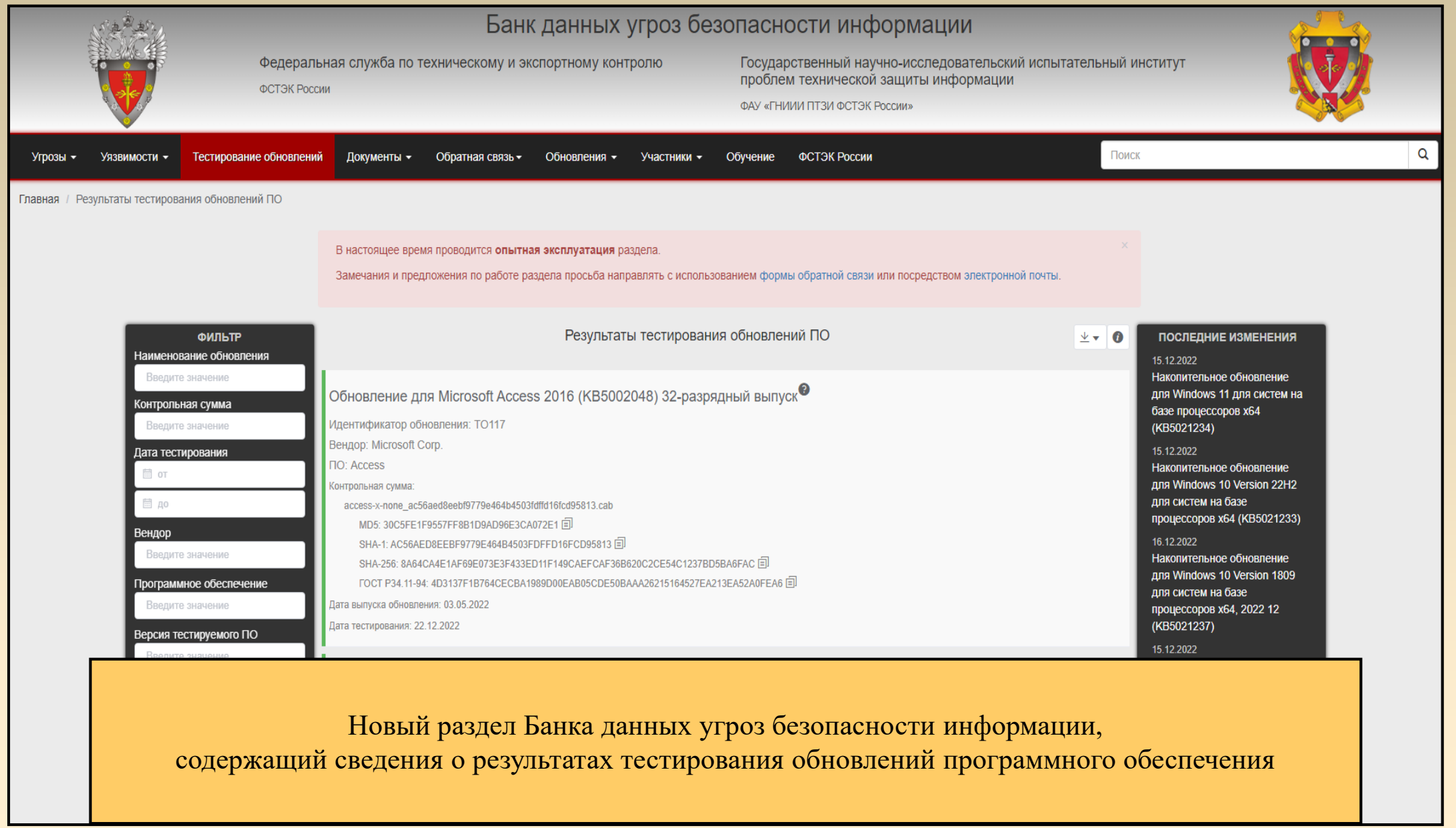
д) мониторинг активности обновлений в среде функционирования

Мониторинг работы обновления со средой функционирования

г) ручной анализ обновлений

Тестирование проводится в следующих средах: исследовательском стенде;
тестовой зоне информационной системы (песочнице);
информационной системе, функционирующей в штатном режиме

Банк данных угроз безопасности информации ФСТЭК России



Новый раздел Банка данных угроз безопасности информации,
содержащий сведения о результатах тестирования обновлений программного обеспечения

Национальные стандарты Российской Федерации

ГОСТ Р 56545-2015 "Защита информации. Уязвимости информационных систем. Правила описания уязвимостей"

ГОСТ Р 56546-2015 "Защита информации. Уязвимости информационных систем. Классификация уязвимостей информационных систем"

ГОСТ Р 59547-2021 "Защита информации. Мониторинг информационной безопасности. Общие положения"

ГОСТ Р 56545-2015 "Защита информации. Уязвимости информационных систем. Правила описания уязвимостей"

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"

Выступление
начальника отдела Управления ФСТЭК России по Приволжскому федеральному округу
Сажина Сергея Владимировича

Организация процесса управления уязвимостями в ВУЗах