Совершенствование банка данных угроз безопасности информации

Начальник управления ФАУ «ГНИИИ ПТЗИ ФСТЭК России»

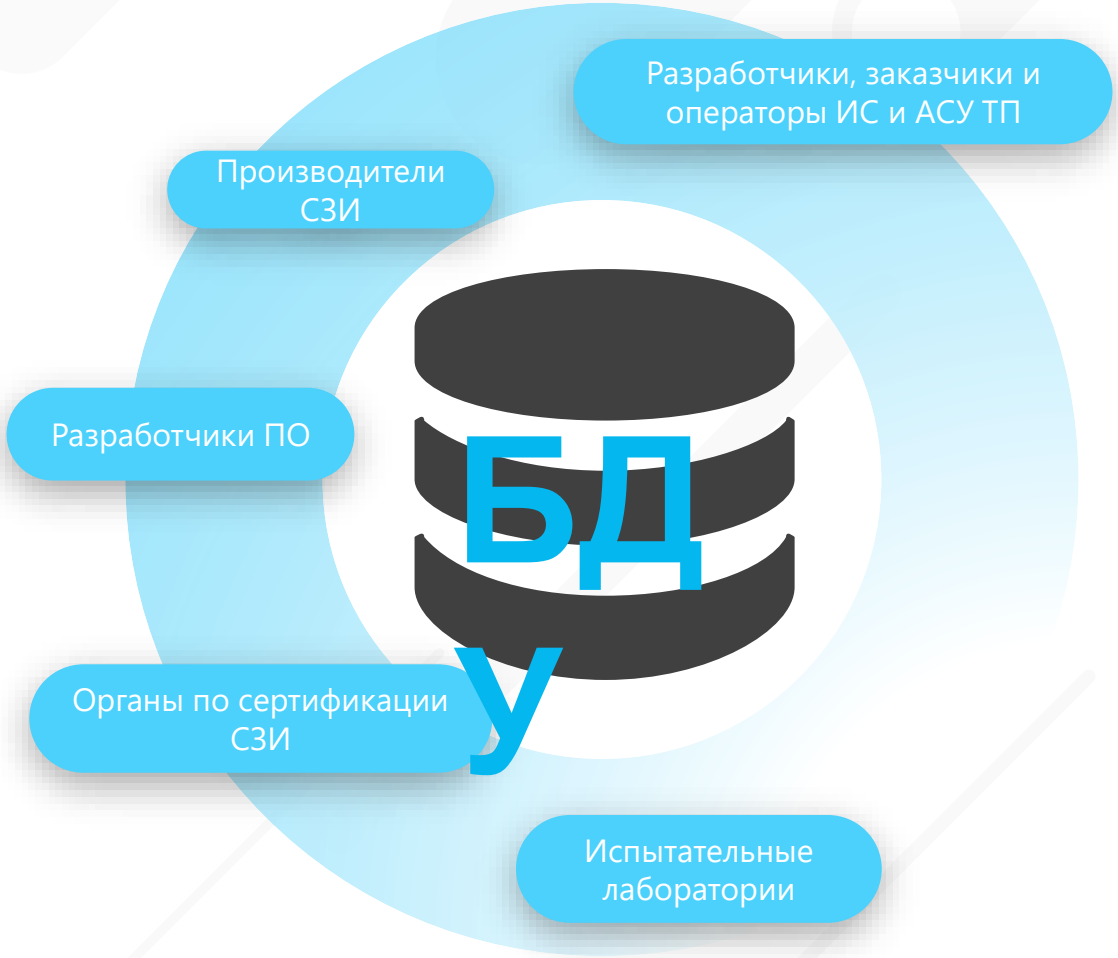
Суховерхов Александр Сергеевич

Банк данных угроз безопасности информации

Единый отечественный информационный ресурс, содержащий сведения об угрозах и уязвимостях отечественных и зарубежных программных и программно-аппаратных средств

- *определение и оценка угроз*
- *выявление, анализ и устранение уязвимостей*
- *производство и поддержание в актуальном состоянии СЗИ*

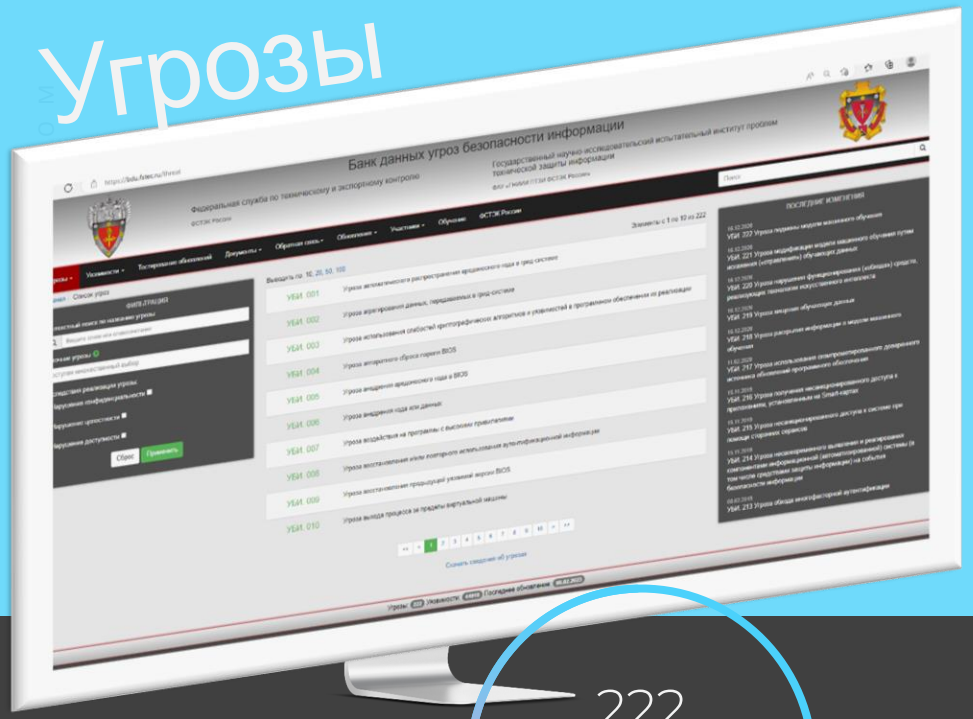
Информационная и методическая поддержка



Банк данных угроз безопасности информации

Введен в эксплуатацию в 2015 году

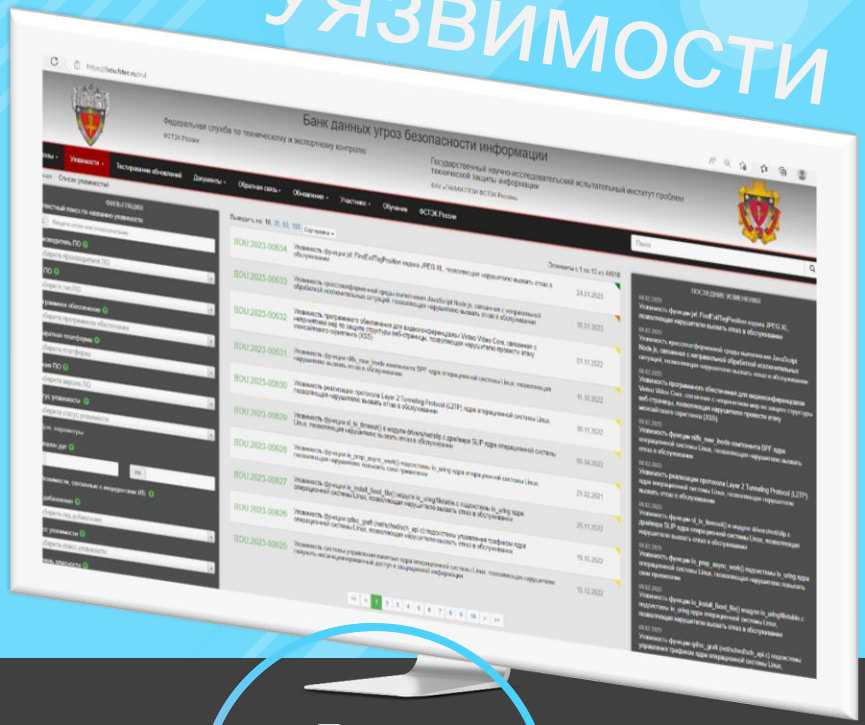
Угрозы



222 записи

БДУ

Уязвимости



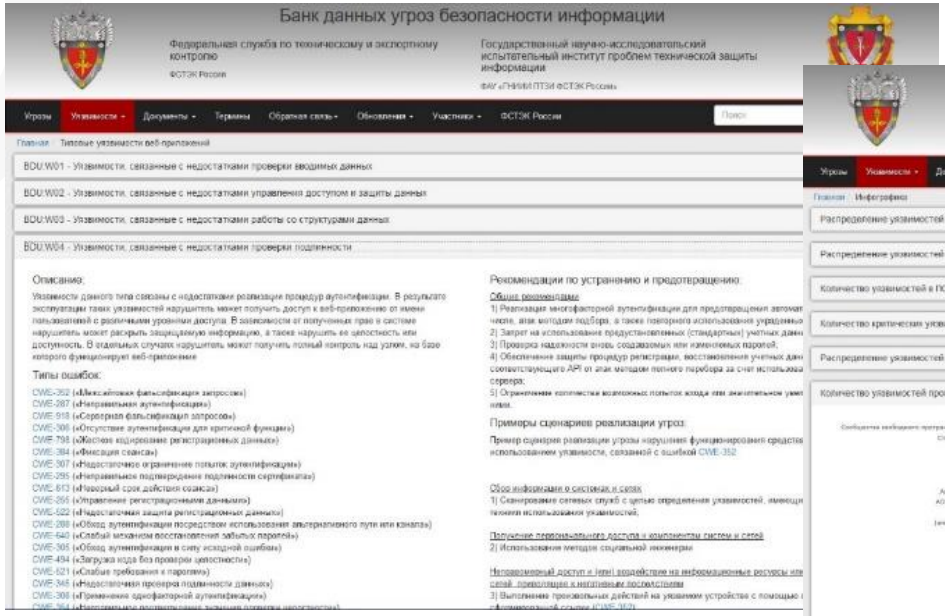
Более 44000 записей

Адрес сайта БДУ:

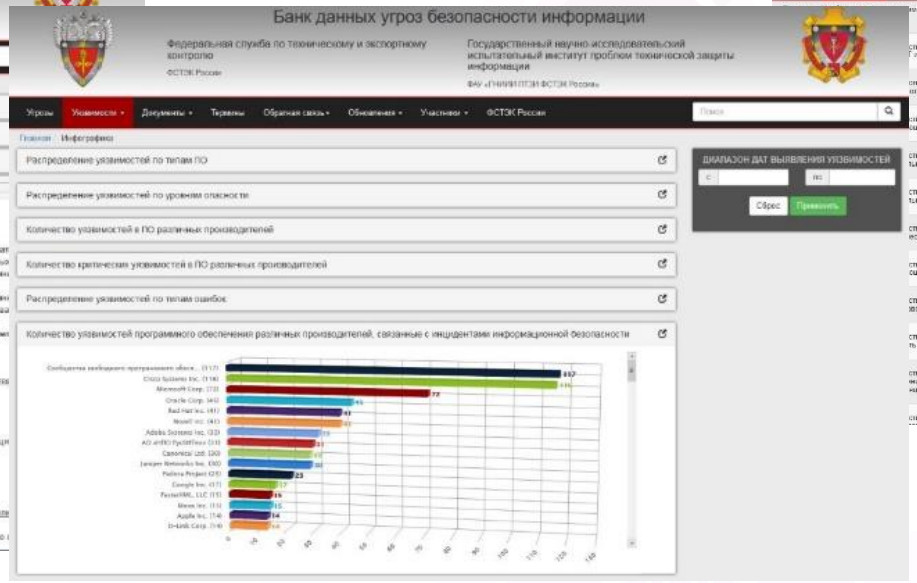
https://bdu.fstec.ru

Банк данных угроз безопасности информации

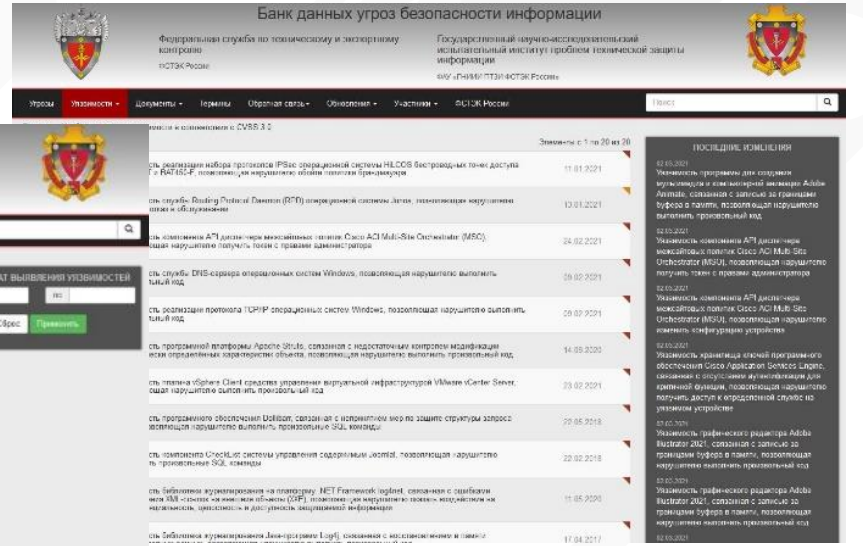
Разделы сайта (2021)



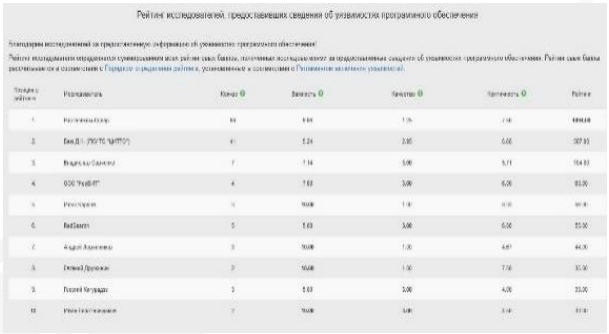
Типовые уязвимости веб-приложений



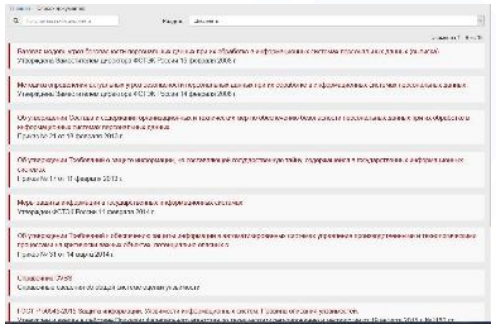
Обновленный раздел «Инфографика»



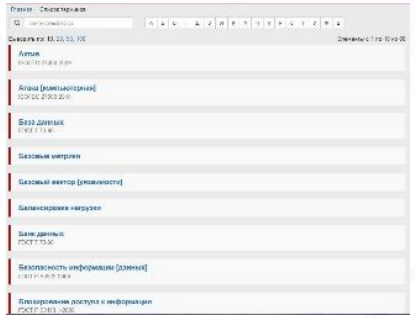
20 наиболее опасных уязвимостей



Рейтинг исследователей

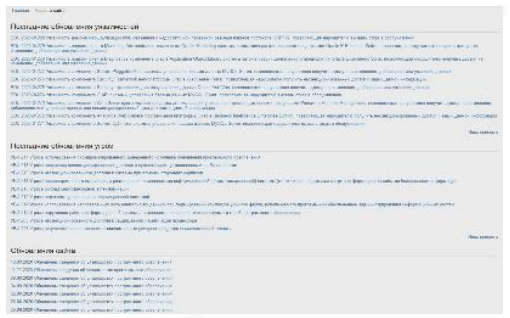


Документы



Термины

Обратная связь

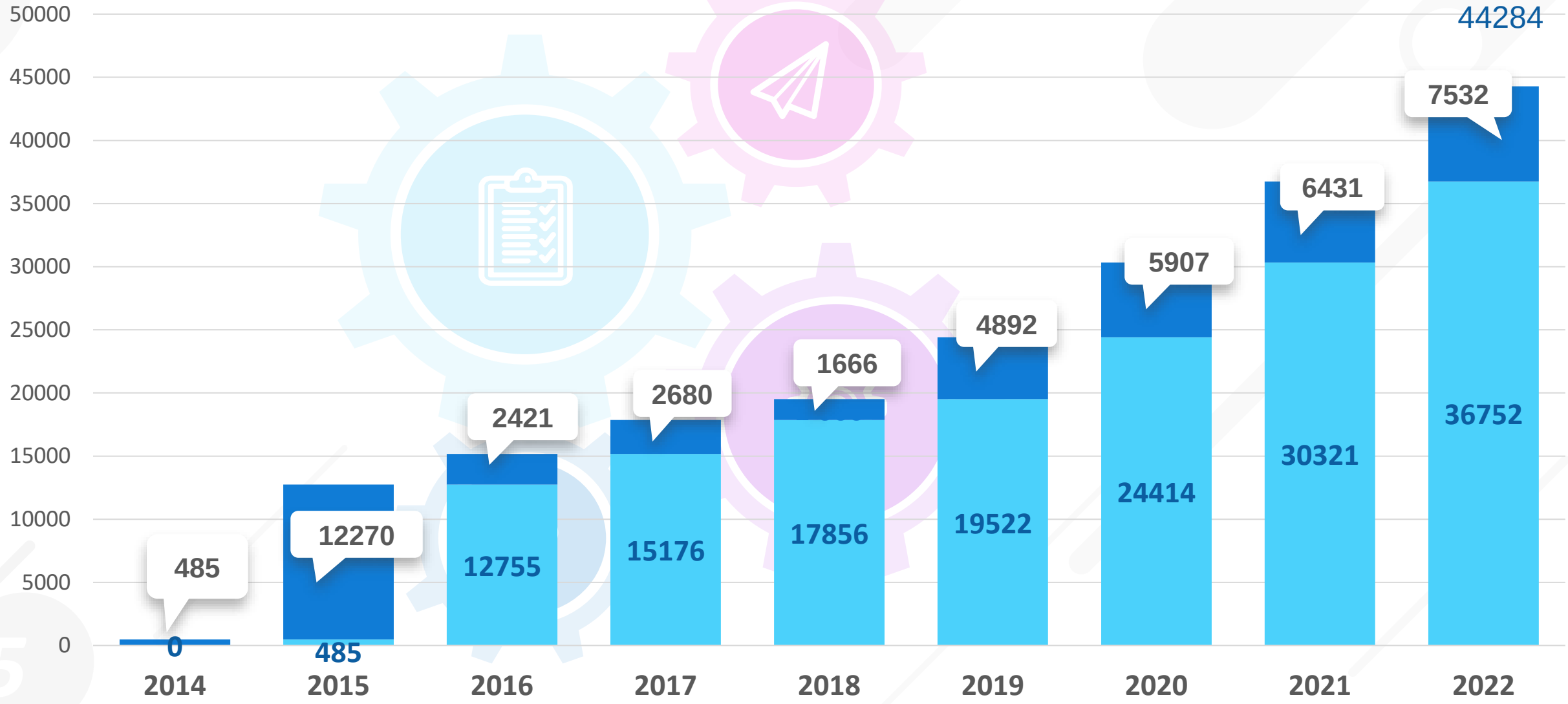


Обновления

Банк данных угроз безопасности информации

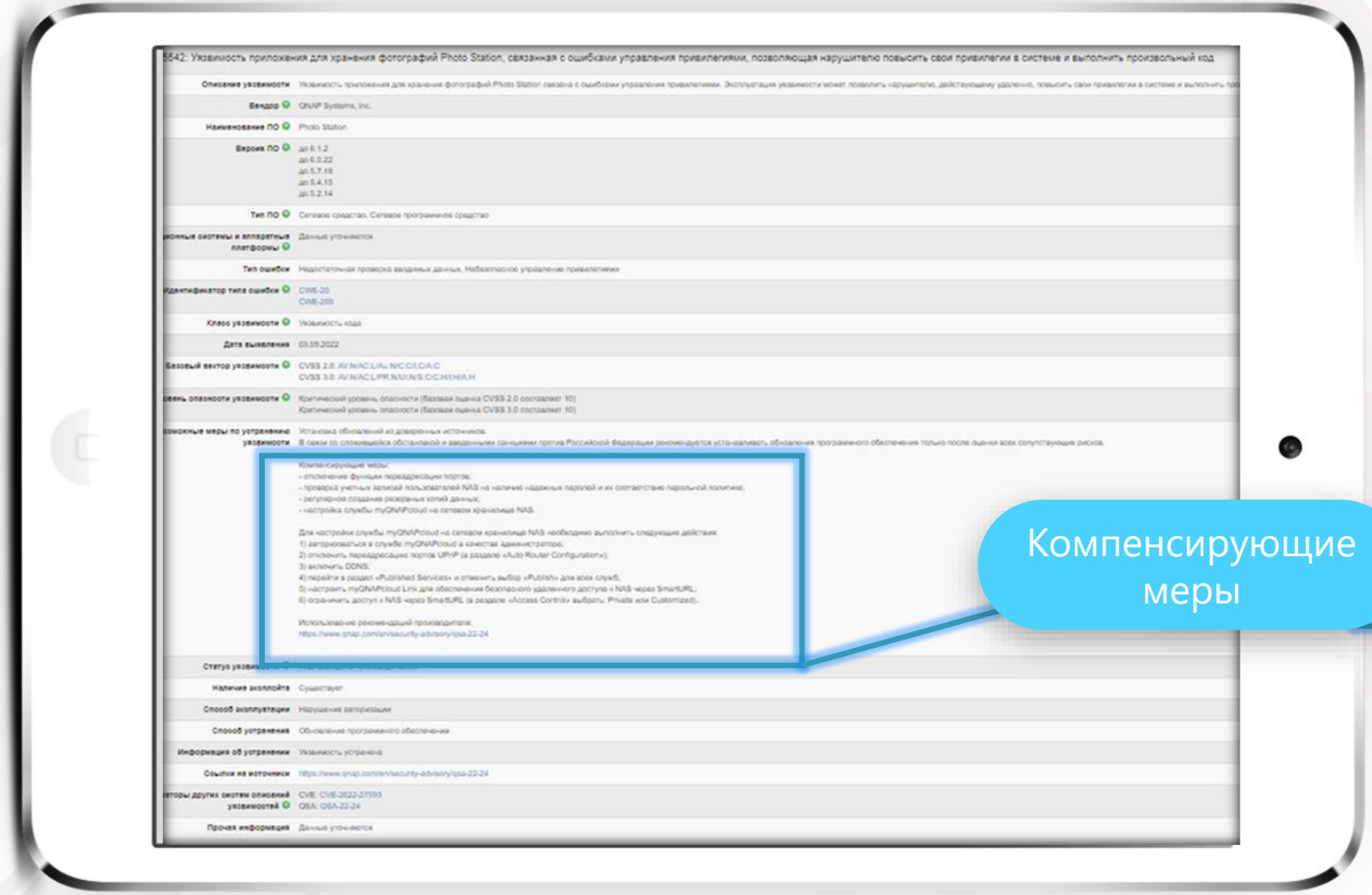
Характеристика накопленных сведений об уязвимостях.

Включение записей об уязвимостях программного обеспечения по годам



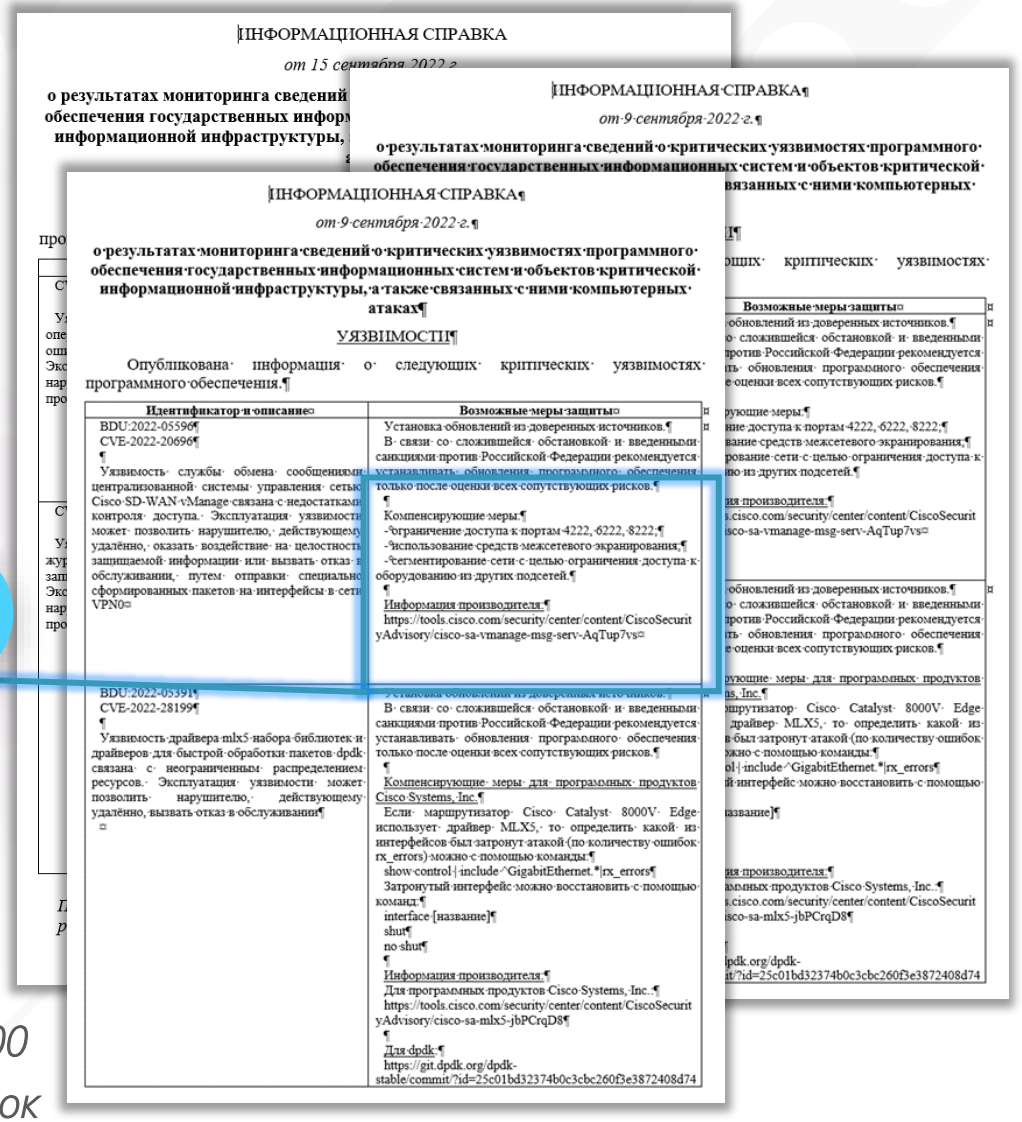
Уязвимости программного обеспечения

Сведения об уязвимости



Компенсирующие меры

Информационные справки


ИНФОРМАЦИОННАЯ СПРАВКА

от 15 сентября 2022 г.

о результатах мониторинга сведений
обеспечения государственных инфор
информационной инфраструктуры,

ИНФОРМАЦИОННАЯ СПРАВКА

от 9 сентября 2022 г.

о результатах мониторинга сведений о критических уязвимостях программного обеспечения государственных информационных систем и объектов критической

связанных с ними компьютерных

ИНФОРМАЦИОННАЯ СПРАВКА

от 9 сентября 2022 г.

о результатах мониторинга сведений о критических уязвимостях программного обеспечения государственных информационных систем и объектов критической информационной инфраструктуры, а также связанных с ними компьютерных атаках

УЯЗВИМОСТИ

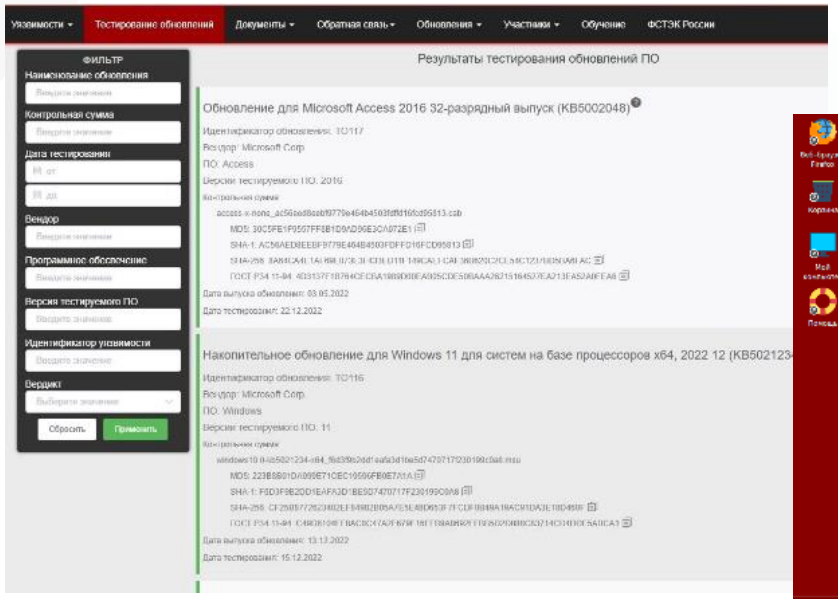
Опубликована информация о следующих критических уязвимостях программного обеспечения.

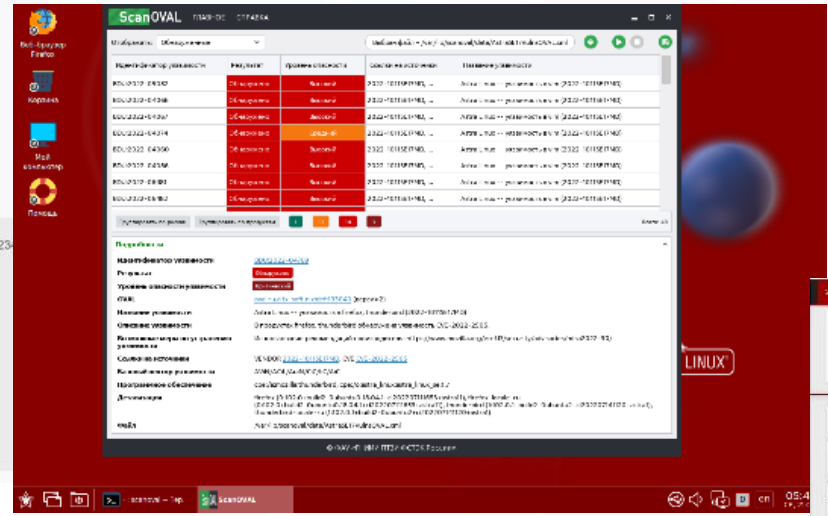
Идентификатор и описание	Возможные меры защиты
BDU:2022-05596 CVE-2022-20696 Уязвимость службы обмена сообщениями централизованной системы управления сетью Cisco SD-WAN vManage связана с недостатками контроля доступа. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, оказать воздействие на целостность защищаемой информации или вызвать отказ в обслуживании, путем отправки специально сформированных пакетов на интерфейсы в сети VPN0	Установка обновлений из доверенных источников. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуется устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков. Компенсирующие меры: -ограничение доступа к портам 4222, 6222, 8222; -использование средств межсетевого экранирования; -сегментирование сети с целью ограничения доступа к оборудованию из других подсетей. Информация производителя: https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-vmanage-msg-serv-AqTup7vs
BDU:2022-05391 CVE-2022-28199 Уязвимость драйвера mlx5 набора библиотек и драйверов для быстрой обработки пакетов dpdk связана с неограниченным распределением ресурсов. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, вызвать отказ в обслуживании	В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуется устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков. Компенсирующие меры для программных продуктов Cisco Systems, Inc.: Если маршрутизатор Cisco Catalyst 8000V Edge использует драйвер MLX5, то определить какой из интерфейсов был затронут атакой (по количеству ошибок rx_errors) можно с помощью команды: show control-plane	include "GigabitEthernet.*|rx_errors" Затронутый интерфейс можно восстановить с помощью команд: interface [название] shut no shut Информация производителя: Для программных продуктов Cisco Systems, Inc.: https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-mlx5-jbPCrqD8 Для dpdk: https://git.dpdk.org/dpdk-stable/commit/?id=25c01bd32374b0c3cbc260f3e3872408d74

Отправлено порядка 200 информационных справок

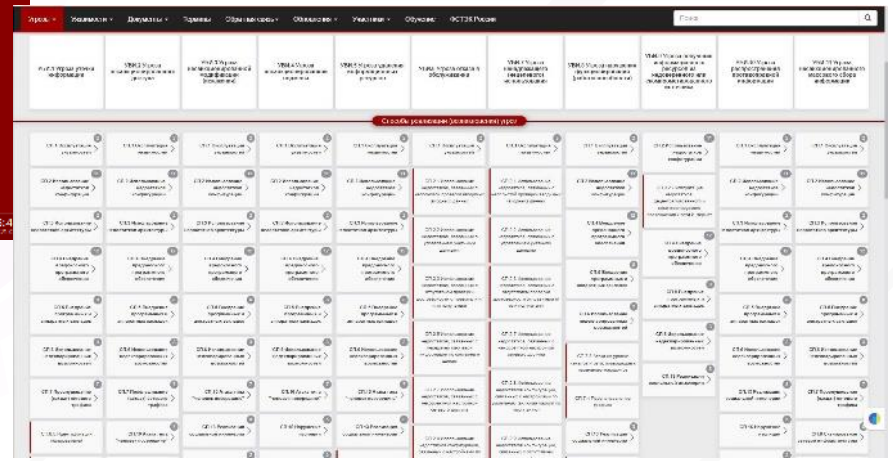
Банк данных угроз безопасности информации

Разделы сайта (2022-2023)





TELEGRAM-КАНАЛ



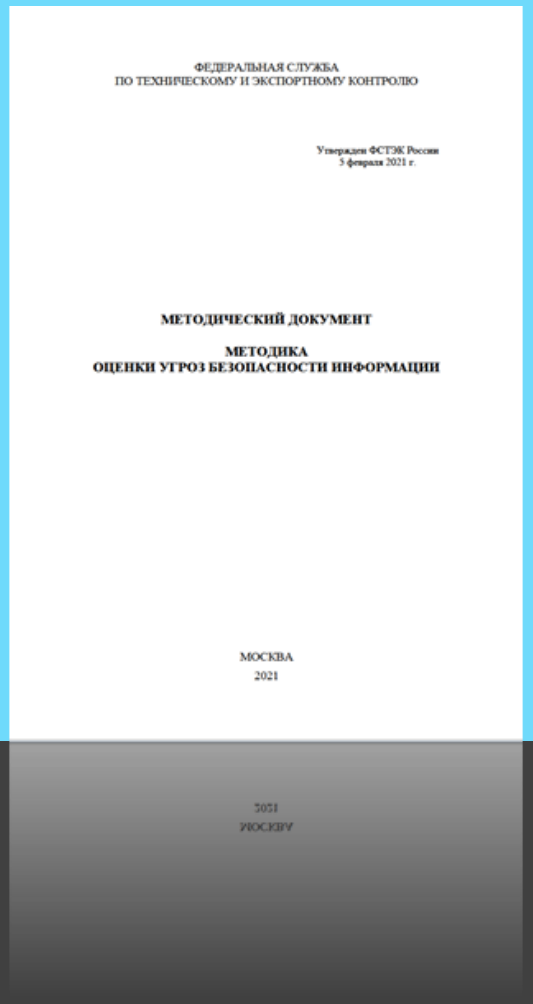
Раздел тестирования обновлений безопасности

Пополнение программ ScanOVAL

Новый раздел угроз

Угрозы безопасности информации

Методика оценки угроз безопасности информации


ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ

Утвержден ФСТЭК России
5 февраля 2021 г.

МЕТОДИЧЕСКИЙ ДОКУМЕНТ

МЕТОДИКА
ОЦЕНКИ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

МОСКВА
2021

Этап 1 – Определение негативных последствий

- Определение негативных последствий, которые могут наступить от реализации УБИ

Этап 2 – Определение объектов воздействий

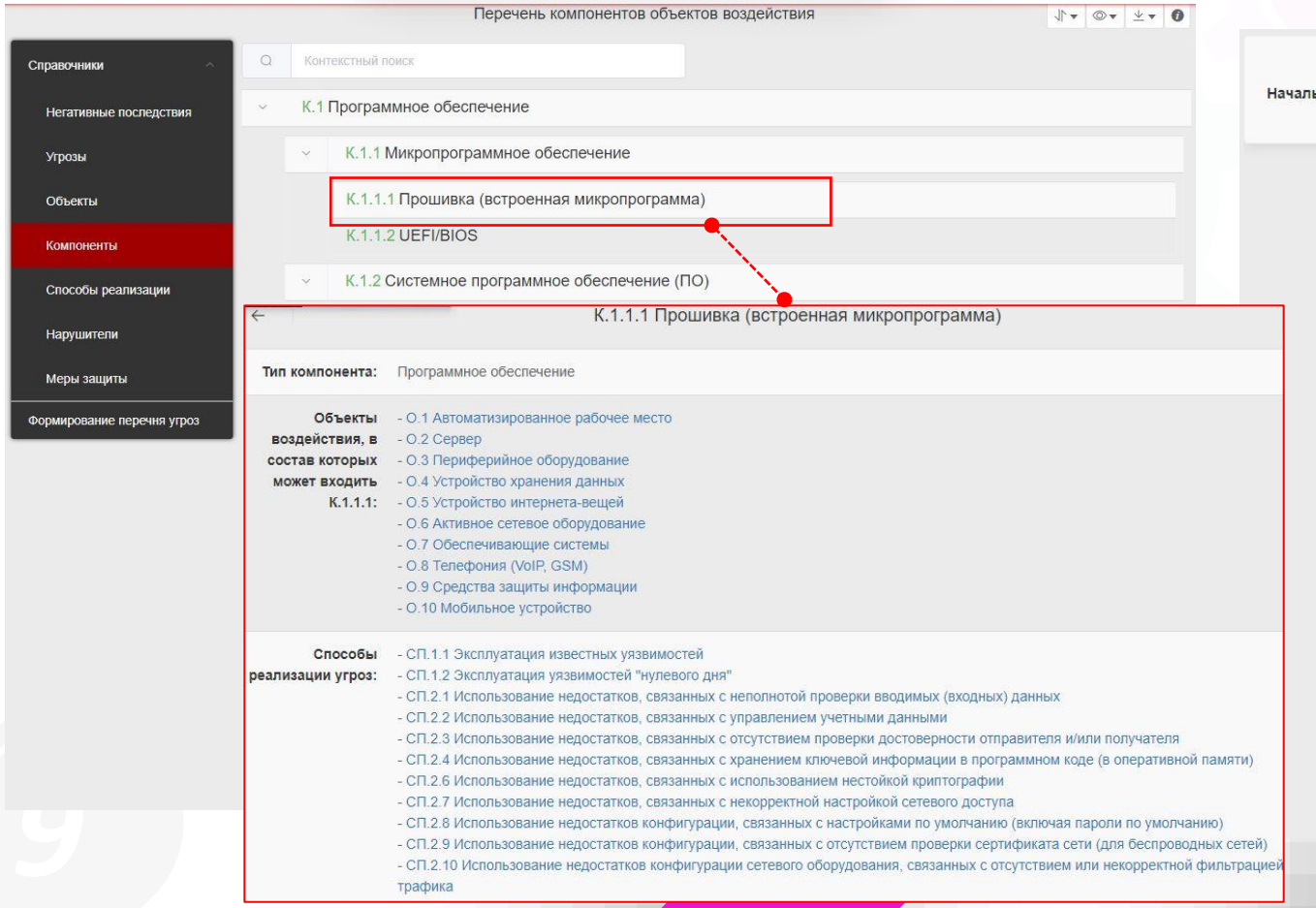
- Инвентаризация систем и сетей и определение возможных объектов воздействия УБИ

Этап 3 – Оценка возможности реализации угроз

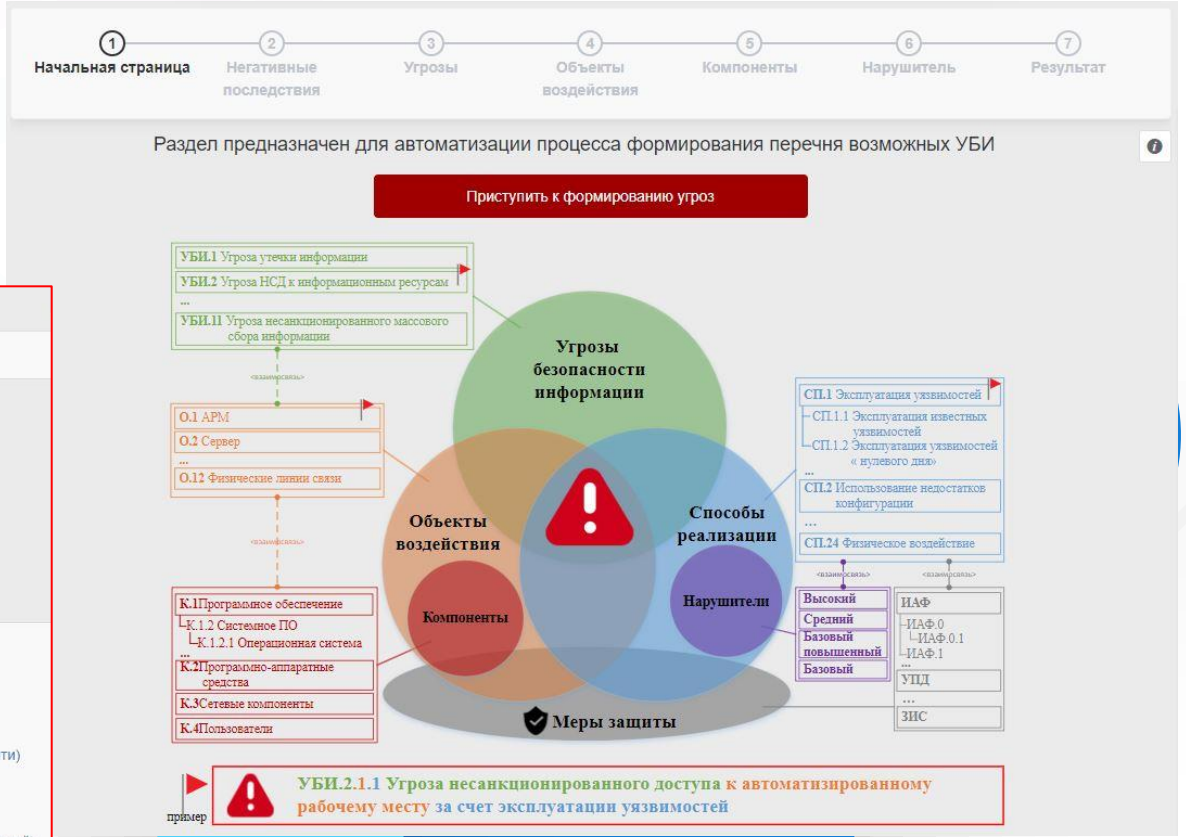
- Определение источников УБИ и оценка возможностей нарушителей по реализации УБИ
- Оценка способов реализации УБИ
- Оценка сценариев реализации УБИ

Новый раздел угроз безопасности информации

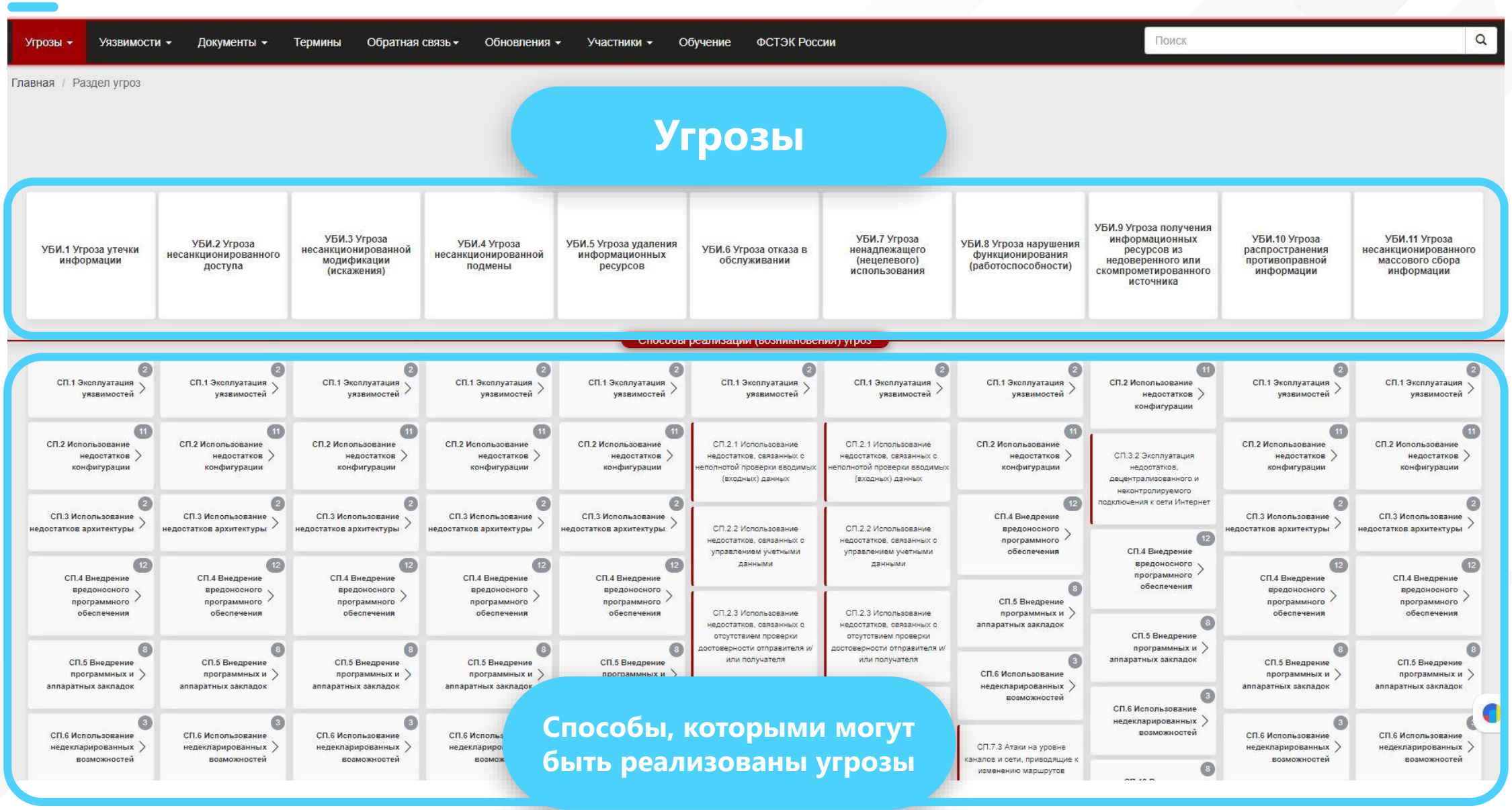
Справочники



Автоматизированное формирование перечня угроз



Новый раздел угроз безопасности информации



Новый раздел угроз безопасности информации

Определение негативных последствий

- Н.1 Угроза жизни или здоровью.
- Н.2 Нарушение неприкосновенности частной жизни.
- Н.3 Нарушение личной, семейной тайны, утрата чести и доброго имени.

Определение объектов воздействий

- О.1 Автоматизированное рабочее место
- О.2 Сервер
- О.3 Периферийное оборудование

- К.1.1.1 Прошивка (встроенная микропрограмма)
- К.1.1.2 UEFI/BIOS
- К.1.2.1 Операционная система

Оценка возможности реализации угроз

- СП.1 Эксплуатация уязвимостей
- СП.1.1 Эксплуатация известных уязвимостей
- СП.1.2 Эксплуатация уязвимостей "нулевого дня"

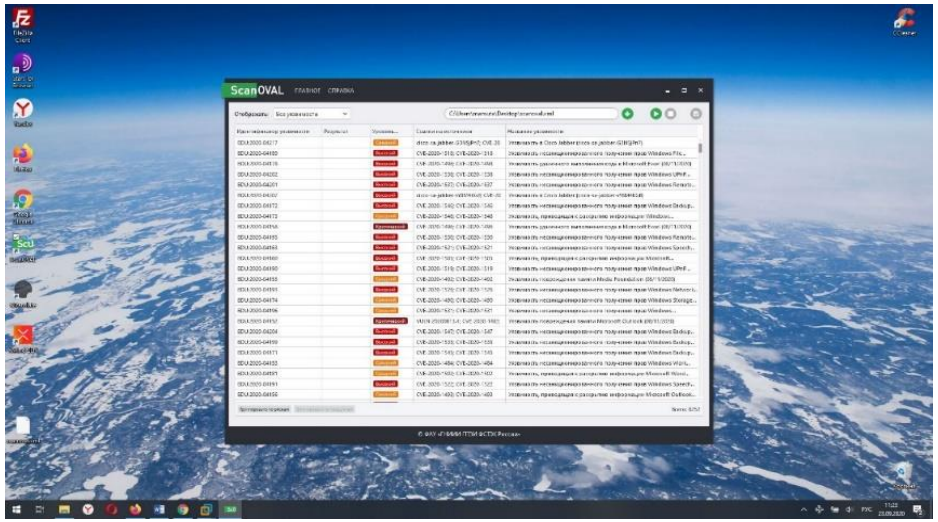
- УБИ.1 Угроза утечки информации
- УБИ.2 Угроза несанкционированного доступа
- УБИ.3 Угроза несанкционированной модификации (искажения)

- В.1 Нарушитель, обладающий базовыми возможностями
- В.2 Нарушитель, обладающий базовыми повышенными возможностями
- В.3 Нарушитель, обладающий средними возможностями

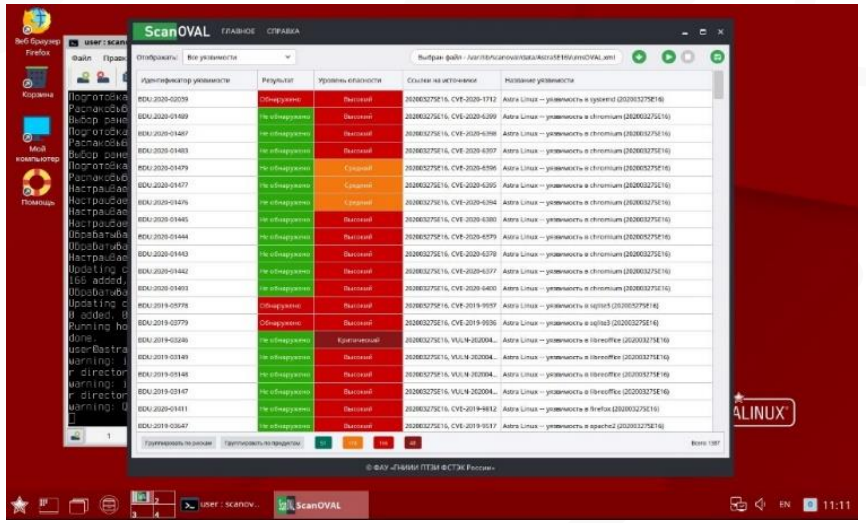
Уязвимости программного обеспечения

Автоматический поиск уязвимостей. Программы ScanOVAL

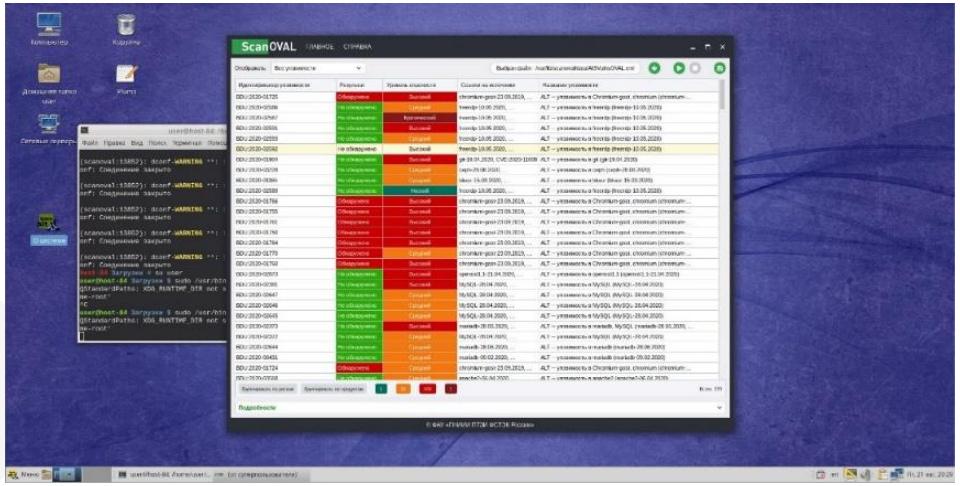
Windows



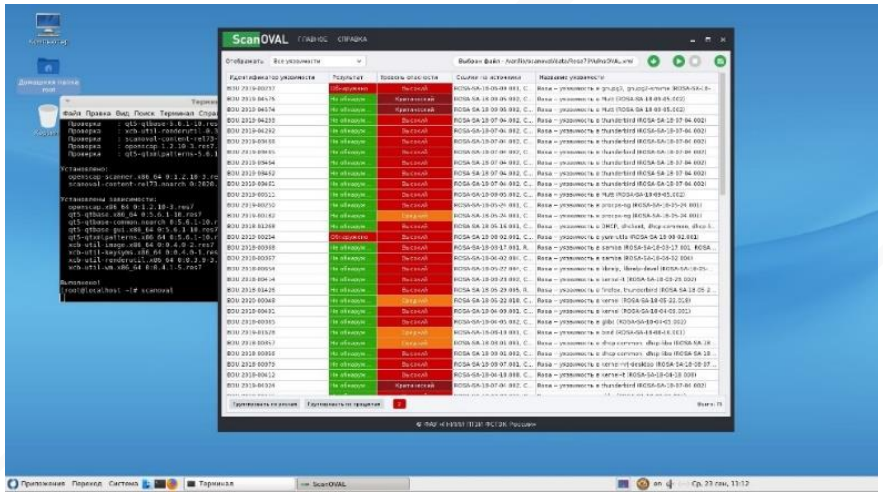
Astra Linux Special Edition 1.6



Alt Linux 9

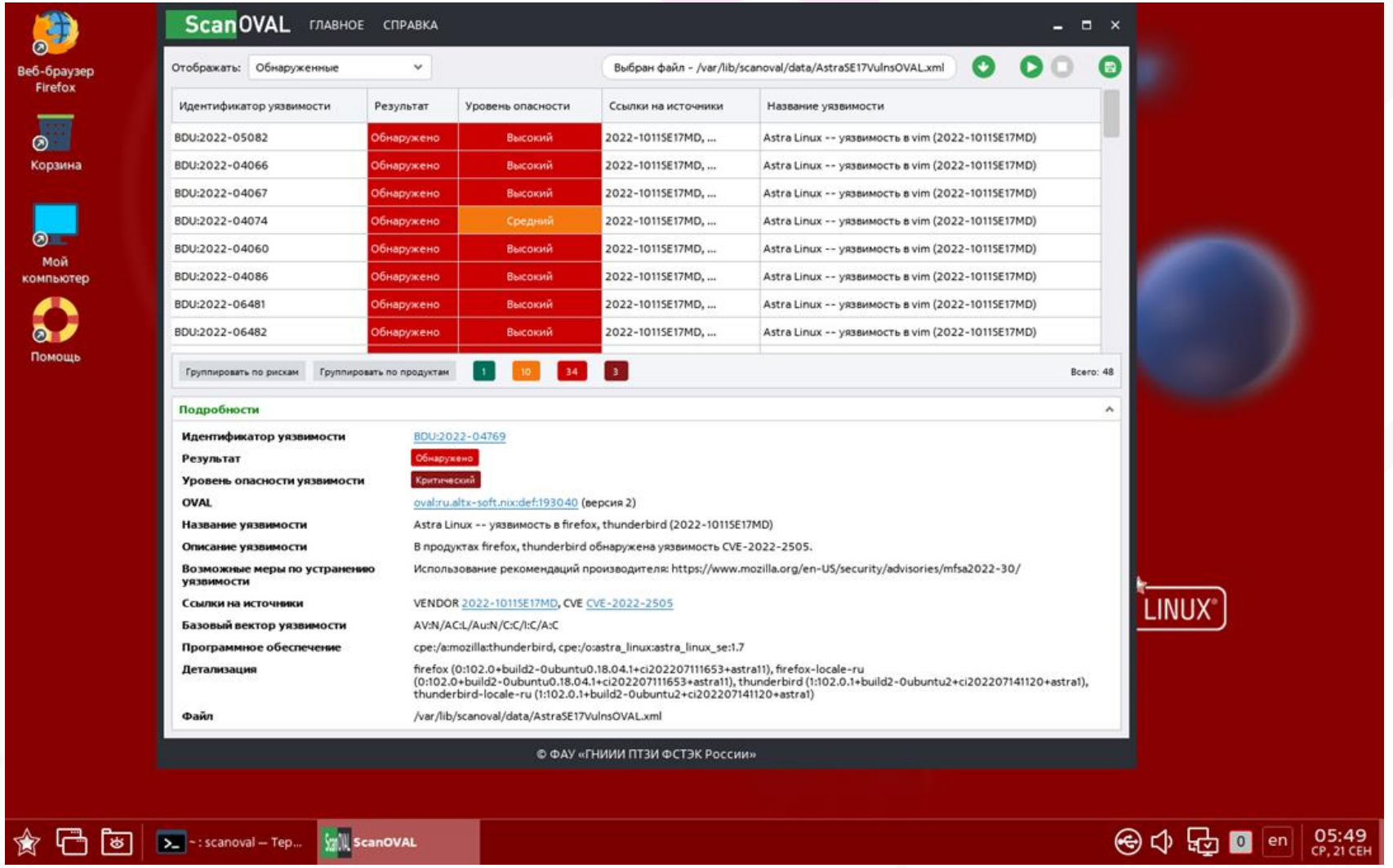


РОСА «КОБАЛЬТ»



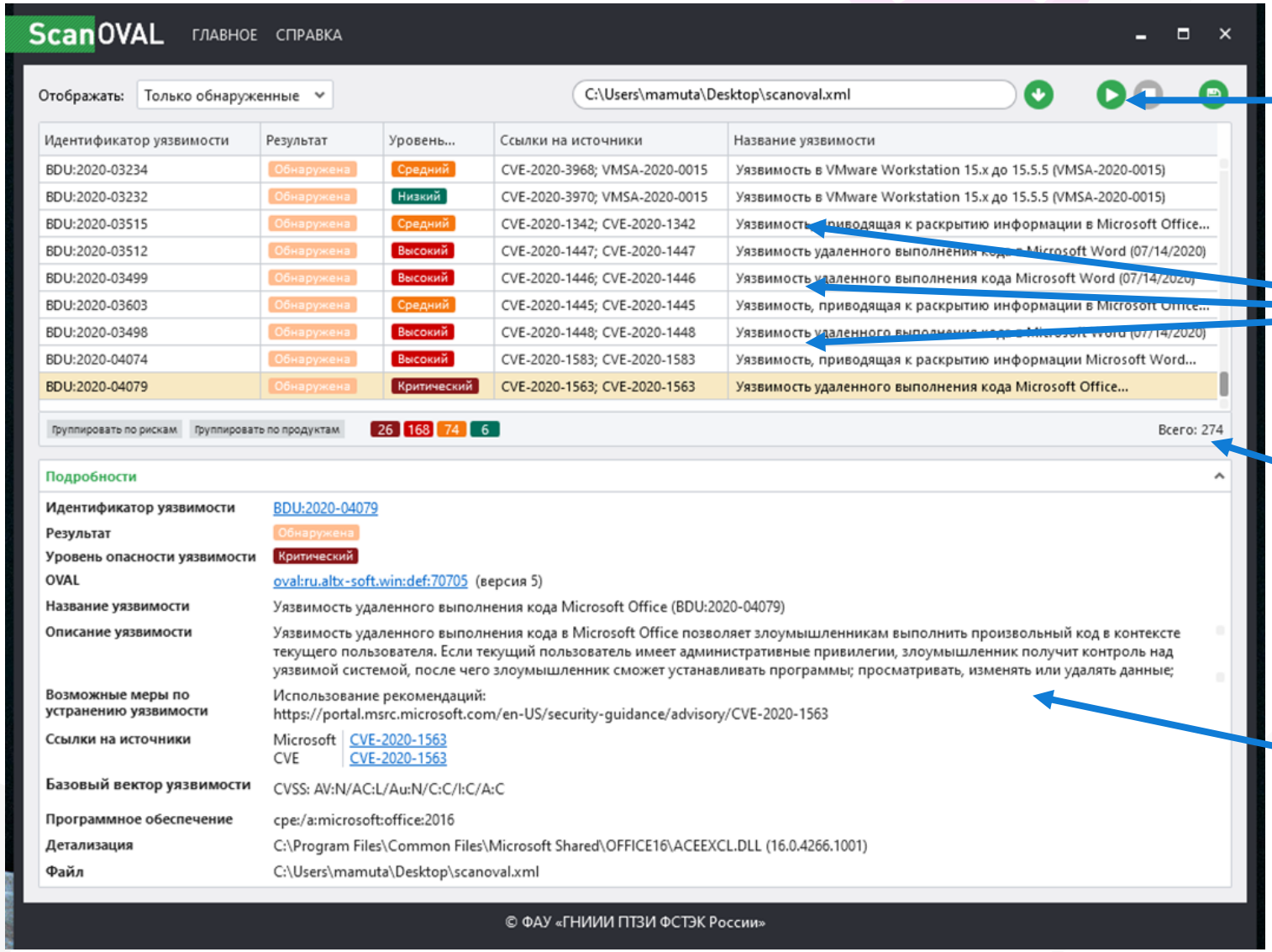
Уязвимости программного обеспечения

Astra Linux Special Edition 1.7 уже на сайте БДУ ФСТЭК России



Уязвимости программного обеспечения

Программы ScanOVAL. Результат сканирования



Кнопка запуска проверки

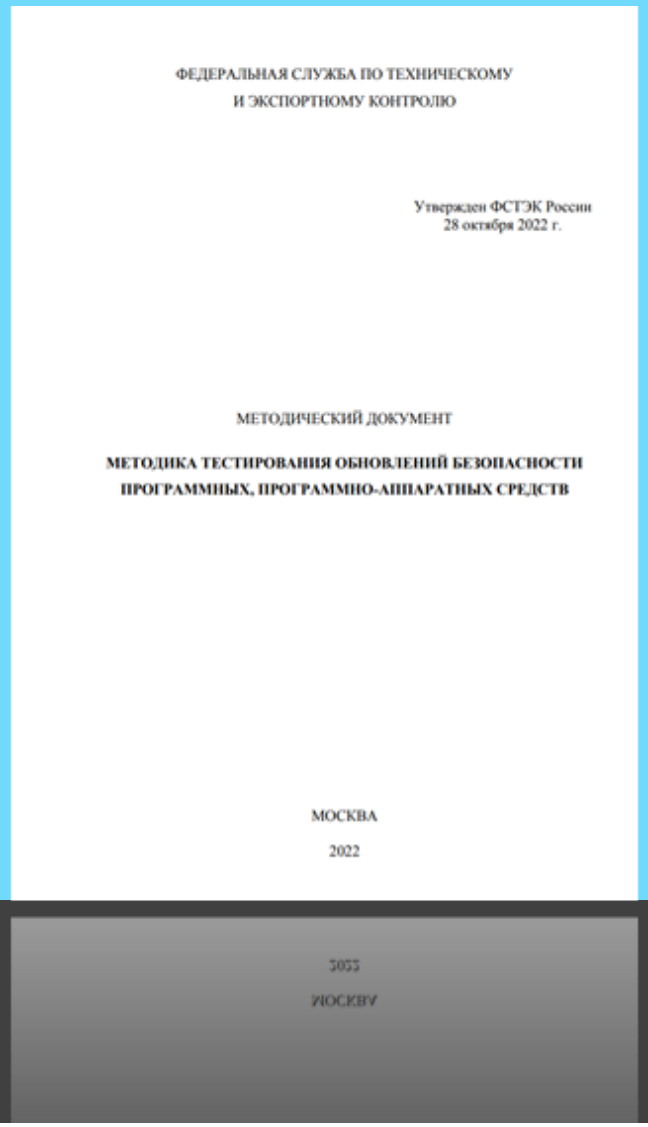
Обнаруженные уязвимости

Количество обнаруженных уязвимостей

Детализированная информация по выбранной записи

Уязвимости программного обеспечения

Методика тестирования обновлений безопасности программных, программно-аппаратных средств


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

- *T001 – Сверка идентичности*
  - *Сравнение контрольных сумм*
- *T002 – Проверка подлинности*
  - *Определение разработчика*
- *T003 – Антивирусный контроль*
  - *Сигнатурный и эвристический анализ*
- *T004 – Поиск опасных конструкций*
  - *Сигнатурный и эвристический анализ*
- *T005 – Мониторинг активности*
  - *Анализ поведения в среде функционирования*
- *T006 – Ручной анализ*
  - *Анализ логики работы, статический и динамический анализ и др.*

Уязвимости программного обеспечения

Рабочая группа по тестированию обновлений

Верификация результатов тестирования

Размещение результатов тестирования обновлений

Тестирование обновлений

СБЕР

ИНТЕР РАО

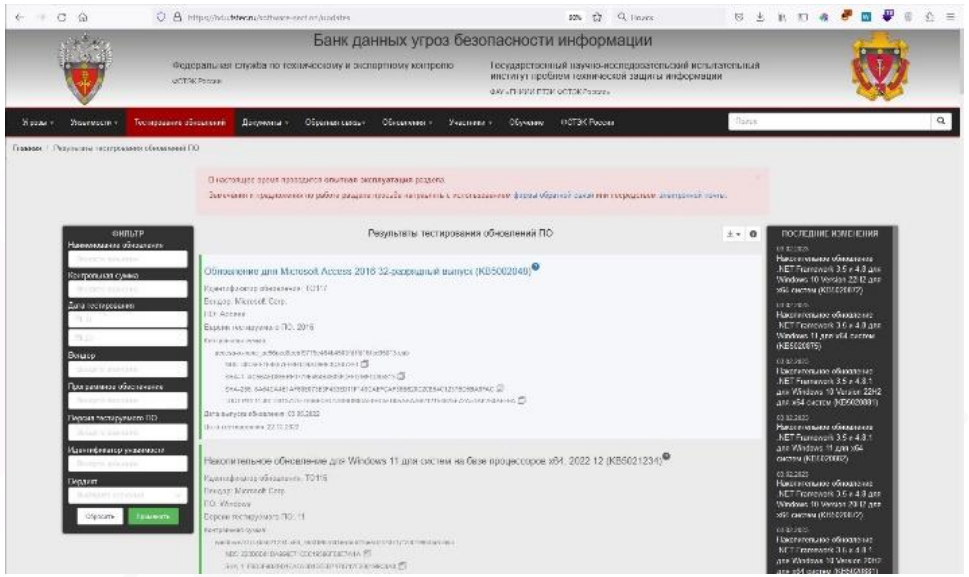
ДЕПАРТАМЕНТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ ГОРОДА МОСКВЫ

positive technologies

ИСП РАН

Рабочая группа

ГНИИИ ПТЗИ ФСТЭК России

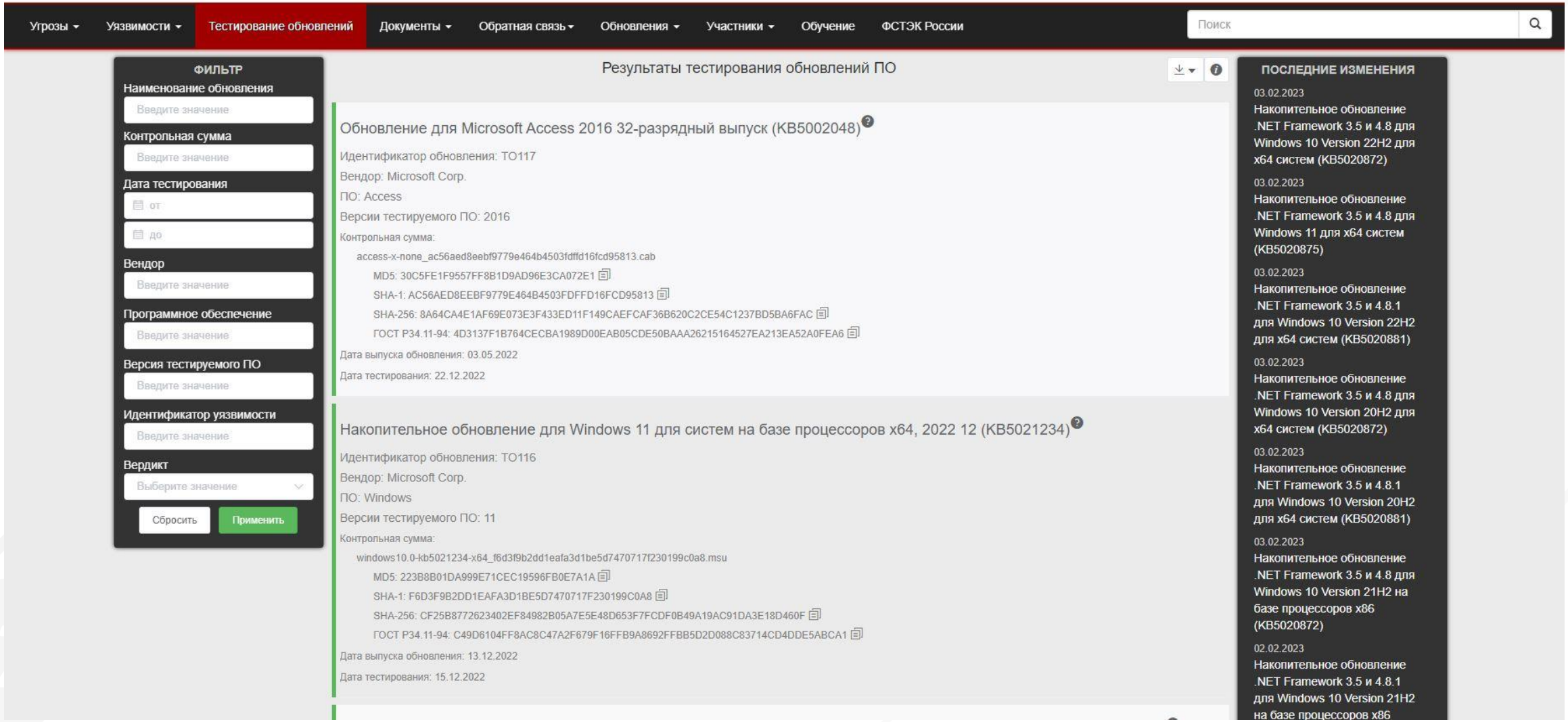


БДУ ФСТЭК России

Уязвимости программного обеспечения

Раздел тестирования обновлений БДУ

bdu.fstec.ru/software-section/updates



Уязвимости программного обеспечения

Раздел тестирования обновлений БДУ ФСТЭК России

Описание результатов тестирования

← Обновление для системы безопасности Microsoft Visio 2016 32-разрядный выпуск (KB5002286)

Идентификатор обновления:	TO102
Наименование:	Обновление для системы безопасности Microsoft Visio 2016 32-разрядный выпуск (KB5002286)
Описание:	https://support.microsoft.com/help/5002286
URI:	https://catalog.s.download.windowsupdate.com/c/msdownload/update/software/secu/2022/11/visio-x-none_80d9120cdce1d2bcd022fa5c1217663379a8ae50.cab https://www.catalog.update.microsoft.com/Search.aspx?q=5002286
Контрольная сумма:	**visio-x-none_80d9120cdce1d2bcd022fa5c1217663379a8ae50.cab**: MD5: 8AF40BAD0C4F27301F9FC3FEB8C5CC61 SHA-1: 80D9120CDCE1D2BCD022FA5C1217663379A8AE50 SHA-256: B5A15CC1F3B29DF70F6D451796D7C52B63B9AD56986C48F219C4B176220D9A40 ГОСТ Р34.11-94: 4E17129CDACB0130B97F5A583F0531829755758AD89FCE12ABF23E5508AD2114
Дата выпуска обновления:	13.12.2022
Вендор:	Microsoft Corp.
ПО:	Microsoft Visio
Версии уязвимого ПО:	2016
Версии тестируемого ПО:	2016
Обновление направлено на устранение уязвимостей:	BDU:2022-07399
Идентификаторы других систем описаний уязвимостей:	CVE: CVE-2022-44695 ZDI: ZDI-22-1672
Вердикт:	Негативного влияния не выявлено

Уязвимости программного обеспечения

Раздел тестирования обновлений БДУ ФСТЭК России

Результаты выполнения тестов

Результаты тестирования:

Организация 1

Наименование теста	Результат	Среда тестирования
Сверка идентичности обновлений, полученных из разных источников (T001)	Обновления идентичны	Исследовательский стенд
Проверка подлинности обновлений (T002)	Установлена подлинность обновлений	Исследовательский стенд
Антивирусный контроль обновлений (T003)	Не выявлены признаки вредоносной активности	Исследовательский стенд
Поиск опасных конструкций (T004)	Опасные конструкции не найдены	Исследовательский стенд
Производилась проверка распакованных файлов и сетевого трафика на индикаторы компрометации (IOC)	Не выявлено признаков не декларированных возможностей или деструктивного функционала	Исследовательский стенд
Ручной анализ обновления (T006)	Не проводился	-

Уязвимости программного обеспечения

Раздел тестирования обновлений БДУ ФСТЭК России

Сведения о результатах тестирований в описаниях уязвимостей

BDU:2022-07399: Уязвимость графического редактора Microsoft Visio, пакетов программ Microsoft Office и 365 Apps for Enterprise, связанная с использованием памяти после ее освобождения, позволяющая нарушителю выполнить произвольный код

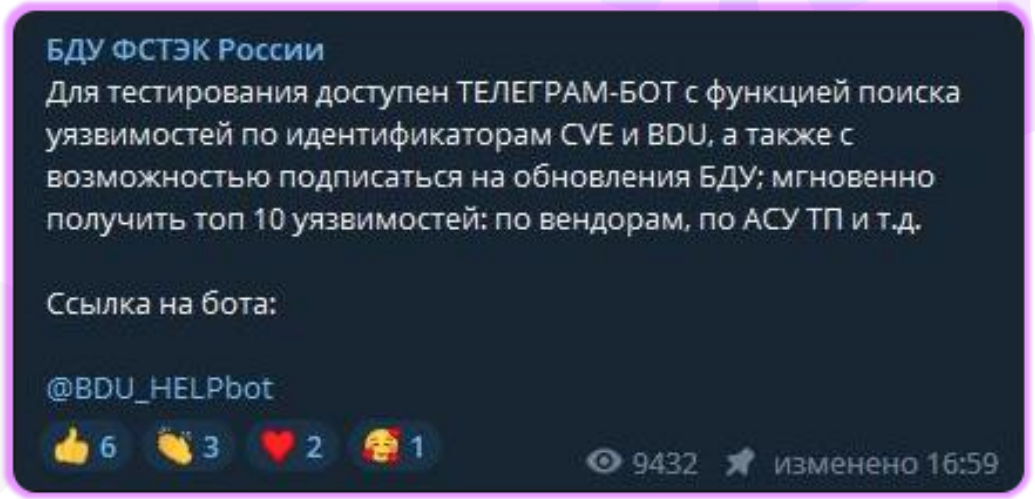
Вид

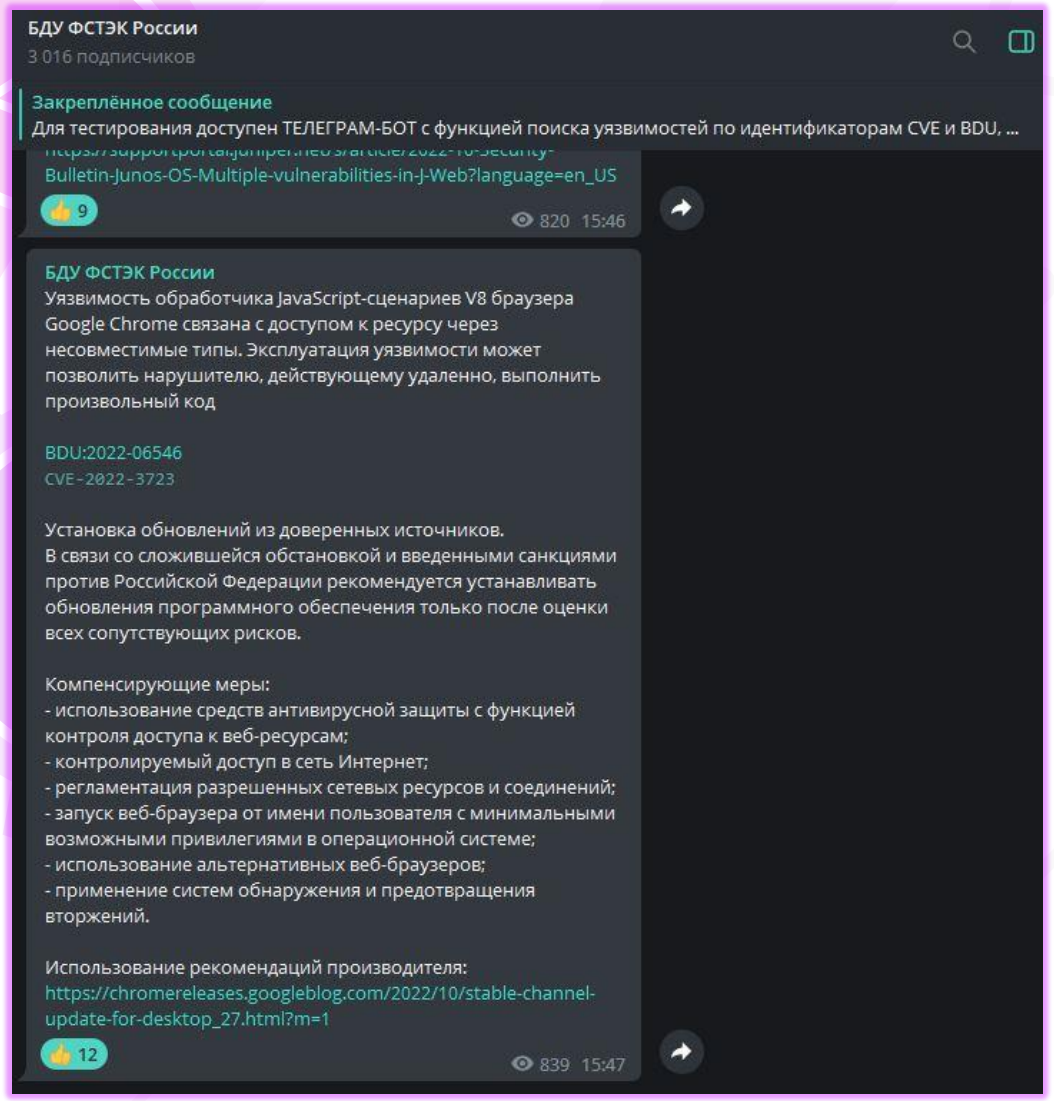
Описание уязвимости	Уязвимость графического редактора Microsoft Visio, пакетов программ Microsoft Office и 365 Apps for Enterprise связана с использованием памяти после ее освобождения. Эксплуатация уязвимости может позволить нарушителю выполнить произвольный код с помощью специально созданного файла DWG
Вендор	Microsoft Corp.
Наименование ПО	Microsoft Office, Microsoft Visio, 365 Apps for Enterprise
Версия ПО	2019 (Microsoft Office) 2013 SP1 (Microsoft Visio) 2016 (Microsoft Visio) - (365 Apps for Enterprise) LTSC 2021 (Microsoft Office)
Тип ПО	Прикладное ПО информационных систем
Операционные системы и аппаратные платформы	Данные уточняются
Тип ошибки	Использование после освобождения
Идентификатор типа ошибки	CWE-416
Класс уязвимости	Уязвимость кода
Дата выявления	13.12.2022
Базовый вектор уязвимости	CVSS 2.0: AV:L/AC:L/Au:N/C:C/I:C/A:C CVSS 3.0: AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
Уровень опасности уязвимости	Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,2) Высокий уровень опасности (базовая оценка CVSS 3.0 составляет 7,8)
Возможные меры по устранению уязвимости	Использование рекомендаций производителя: Результаты тестирования обновлений: Обновление для системы безопасности Microsoft Visio 2016 32-разрядный выпуск (KB5002286) Обновление для системы безопасности Microsoft Visio 2016 64-разрядный выпуск (KB5002286)
Статус уязвимости	Подтверждена производителем
Наличие эксплойта	Данные уточняются

Новые возможности банка данных угроз безопасности информации

Telegram-канал и БОТ с возможностью подписки на рассылку

t.me/bdufstecru





Уязвимости программного обеспечения

Проведены работы по устранению 739 уязвимостей «нулевого дня»

Среднее время реагирования вендора:
5 ДНЕЙ

Среднее время устранения уязвимости:
30 ДНЕЙ

Направления совершенствования банка данных угроз

1.Развитие и совершенствование нового раздела угроз безопасности информации

2.Развитие API-интерфейса и предоставление к нему доступа пользователям

3.Развитие раздела, содержащего результаты тестирования обновлений

4.Модернизация раздела уязвимостей (добавление информации об уязвимых компонентах)

5.Разработка новых программ ScanOVAL для дистрибутивов отечественных операционных систем