ФАУ «ГНИИИ ПТЗИ ФСТЭК России»

РАЗВИТИЕ ОТЕЧЕСТВЕННЫХ ИНФОРМАЦИОННЫХ РЕСУРСОВ, СОДЕРЖАЩИХ СВЕДЕНИЯ ОБ УГРОЗАХ БЕЗОПАСНОСТИ ИНФОРМАЦИИ И УЯЗВИМОСТЯХ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Начальник управления ГНИИИ ПТЗИ ФСТЭК России
Александр Суховерхов

ОТЕЧЕСТВЕННЫЕ ИНФОРМАЦИОННЫЕ РЕСУРСЫ

1

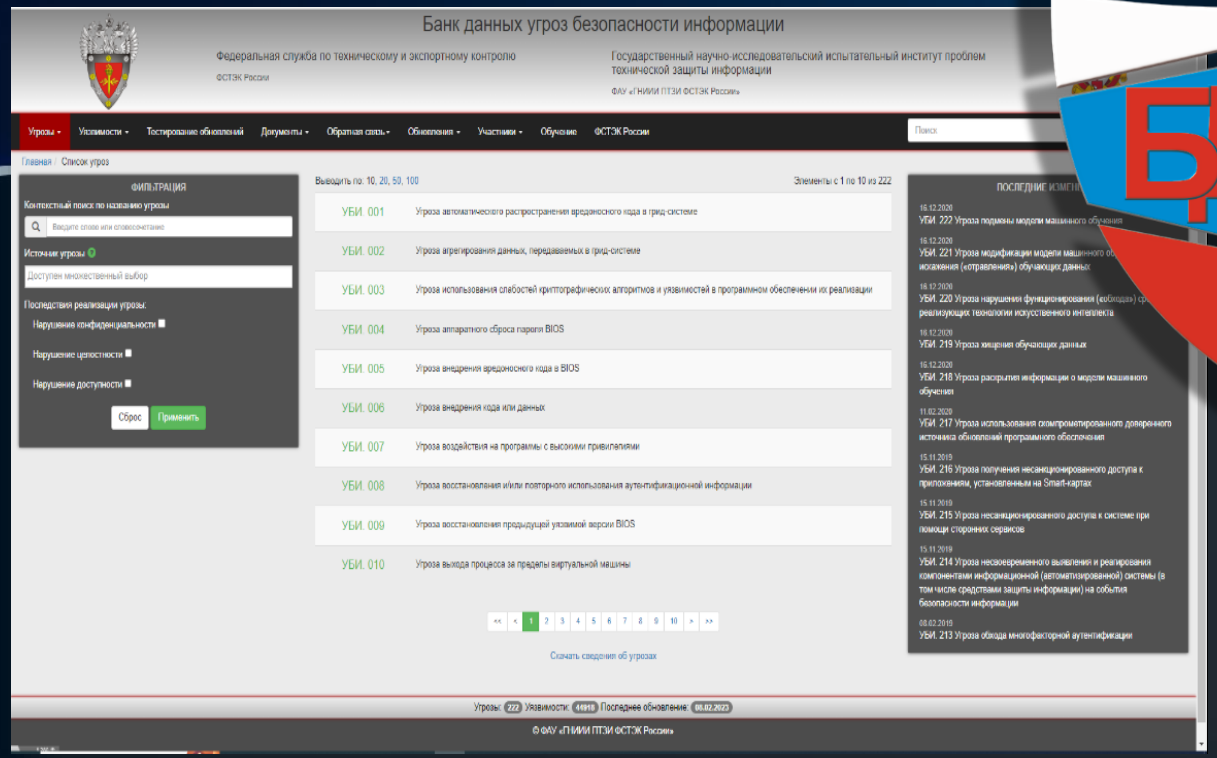
БАНК ДАННЫХ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ ФСТЭК РОССИИ

новинка

2

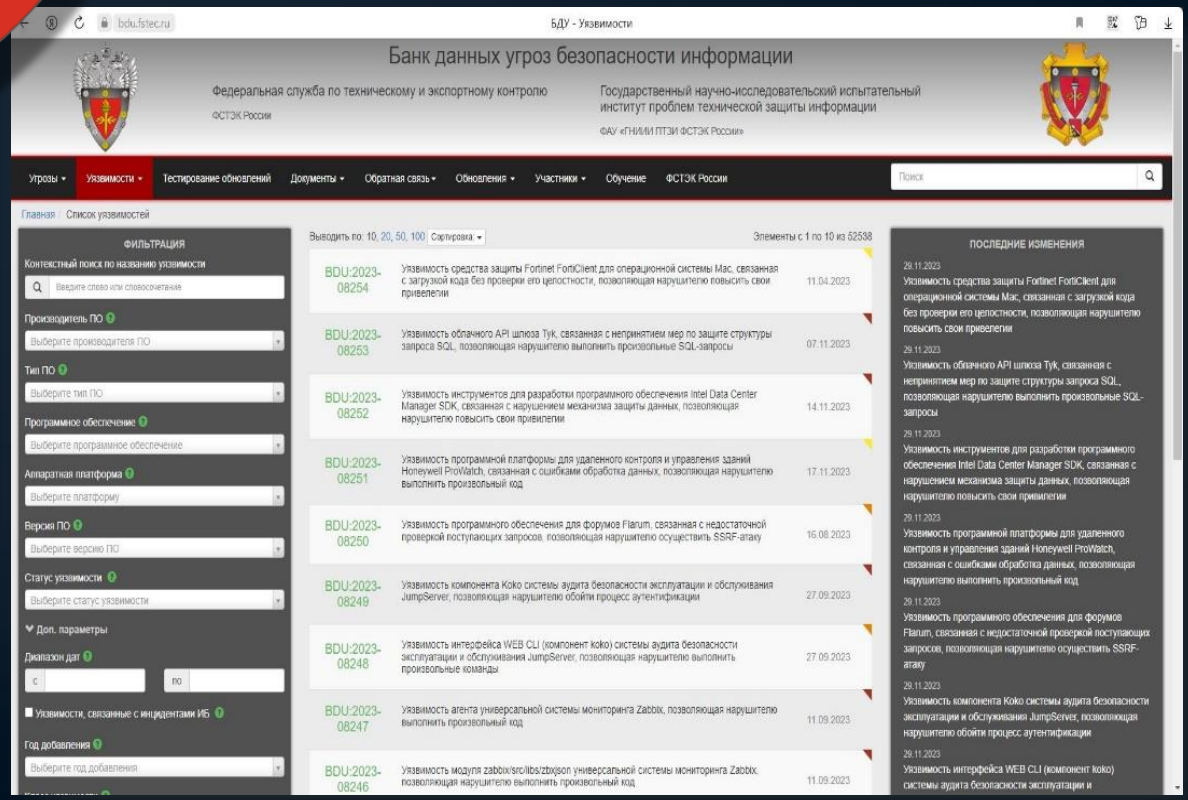
БАНК ДАННЫХ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ АСУ ТП

БАНК ДАННЫХ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ ФСТЭК РОССИИ



БДУ

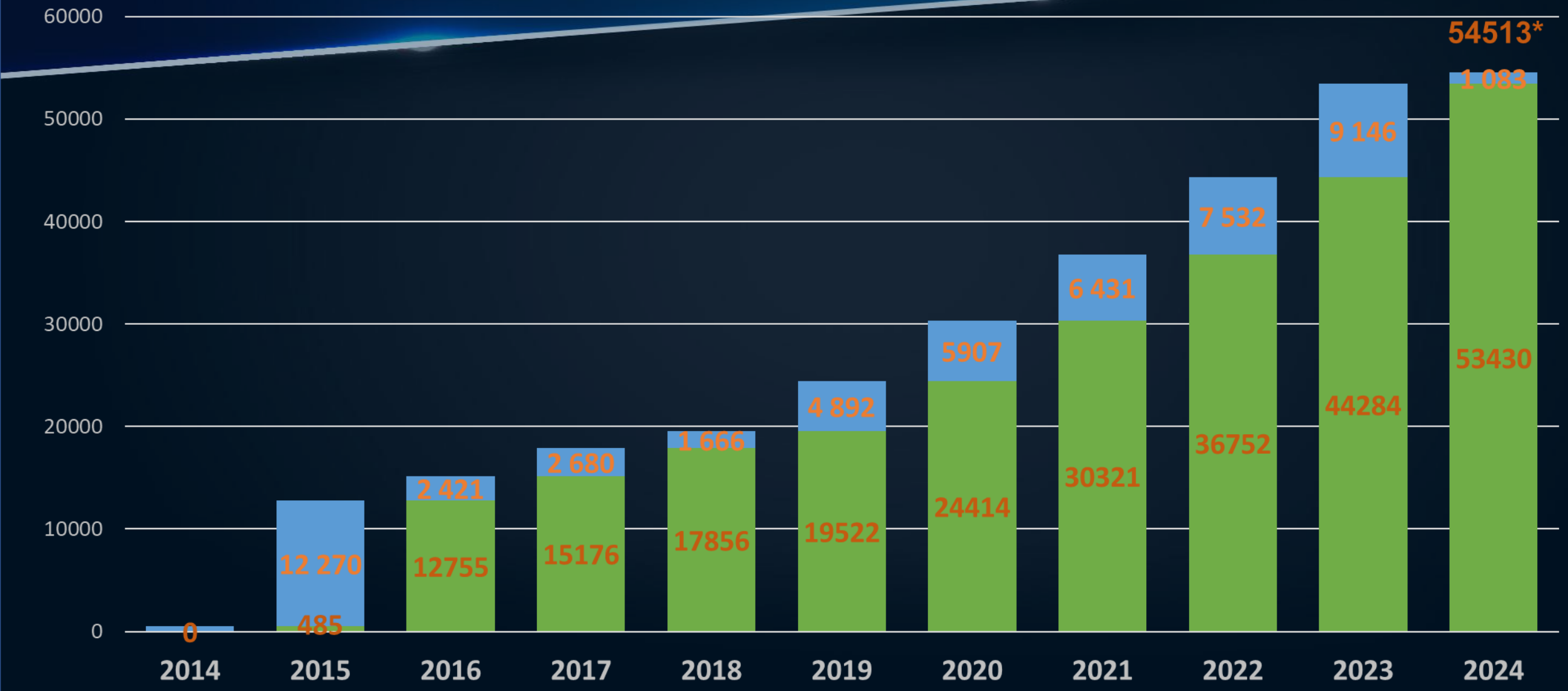
Уязвимости >54000



Угрозы 222

https://bdu.fstec.ru

ВКЛЮЧЕНИЕ ЗАПИСЕЙ ОБ УЯЗВИМОСТЯХ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ В БДУ ФСТЭК РОССИИ ПО ГОДАМ



* Данные актуальны по состоянию на 08.02.2024

НОВЫЙ РАЗДЕЛ УГРОЗ БДУ ФСТЭК РОССИИ

Последствия	Угрозы	Объекты	Компоненты	Способы	Типы нарушителей	Меры защиты
52	11	13	52	173	4	490

Справочники
- Негативные последствия
- Угрозы
- Объекты
- Компоненты
- Способы реализации
- Нарушители
- Меры защиты

Формирование перечня угроз

Справочники
- Негативные последствия
- Угрозы
- Объекты
- Компоненты
- Способы реализации
- Нарушители
- Меры защиты

Формирование перечня угроз

Справочники
- Негативные последствия
- Угрозы
- Объекты
- Компоненты
- Способы реализации
- Нарушители
- Меры защиты

Формирование перечня угроз

Справочники
- Негативные последствия
- Угрозы
- Объекты
- Компоненты
- Способы реализации
- Нарушители
- Меры защиты

Формирование перечня угроз

Справочники
- Негативные последствия
- Угрозы
- Объекты
- Компоненты
- Способы реализации
- Нарушители
- Меры защиты

Формирование перечня угроз

Справочники
- Негативные последствия
- Угрозы
- Объекты
- Компоненты
- Способы реализации
- Нарушители
- Меры защиты

Формирование перечня угроз

Справочники
- Негативные последствия
- Угрозы
- Объекты
- Компоненты
- Способы реализации
- Нарушители
- Меры защиты

Формирование перечня угроз

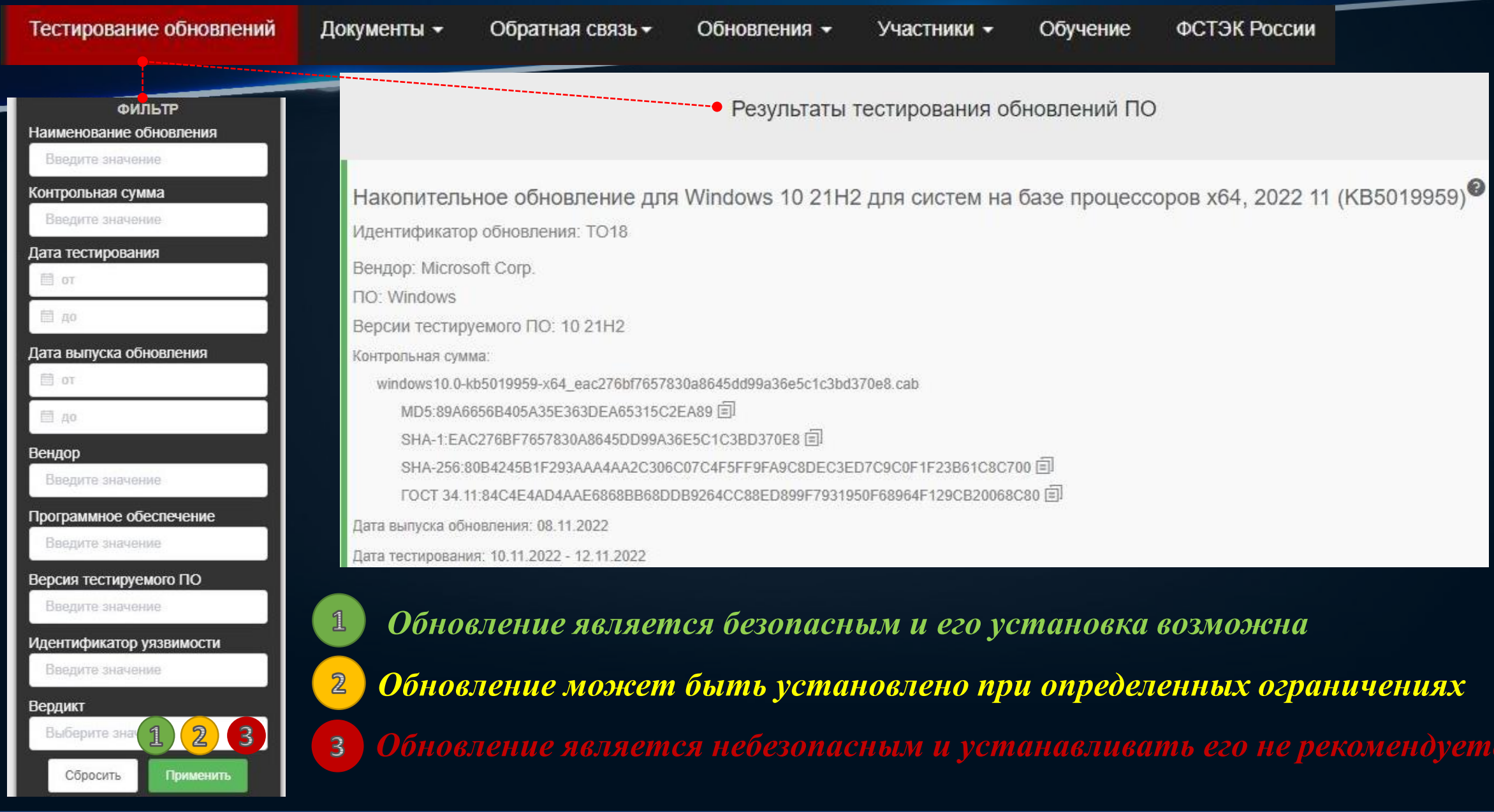
- О.1 Автоматизированное рабочее место
- О.2 Сервер
- О.3 Периферийное оборудование
- О.4 Устройство хранения данных
- О.5 Устройство интернета-вещей

К.1 Программное обеспечение
- К.1.1 Микропрограммное обеспечение
  - К.1.1.1 Прошивка (встроенная микропрограмма)
  - К.1.1.2 UEFI/BIOS
- К.1.2 Системное программное обеспечение (ПО)
  - К.1.2.1 Операционная система
  - К.1.2.2 Мобильная операционная система

- СП.1.1 Эксплуатация известных уязвимостей
- СП.1.2 Эксплуатация уязвимостей "нулевого дня"
- СП.2.1 Использование недостатков, связанных с неполнотой проверки вводимых (входных) данных
- СП.2.2 Использование недостатков, связанных с управлением учетными данными
- СП.2.3 Использование недостатков, связанных с отсутствием проверки достоверности отправителя и/или получателя
- СП.2.4 Использование недостатков, связанных с хранением ключевой информации в программном коде (в оперативно
- СП.2.6 Использование недостатков, связанных с использованием нестойкой криптографии
- СП.2.7 Использование недостатков, связанных с некорректной настройкой сетевого доступа
- СП.2.8 Использование недостатков конфигурации, связанных с настройками по умолчанию (включая пароли по умолча
- СП.2.9 Использование недостатков конфигурации, связанных с отсутствием проверки сертификата сети (для беспрово
- СП.2.10 Использование недостатков конфигурации сетевого оборудования, связанных с отсутствием или некорректной трафика

РАЗДЕЛ ТЕСТИРОВАНИЯ ОБНОВЛЕНИЙ БДУ ФСТЭК РОССИИ

bdu.fstec.ru/software-section/updates



1 *Обновление является безопасным и его установка возможна*

2 *Обновление может быть установлено при определенных ограничениях*

3 *Обновление является небезопасным и устанавливать его не рекомендуется*

ТЕСТИРОВАНИЕ ОБНОВЛЕНИЙ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

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

АЛГОРИТМ ПРОВЕДЕНИЯ ТЕСТИРОВАНИЯ

Сверка идентичности (T001) и проверка подлинности (T002) обновлений

T001

Сверка идентичности обновлений безопасности предусматривает:

1) получение обновления безопасности разными способами и (или) из различных источников

2) расчет контрольных сумм обновления безопасности

3) сравнение обновлений безопасности путем сравнения их контрольных сумм

Выводы:

- обновления идентичны
- выявлены различия, объяснены исследователем и не вызывают опасности

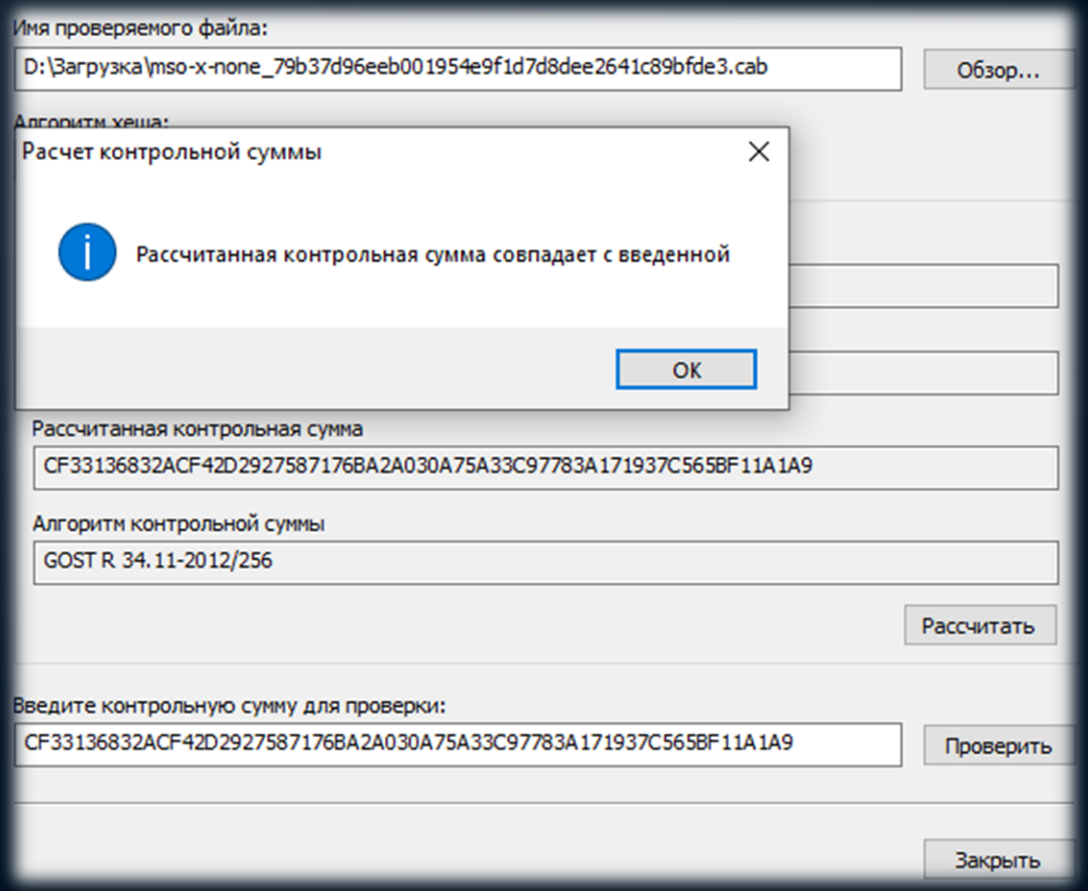
- выявлены различия, идентифицировать назначение которых не удалось

- выявлены признаки недекларированных возможностей

T002

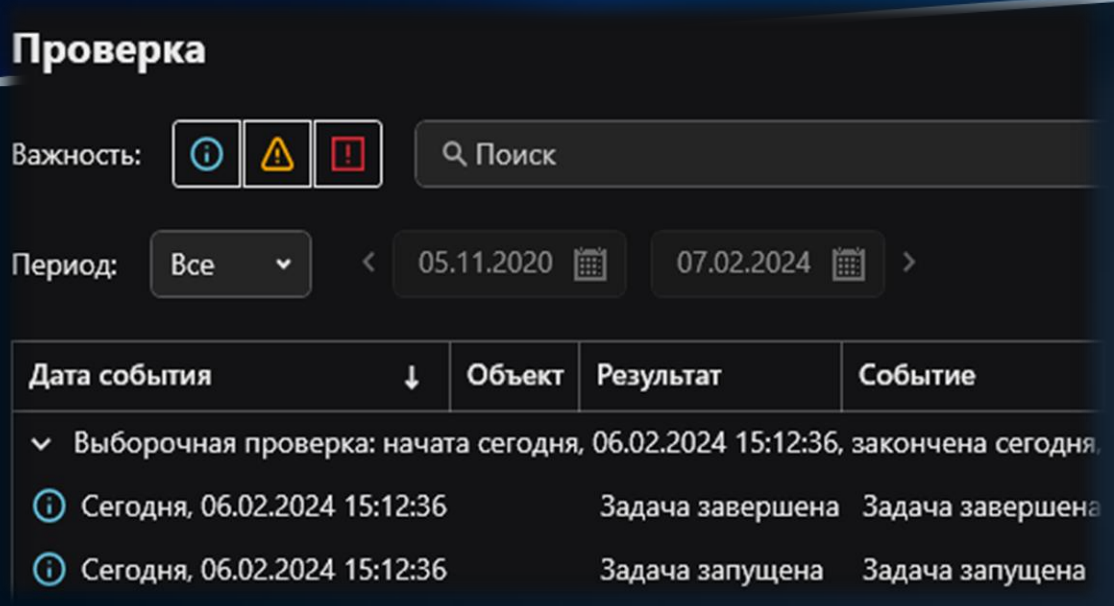
Выводы:

- установлена подлинность обновлений
- обновления не прошли проверку подлинности



Антивирусный контроль обновлений (T003) и поиск опасных конструкций (T004)

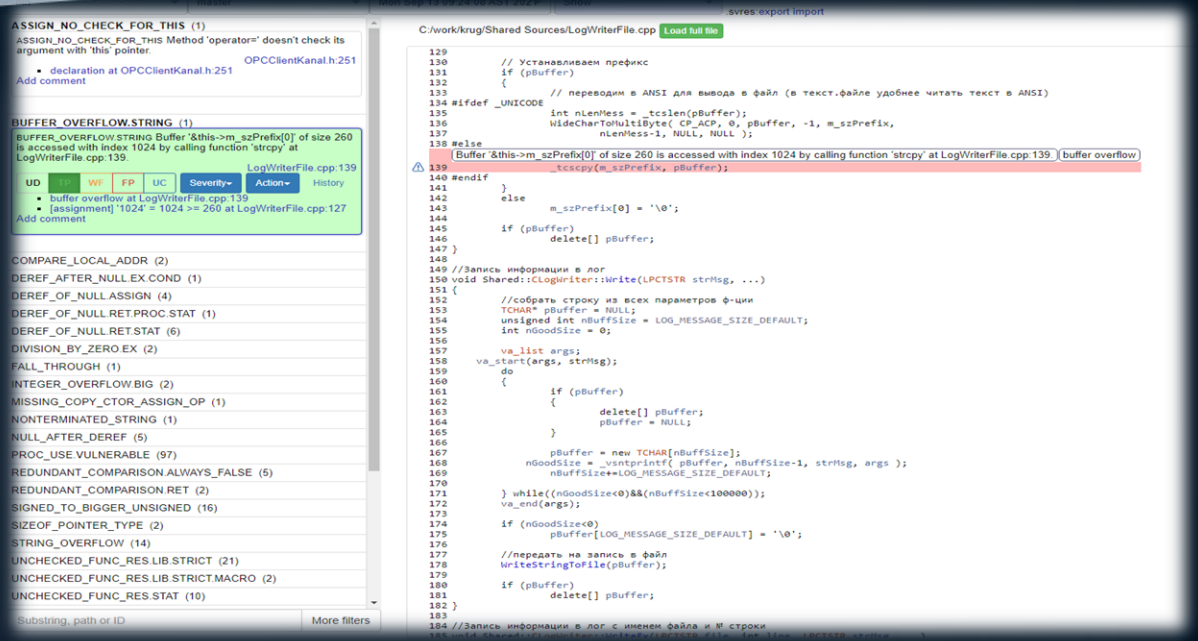
T003



Выводы:

- не выявлены признаки вредоносной активности
- **признаки вредоносной активности выявлены, сигнатура ВПО не определена**
- **признаки вредоносной активности выявлены, сигнатура ВПО определена**

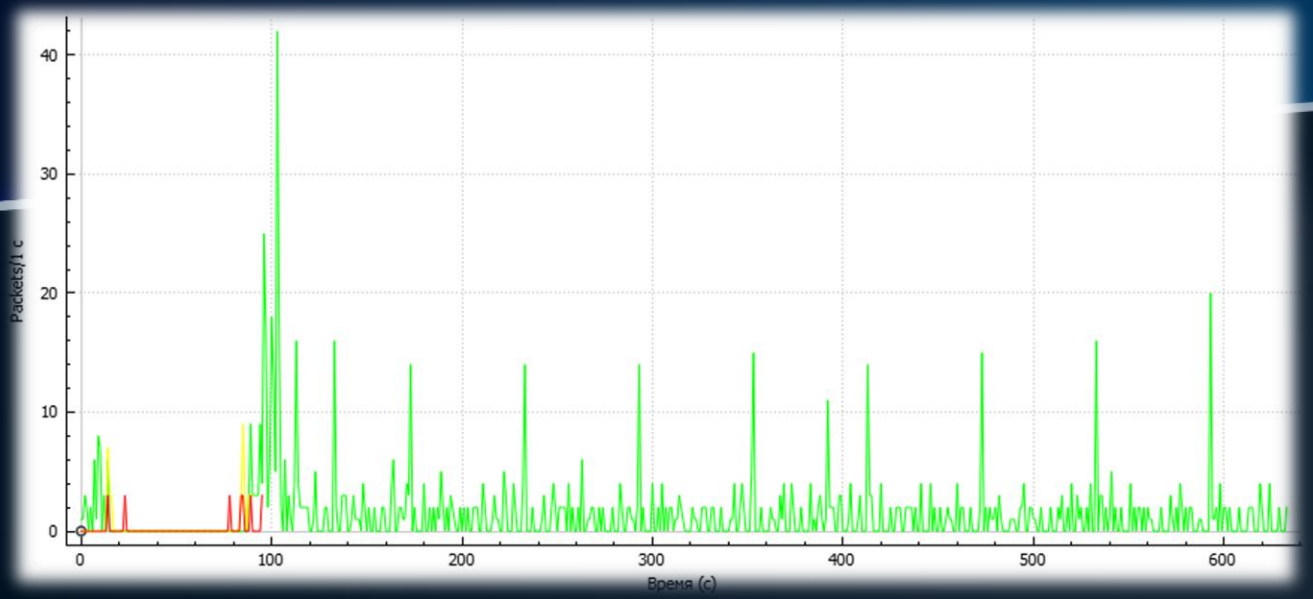
T004

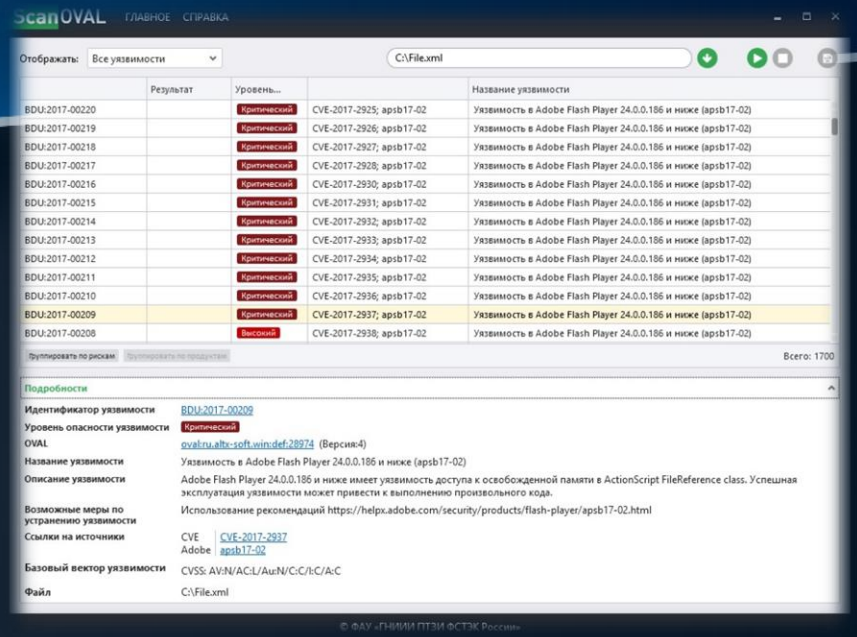


Выводы:

- опасные конструкции не найдены
- **найдены потенциально конструкции, идентифицировать назначение которых не удалось**
- опасные конструкции найдены

Мониторинг активности обновлений в среде функционирования (T005)





Мониторинг активности обновлений безопасности в среде тестирования предусматривает необходимость проведения:

а) анализа результатов выполнения системных вызовов обновленного ПО

б) анализа получаемых и отправляемых обновленным ПО сетевых пакетов

в) анализа состава файловой системы до и после установки обновления ПО

г) сигнатурного поиска известных уязвимостей

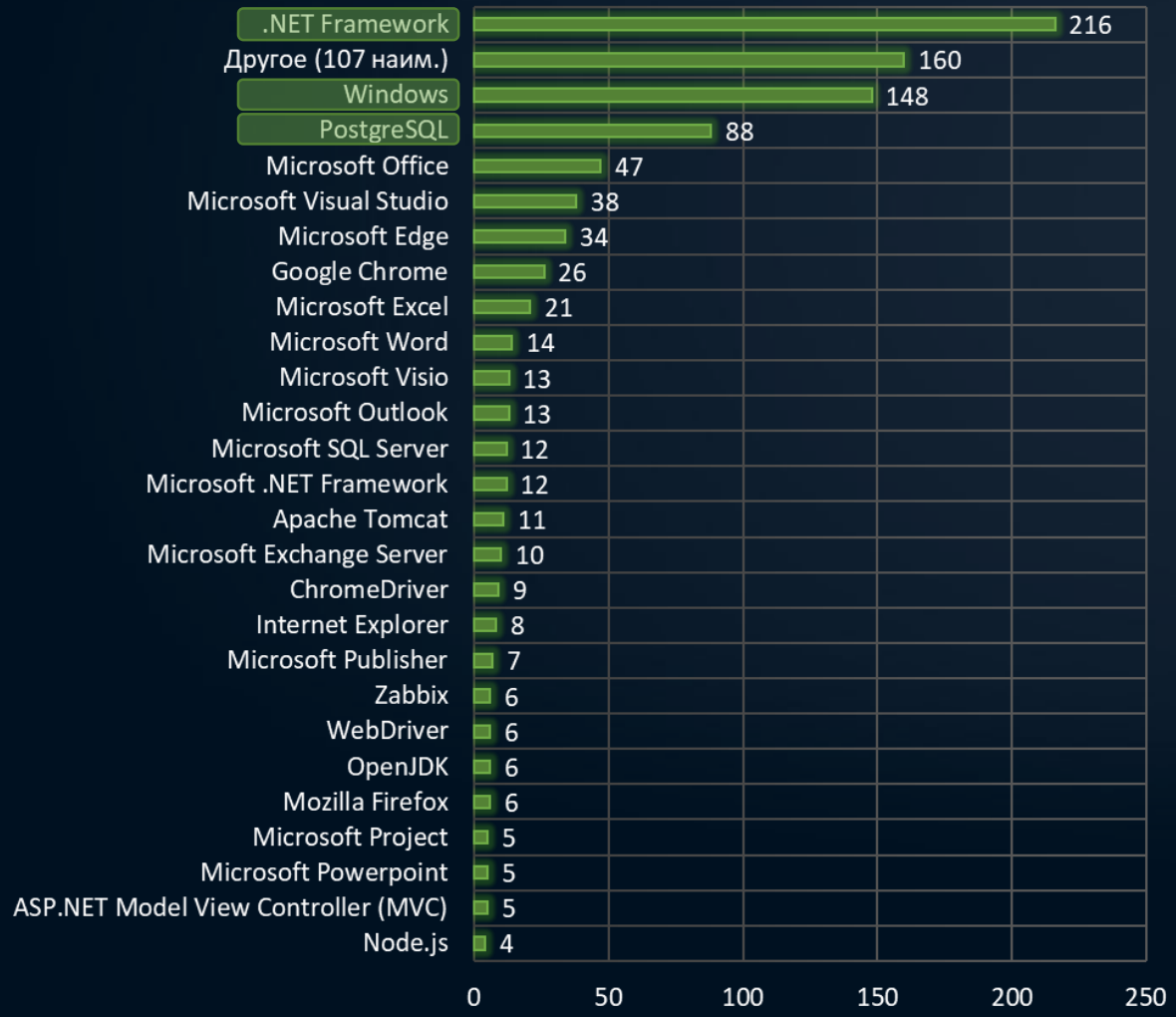
Выводы:

- **не выявлено признаков недекларированных возможностей**
- **найдены признаки недекларированных возможностей, идентифицировать назначение которых не удалось**
- **найдены признаки недекларированных возможностей**

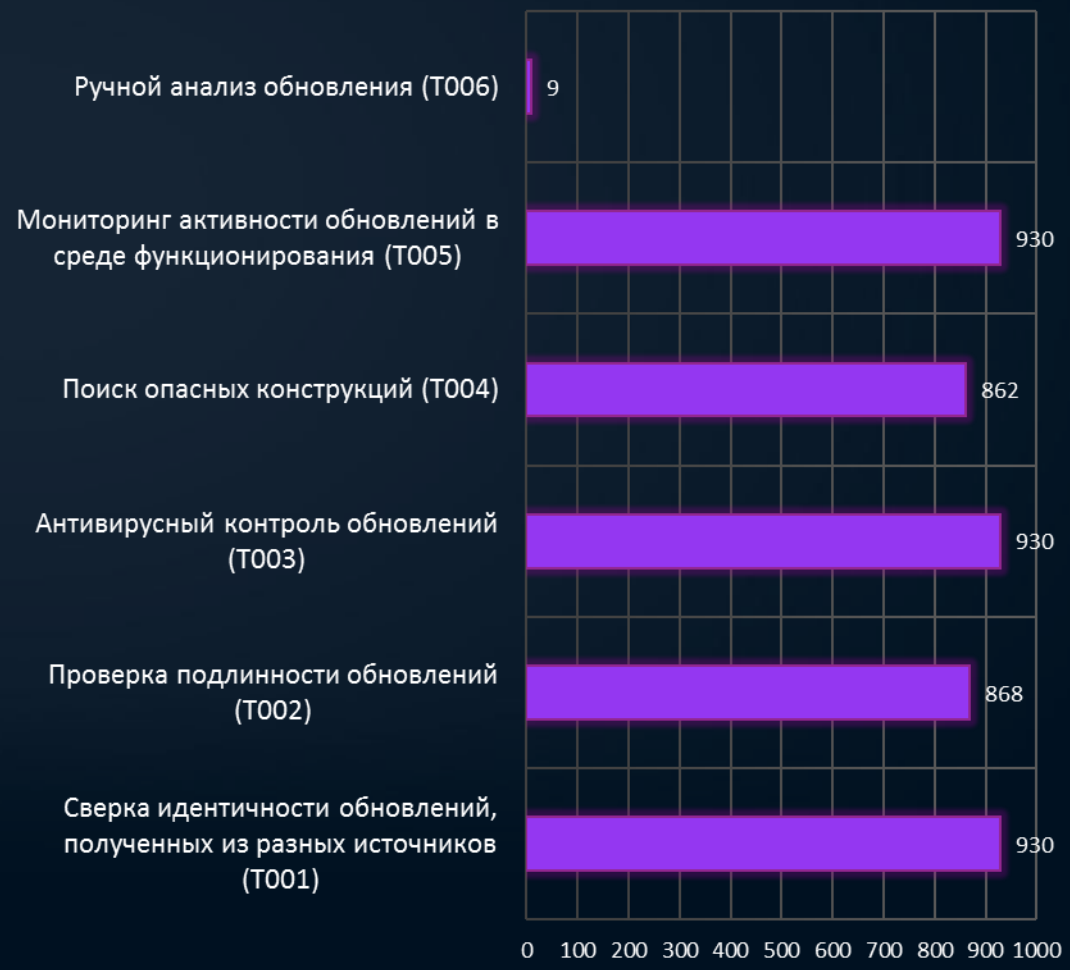
Результаты тестирования ПО

930

Тестируемое ПО



Проводимые тесты



РАБОЧАЯ ГРУППА ПО ТЕСТИРОВАНИЮ ОБНОВЛЕНИЙ

Верификация результатов тестирования

Размещение результатов тестирования обновлений

Тестирование обновлений

СБЕР

ИНТЕР РАО

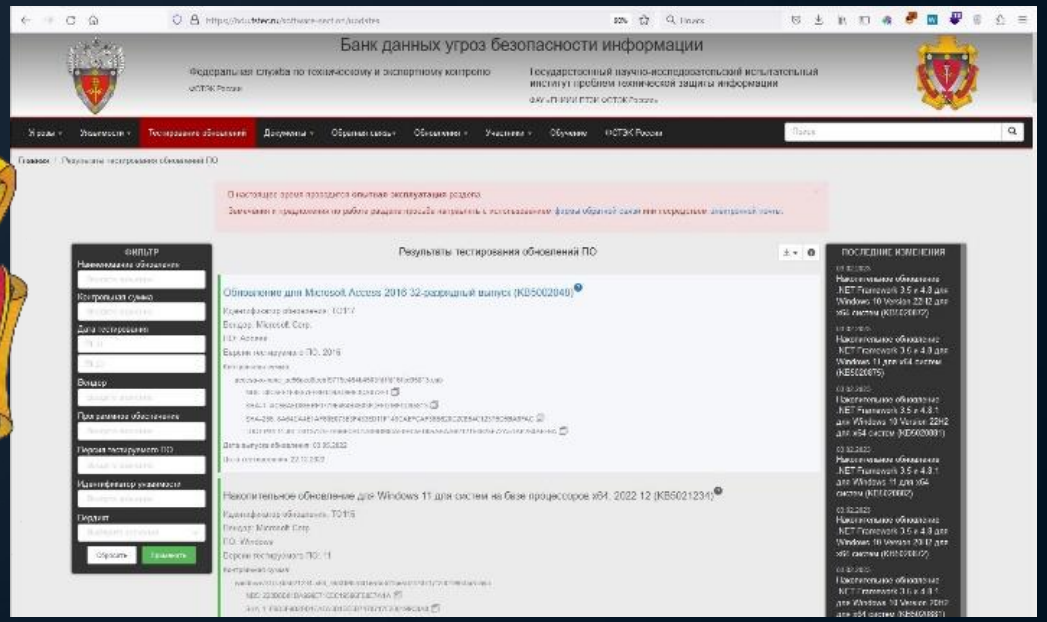
ДЕПАРТАМЕНТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ ГОРОДА МОСКВЫ

ИСП РАН

positive technologies

Рабочая группа

ГНИИИ ПТЗИ ФСТЭК России



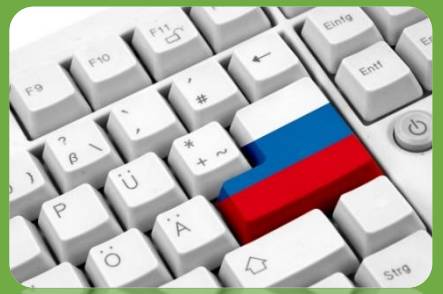
БДУ ФСТЭК России

АКТУАЛЬНОСТЬ СОЗДАНИЯ БДУ АСУ ТП

Значительный рост числа компьютерных

- За **2023** год в мире зафиксировано **более 600 атак** на промышленные предприятия, что на **87 % больше**, чем в **2022** году
- Групп программ-вымогателей, нацеленных на промышленные предприятия, стало **на 35% больше**
- Доля компонентов АСУ ТП, на которых заблокированы вредоносные программы, составляет в России **более 35%**.

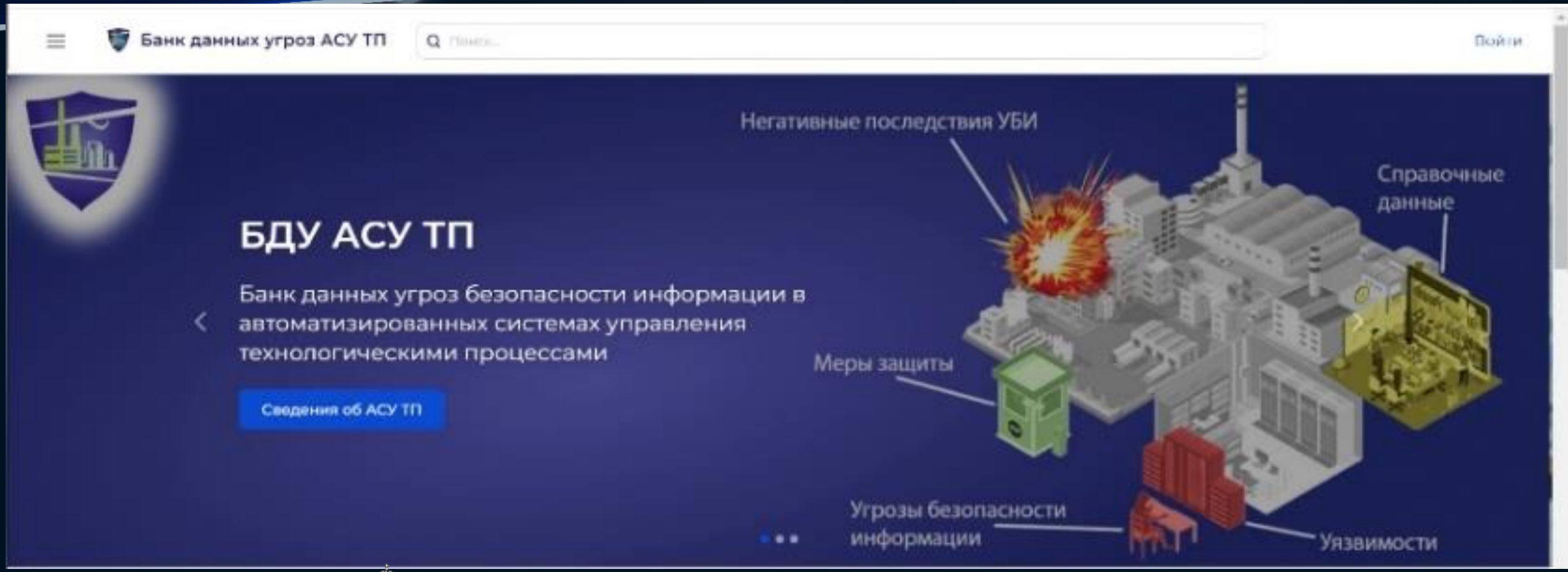
Импортозамещение



- **Существенное возрастание потребности в исследованиях защищенности** отечественных средств промышленной автоматизации (ПЛК, SCADA-систем).

ЦЕЛЬ СОЗДАНИЯ

Совершенствование системы защиты информации АСУ ТП, повышение качества их ПО



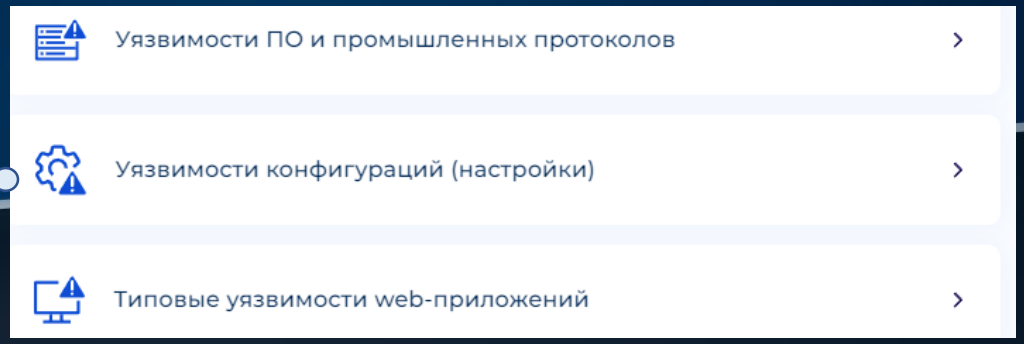
Участники создания:

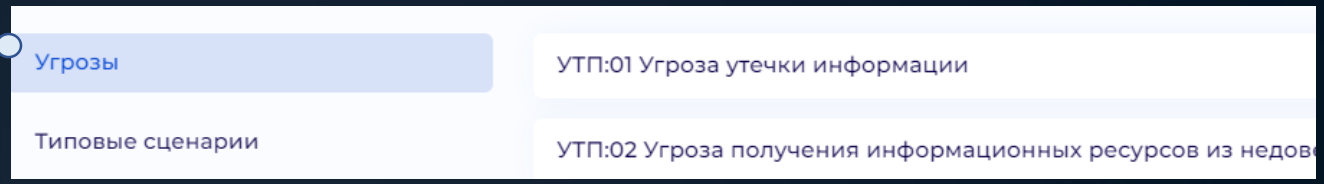
TELECOM INTEGRATION

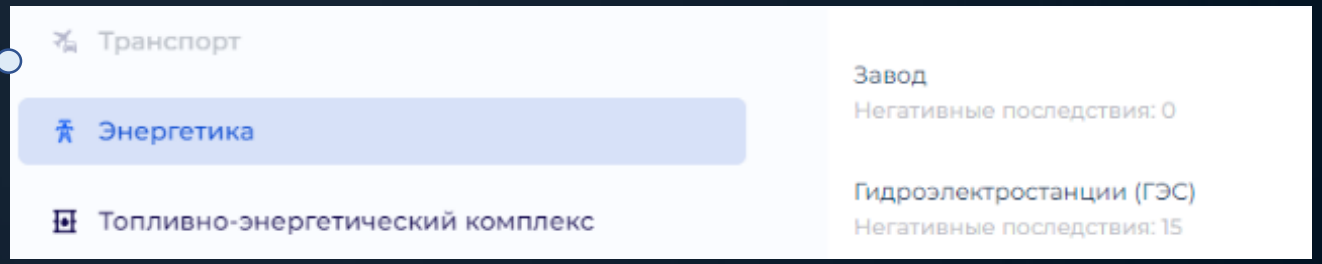
Ростелеком Солар

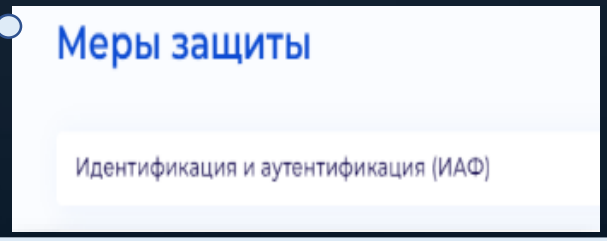
ОСНОВНЫЕ МОДУЛИ БДУ АСУ ТП

1. Модуль уязвимостей
2. Модуль угроз
3. Модуль негативных последствий
4. Модуль мер защиты
5. Модуль справочных данных
6. Модуль инфографики









ИССЛЕДОВАТЕЛЬСКИЙ СТЕНД

Задачи

- выявление уязвимостей
- оценка угроз и способов их реализации
- оценка защищенности новых технологий АСУ ТП (виртуализация, цифровые двойники)
- оценка потенциальных негативных последствий
- выбор мер защиты
- оповещение
- тестирование специалистов по ЗИ в АСУ ТП

БДУ АСУ ТП. СЕРВИСЫ И КОНТЕНТ

Сервисы БДУ АСУ ТП

Публикация новостей

Выгрузка сведений

Инфографика

Тестирование

Личные кабинеты

Целевое информирование

Рейтинг исследователей

Предоставление доступа к стенду

Контент БДУ АСУ ТП

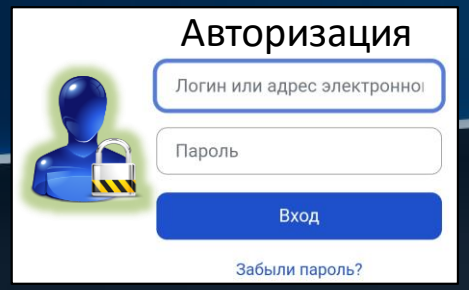
- Уязвимости
- Угрозы
- Меры защиты
- Негативные последствия
- Справочные сведения
- Новости

https://bduasutp.fstec.ru

БДУ АСУ ТП. Алгоритм работы

Пользователи

- Исследователи
- Разработчики АСУ ТП
- Владельцы АСУ ТП
- Интеграторы систем защиты
- Специалисты испытательных лабораторий
- Обучаемые специалисты



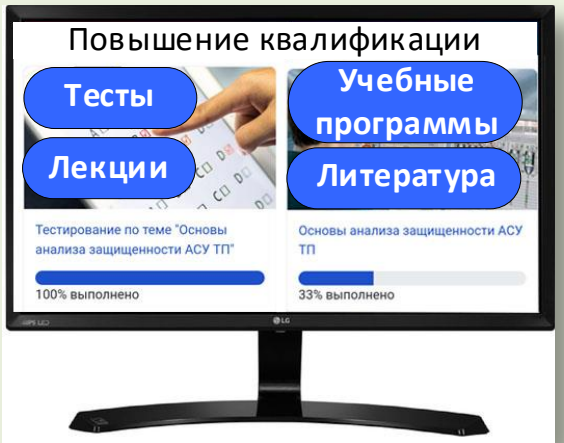
Выбор режима работы

1 Тестирование

2 Получение информации

3 Исследования

LMS moodle



Выбор объекта исследования

База данных раздела БДУ

Проведение исследований

Формирование отчета об исследовании

ЭФФЕКТЫ СОЗДАНИЯ РЕСУРСА АСУ ТП

Повышение защищенности

Повышение защищенности критической инфраструктуры Российской Федерации и эффективности систем обеспечения безопасности за счет централизованного проведения комплекса исследований угроз и уязвимостей в кооперации исследователей безопасности, разработчиков, владельцев и операторов АСУ, а также оперативного информирования пользователей о выявляемых угрозах, уязвимостях и необходимых мерах защиты

Информирование об угрозах

Накопление в отечественном ресурсе знаний о способах реализации и лучших практиках выявления и предотвращения угроз безопасности информации в интересах своевременного принятия мер защиты при проектировании и эксплуатации АСУ ТП в различных сферах деятельности

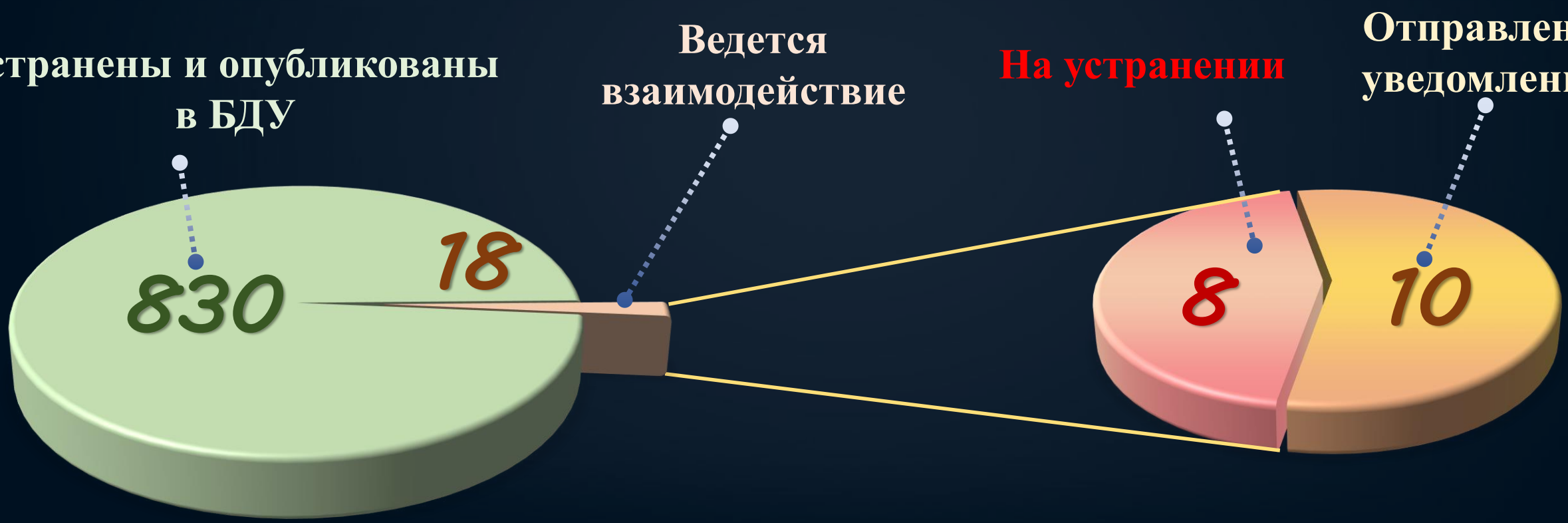
Импортозамещение

Создание условий для безопасного перехода субъектов КИИ на отечественные средства промышленной автоматизации путем реализации технологии обеспечения конструктивной безопасности с учетом результатов исследований защищенности разрабатываемых элементов АСУ ТП

Повышение квалификации персонала

Повышение уровня квалификации персонала, ответственного за реализацию мероприятий по обеспечению безопасности КИИ, за счет созданной системы тестирования специалистов в области защиты информации

Проведены работы по устранению 830 уязвимостей «нулевого дня»



Среднее время реагирования разработчика:

5 ДНЕЙ

Среднее время устранения уязвимости:

30 ДНЕЙ

РАЗВИТИЕ ОТЕЧЕСТВЕННЫХ ИНФОРМАЦИОННЫХ РЕСУРСОВ, СОДЕРЖАЩИХ СВЕДЕНИЯ ОБ УГРОЗАХ БЕЗОПАСНОСТИ ИНФОРМАЦИИ И УЯЗВИМОСТЯХ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

СПАСИБО ЗА ВНИМАНИЕ!

Начальник управления ГНИИИ ПТЗИ ФСТЭК России
Александр Суховерхов