



Выступление

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

Организация процесса управления уязвимостями в ВУЗах

Требования по управлению уязвимостями

| | |
|--|---|
| <p>Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденные приказом ФСТЭК России от 11 февраля 2013 г. № 17</p> | <p>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</p> |
| <p>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</p> | <p>АНЗ.1 Выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей</p> |
| <p>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</p> | <p>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</p> |
| <p>Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации, утвержденные приказом ФСТЭК России от 25 декабря 2017 г. № 239</p> | <p>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</p> |

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

е) 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



Федеральная служба по техническому и экспортному контролю
ФСТЭК России

Государственный научно-исследовательский испытательный институт
проблем технической защиты информации
ФАУ «ГНИИИ ПТЗИ ФСТЭК России»



Угрозы ▾ Уязвимости ▾ **Тестирование обновлений** Документы ▾ Обратная связь ▾ Обновления ▾ Участники ▾ Обучение ФСТЭК России

Поиск



Главная / Результаты тестирования обновлений ПО

В настоящее время проводится **опытная эксплуатация** раздела.

Замечания и предложения по работе раздела просьба направлять с использованием [формы обратной связи](#) или посредством [электронной почты](#).

ФИЛЬТР

Наименование обновления

Контрольная сумма

Дата тестирования
от
до

Вендор

Программное обеспечение

Версия тестируемого ПО

Результаты тестирования обновлений ПО



Обновление для Microsoft Access 2016 (KB5002048) 32-разрядный выпуск [?]

Идентификатор обновления: TO117

Вендор: Microsoft Corp.

ПО: Access

Контрольная сумма:

access-x-none_ac56aed8eebf9779e464b4503fdffd16fcd95813.cab

MD5: 30C5FE1F9557FF8B1D9AD96E3CA072E1

SHA-1: AC56AED8EEBF9779E464B4503FDFFD16FCD95813

SHA-256: 8A64CA4E1AF69E073E3F433ED11F149CAEFCAF36B620C2CE54C1237BD5BA6FAC

ГОСТ Р34.11-94: 4D3137F1B764CECBA1989D00EAB05CDE50BAAA26215164527EA213EA52A0FEA6

Дата выпуска обновления: 03.05.2022

Дата тестирования: 22.12.2022

ПОСЛЕДНИЕ ИЗМЕНЕНИЯ

15.12.2022

Накопительное обновление для Windows 11 для систем на базе процессоров x64 (KB5021234)

15.12.2022

Накопительное обновление для Windows 10 Version 22H2 для систем на базе процессоров x64 (KB5021233)

16.12.2022

Накопительное обновление для Windows 10 Version 1809 для систем на базе процессоров x64, 2022 12 (KB5021237)

15.12.2022

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

Национальные стандарты Российской Федерации

| | | | |
|--|---|---|--|
| <p>ФЕДЕРАЛЬНОЕ АГЕНТСТВО ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ</p> | <p>ФЕДЕРАЛЬНОЕ АГЕНТСТВО ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ</p> | <p>ФЕДЕРАЛЬНОЕ АГЕНТСТВО ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ</p> | <p>ФЕДЕРАЛЬНОЕ АГЕНТСТВО ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ</p> |
|  <p>НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ</p> |  <p>НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ</p> |  <p>НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ</p> |  <p>НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ</p> <p>ГОСТ Р 59712— 2022</p> |
| <p>Защита информации УЯЗВИМОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ</p> | <p>Защита информации УПРАВЛЕНИЕ</p> | <p>Защита информации МОНИТОРИНГ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ</p> | <p>Защита информации УПРАВЛЕНИЕ КОМПЬЮТЕРНЫМИ ИНЦИДЕНТАМИ</p> <p>Руководство по реагированию на компьютерные инциденты</p> |

- 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