



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

1

**БАНК ДАННЫХ УГРОЗ
БЕЗОПАСНОСТИ ИНФОРМАЦИИ ФСТЭК РОССИИ**



2

**БАНК ДАННЫХ УГРОЗ
БЕЗОПАСНОСТИ ИНФОРМАЦИИ АСУ ТП**



новинка

Банк данных угроз безопасности информации
Федеральная служба по техническому и экспортному контролю
ФСТЭК России
Государственный научно-исследовательский испытательный институт проблем технической защиты информации
ФАН И НИИМ ПТЗИ ФСТЭК России

Угрозы • Уязвимости • Тестирование обновлений • Документы • Обратная связь • Обновления • Участия • Обучение • ФСТЭК России

Главная • Список угроз

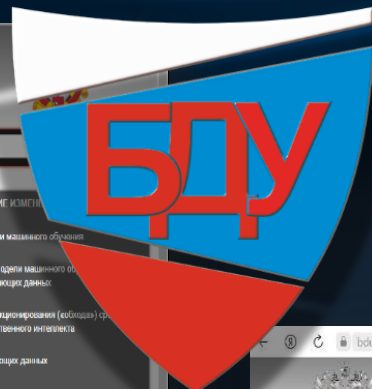
Фильтрация: Контекстный поиск по названию угрозы, Источники угроз, Последствия реализации угрозы, Нарушение конфиденциальности, Нарушение целостности, Нарушение доступности.

Выводить по: 10, 20, 50, 100. Элементы с 1 по 10 из 222

УБИ_001	Угроза автоматического распространения вредоносного кода в грид-системе
УБИ_002	Угроза агрегирования данных, передаваемых в грид-системе
УБИ_003	Угроза использования слабостей криптографических алгоритмов и уязвимостей в программном обеспечении их реализации
УБИ_004	Угроза аппаратного сброса пароля BIOS
УБИ_005	Угроза внедрения вредоносного кода в BIOS
УБИ_006	Угроза внедрения кода или данных
УБИ_007	Угроза воздействия на программы с высокими привилегиями
УБИ_008	Угроза восстановления или повторного использования аутентификационной информации
УБИ_009	Угроза восстановления производимой уязвимой версии BIOS
УБИ_010	Угроза выхода процесса за пределы виртуальной машины

Последние изменения: УБИ_222 Угроза парковки модуля мультимедийного обучения (16.12.2020), УБИ_221 Угроза модификации модели машинного обучения (отравления) обучающих данных (16.12.2020), УБИ_220 Угроза нарушения функционирования (сбои/падения) серверов (16.12.2020), УБИ_219 Угроза хищения обучающих данных (16.12.2020), УБИ_218 Угроза раскрытия информации о модели машинного обучения (16.12.2020), УБИ_217 Угроза использования оптимизированного древовидного источника объектов программного обеспечения (11.02.2020), УБИ_216 Угроза получения несанкционированного доступа к приложениям, установленным на Smart-картах (15.11.2019), УБИ_215 Угроза несанкционированного доступа к системе при помощи спящих сервисов (15.11.2019), УБИ_214 Угроза несанкционированного выполнения и реализации компонентов информационной (автоматизированной) системы (в том числе средствами защиты информации) на объектах безопасности информации (15.11.2019), УБИ_213 Угроза обхода многофакторной аутентификации (08.02.2019).

Угрозы: 222 | Уязвимости: 4191 | Последнее обновление: 08.02.2022
ФАН И НИИМ ПТЗИ ФСТЭК России



Уязвимости >54000

Банк данных угроз безопасности информации
Федеральная служба по техническому и экспортному контролю
ФСТЭК России
Государственный научно-исследовательский испытательный институт проблем технической защиты информации
ФАН И НИИМ ПТЗИ ФСТЭК России

Угрозы • Уязвимости • Тестирование обновлений • Документы • Обратная связь • Обновления • Участия • Обучение • ФСТЭК России

Главная • Список уязвимостей

Фильтрация: Контекстный поиск по названию уязвимости, Производитель ПО, Тип ПО, Программное обеспечение, Аппаратная платформа, Версия ПО, Статус уязвимости, Доп. параметры, Диагност. дат, Год добавления.

Выводить по: 10, 20, 50, 100. Страница 1. Элементы с 1 по 10 из 52538

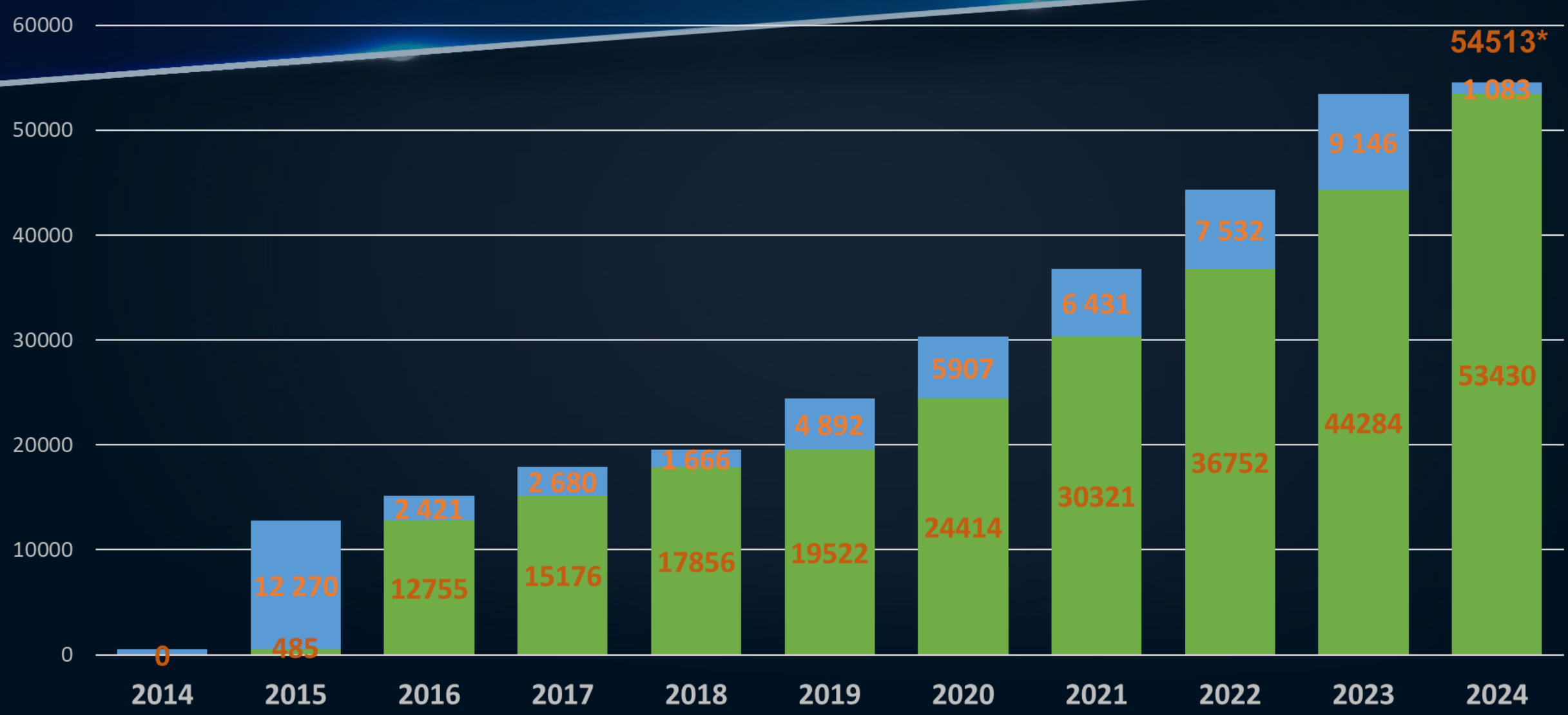
BDU-2023-08254	Уязвимость средства защиты Fortinet FortiClient для операционной системы Mac, связанная с загрузкой кода без проверки его целостности, позволяющая нарушителю повысить свои привилегии	11.04.2023
BDU-2023-08253	Уязвимость облачного API шлюза Tux, связанная с неприятием мер по защите структуры запроса SQL, позволяющая нарушителю выполнить произвольные SQL-запросы	07.11.2023
BDU-2023-08252	Уязвимость инструментов для разработки программного обеспечения Intel Data Center Manager SDK, связанная с нарушением механизма защиты данных, позволяющая нарушителю повысить свои привилегии	14.11.2023
BDU-2023-08251	Уязвимость программной платформы для удаленного контроля и управления зданиями Honeywell ProWatch, связанная с ошибками обработки данных, позволяющая нарушителю повысить свои привилегии	17.11.2023
BDU-2023-08250	Уязвимость программного обеспечения для форумов Flarum, связанная с недостаточной проверкой поступающих запросов, позволяющая нарушителю осуществить SSRF-атаку	16.08.2023
BDU-2023-08249	Уязвимость компонента Koko системы аудита безопасности эксплуатации и обслуживания JumpServer, позволяющая нарушителю обойти процесс аутентификации	27.09.2023
BDU-2023-08248	Уязвимость интерфейса WEB CLI (компонент koko) системы аудита безопасности эксплуатации и обслуживания JumpServer, позволяющая нарушителю выполнить произвольные команды	27.09.2023
BDU-2023-08247	Уязвимость агента универсальной системы мониторинга Zabbix, позволяющая нарушителю выполнить произвольный код	11.09.2023
BDU-2023-08246	Уязвимость модуля zabbix/collector универсальной системы мониторинга Zabbix, позволяющая нарушителю выполнить произвольный код	11.09.2023

Последние изменения: Уязвимость средства защиты Fortinet FortiClient для операционной системы Mac, связанная с загрузкой кода без проверки его целостности, позволяющая нарушителю повысить свои привилегии (29.11.2023), Уязвимость облачного API шлюза Tux, связанная с неприятием мер по защите структуры запроса SQL, позволяющая нарушителю выполнить произвольные SQL-запросы (29.11.2023), Уязвимость инструментов для разработки программного обеспечения Intel Data Center Manager SDK, связанная с нарушением механизма защиты данных, позволяющая нарушителю повысить свои привилегии (29.11.2023), Уязвимость программной платформы для удаленного контроля и управления зданиями Honeywell ProWatch, связанная с ошибками обработки данных, позволяющая нарушителю повысить свои привилегии (29.11.2023), Уязвимость программного обеспечения для форумов Flarum, связанная с недостаточной проверкой поступающих запросов, позволяющая нарушителю осуществить SSRF-атаку (29.11.2023), Уязвимость компонента Koko системы аудита безопасности эксплуатации и обслуживания JumpServer, позволяющая нарушителю обойти процесс аутентификации (29.11.2023), Уязвимость интерфейса WEB CLI (компонент koko) системы аудита безопасности эксплуатации и обслуживания JumpServer, позволяющая нарушителю выполнить произвольные команды (29.11.2023), Уязвимость агента универсальной системы мониторинга Zabbix, позволяющая нарушителю выполнить произвольный код (29.11.2023), Уязвимость модуля zabbix/collector универсальной системы мониторинга Zabbix, позволяющая нарушителю выполнить произвольный код (29.11.2023).

Угрозы 222

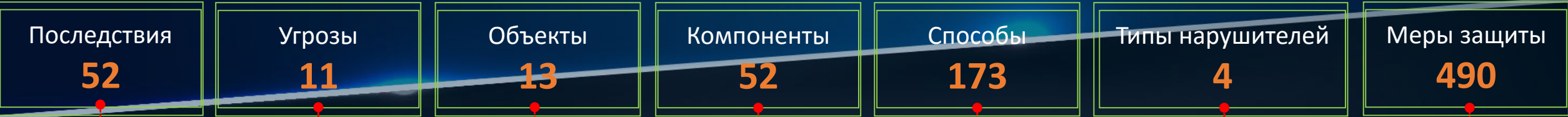
<https://bdu.fstec.ru>

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



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 неполной проверкой 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 оперативной памяти)
- 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 умолчанию)
- СП.2.9 Использование недостатков конфигурации, связанных с отсутствием проверки сертификата сети (для беспроводной связи)
- СП.2.10 Использование недостатков конфигурации сетевого оборудования, связанных с отсутствием или некорректной настройкой трафика

РАЗДЕЛ ТЕСТИРОВАНИЯ ОБНОВЛЕНИЙ БДУ ФСТЭК РОССИИ

bdu.fstec.ru/software-section/updates

- Тестирование обновлений
- Документы ▾
- Обратная связь ▾
- Обновления ▾
- Участники ▾
- Обучение
- ФСТЭК России

ФИЛЬТР

Наименование обновления

Контрольная сумма

Дата тестирования

Дата выпуска обновления

Вендор

Программное обеспечение

Версия тестируемого ПО

Идентификатор уязвимости

Вердикт

1 2 3

Результаты тестирования обновлений ПО

Накопительное обновление для Windows 10 21H2 для систем на базе процессоров x64, 2022 11 (KB5019959) [?]

Идентификатор обновления: TO18

Вендор: Microsoft Corp.

ПО: Windows

Версии тестируемого ПО: 10 21H2

Контрольная сумма:

 windows10.0-kb5019959-x64_eac276bf7657830a8645dd99a36e5c1c3bd370e8.cab

 MD5:89A6656B405A35E363DEA65315C2EA89

 SHA-1:EAC276BF7657830A8645DD99A36E5C1C3BD370E8

 SHA-256:80B4245B1F293AAA4AA2C306C07C4F5FF9FA9C8DEC3ED7C9C0F1F23B61C8C700







 ГОСТ 34.11:84C4E4AD4AAE6868BB68DDB9264CC88ED899F7931950F68964F129CB20068C80

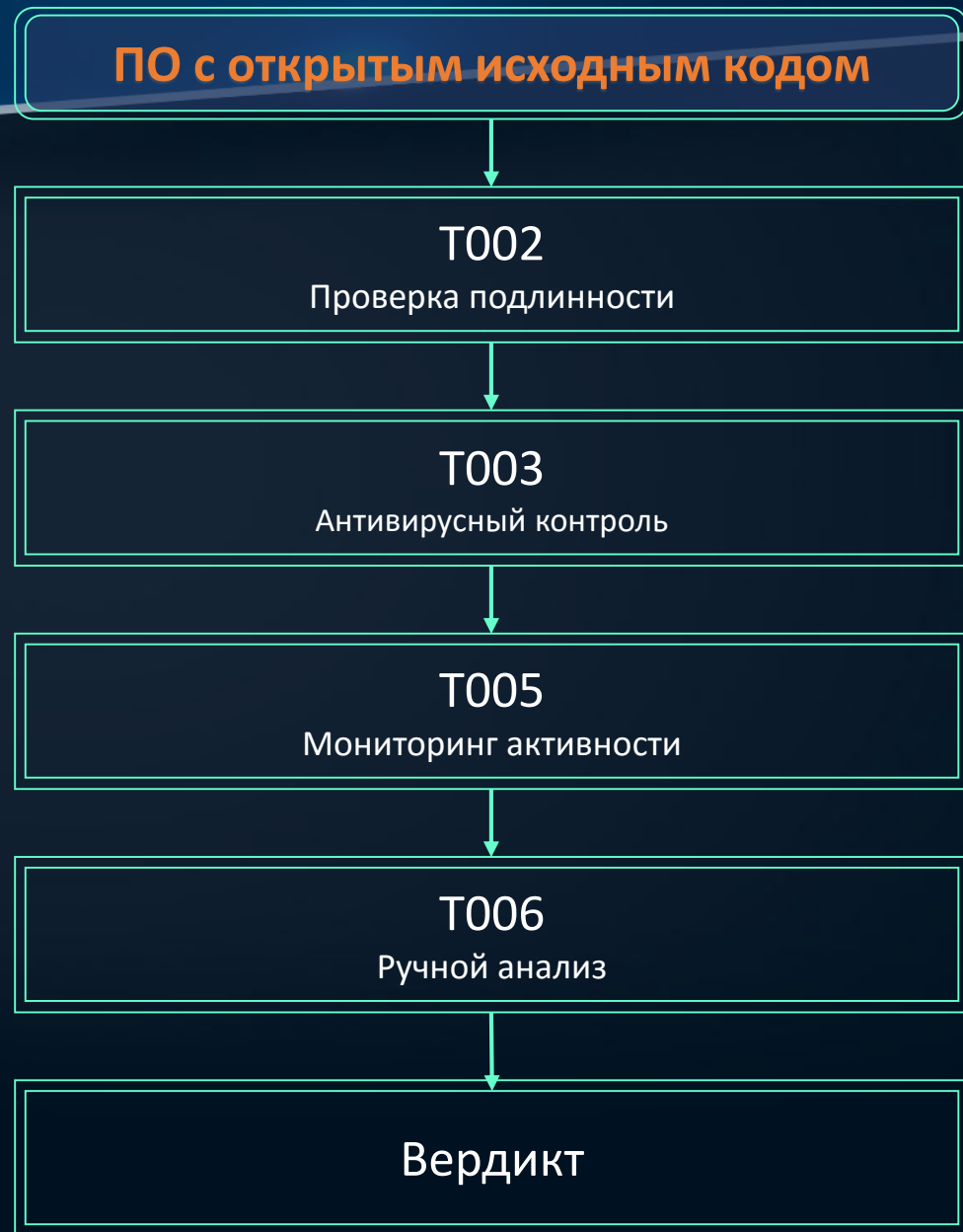
Дата выпуска обновления: 08.11.2022

Дата тестирования: 10.11.2022 - 12.11.2022

- 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**



-  **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**



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 недеklarированных возможностей

T002

Выводы:

- установлена подлинность обновлений
- обновления не прошли проверку подлинности

Имя проверяемого файла:
D:\Загрузка\mso-x-none_79b37d96eeb001954e9f1d7d8dee2641c89bfde3.cab

Обзор...

Алгоритм хэша:
Расчет контрольной суммы

Расчитанная контрольная сумма совпадает с введенной

OK

Расчитанная контрольная сумма
CF33136832ACF42D2927587176BA2A030A75A33C97783A171937C565BF11A1A9

Алгоритм контрольной суммы
GOST R 34.11-2012/256

Расчитать

Введите контрольную сумму для проверки:
CF33136832ACF42D2927587176BA2A030A75A33C97783A171937C565BF11A1A9

Проверить

Закреть

T003

Проверка

Важность: 📌 ⚠️ ❗

Период: Все < 05.11.2020 > 07.02.2024 >

Дата события	Объект	Результат	Событие
▼	Выборочная проверка: начата сегодня, 06.02.2024 15:12:36, закончена сегодня, 06.02.2024 15:12:36		
📌	Сегодня, 06.02.2024 15:12:36	Задача завершена	Задача завершена
📌	Сегодня, 06.02.2024 15:12:36	Задача запущена	Задача запущена

Выводы:

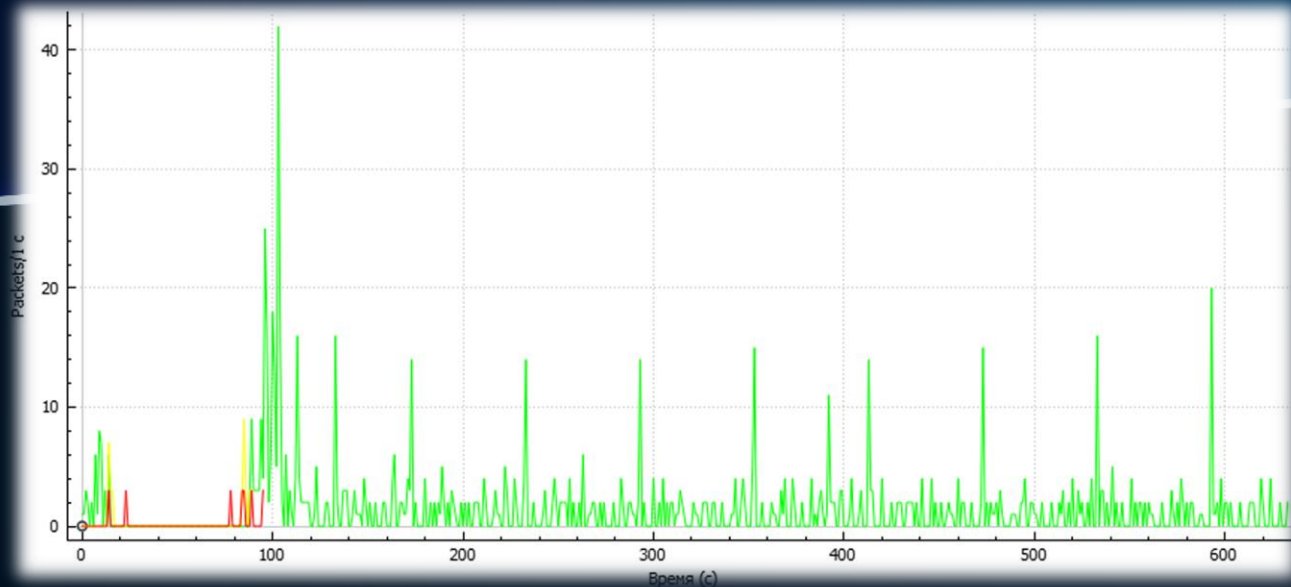
- не выявлены признаки вредоносной активности
- признаки вредоносной активности выявлены, сигнатура ВПО не определена
- признаки вредоносной активности выявлены, сигнатура ВПО определена

T004

The screenshot displays a list of detected vulnerabilities on the left and a corresponding code snippet on the right. The code snippet shows a buffer overflow in a C++ file named LogWriterFile.cpp. The vulnerability is identified as a 'BUFFER_OVERFLOW.STRING' where a buffer of size 260 is accessed with index 1024. The code snippet shows the relevant lines of code, including the definition of the buffer and the function call that causes the overflow.

Выводы:

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



scanOVAL ГЛАВНОЕ СПРАВКА

Отображать: Все уязвимости C:\File.xml

Идентификатор уязвимости	Результат	Уровень...	Идентификатор уязвимости	Название уязвимости
BDU:2017-00220		Критический	CVE-2017-2925; apsb17-02	Уязвимость в Adobe Flash Player 24.0.0.186 и ниже (apsb17-02)
BDU:2017-00219		Критический	CVE-2017-2926; apsb17-02	Уязвимость в Adobe Flash Player 24.0.0.186 и ниже (apsb17-02)
BDU:2017-00218		Критический	CVE-2017-2927; apsb17-02	Уязвимость в Adobe Flash Player 24.0.0.186 и ниже (apsb17-02)
BDU:2017-00217		Критический	CVE-2017-2928; apsb17-02	Уязвимость в Adobe Flash Player 24.0.0.186 и ниже (apsb17-02)
BDU:2017-00216		Критический	CVE-2017-2930; apsb17-02	Уязвимость в Adobe Flash Player 24.0.0.186 и ниже (apsb17-02)
BDU:2017-00215		Критический	CVE-2017-2931; apsb17-02	Уязвимость в Adobe Flash Player 24.0.0.186 и ниже (apsb17-02)
BDU:2017-00214		Критический	CVE-2017-2933; apsb17-02	Уязвимость в Adobe Flash Player 24.0.0.186 и ниже (apsb17-02)
BDU:2017-00213		Критический	CVE-2017-2933; apsb17-02	Уязвимость в Adobe Flash Player 24.0.0.186 и ниже (apsb17-02)
BDU:2017-00212		Критический	CVE-2017-2934; apsb17-02	Уязвимость в Adobe Flash Player 24.0.0.186 и ниже (apsb17-02)
BDU:2017-00211		Критический	CVE-2017-2935; apsb17-02	Уязвимость в Adobe Flash Player 24.0.0.186 и ниже (apsb17-02)
BDU:2017-00210		Критический	CVE-2017-2936; apsb17-02	Уязвимость в Adobe Flash Player 24.0.0.186 и ниже (apsb17-02)
BDU:2017-00209		Критический	CVE-2017-2937; apsb17-02	Уязвимость в Adobe Flash Player 24.0.0.186 и ниже (apsb17-02)
BDU:2017-00208		Высокий	CVE-2017-2938; apsb17-02	Уязвимость в Adobe Flash Player 24.0.0.186 и ниже (apsb17-02)

Всего: 1700

Формировать по рискам | Загружать по рискам

Подробности

Идентификатор уязвимости: **BDU:2017-00209**

Уровень опасности уязвимости: **Критический**

OVAL: [oval:ru.almx-soft:windef:28974](#) (Версия-4)

Название уязвимости: Уязвимость в Adobe Flash Player 24.0.0.186 и ниже (apsb17-02)

Описание уязвимости: Adobe Flash Player 24.0.0.186 и ниже имеет уязвимость доступа к освобожденной памяти в ActionScript FileReference class. Успешная эксплуатация уязвимости может привести к выполнению произвольного кода.

Возможные меры по устранению уязвимости: Использование рекомендаций <https://helpx.adobe.com/security/products/flash-player/apsb17-02.html>

Ссылки на источники: CVE: [CVE-2017-2937](#)
Adobe: [apsb17-02](#)

Базовый вектор уязвимости: CVSS: AV:N/AC:L/Au:N/C/C/I/C/AC

Файл: C:\File.xml

© ФАУ «ГНИИИ ПТЭИ ФСТЭК России»

Мониторинг активности обновлений безопасности в среде тестирования предусматривает необходимость проведения:

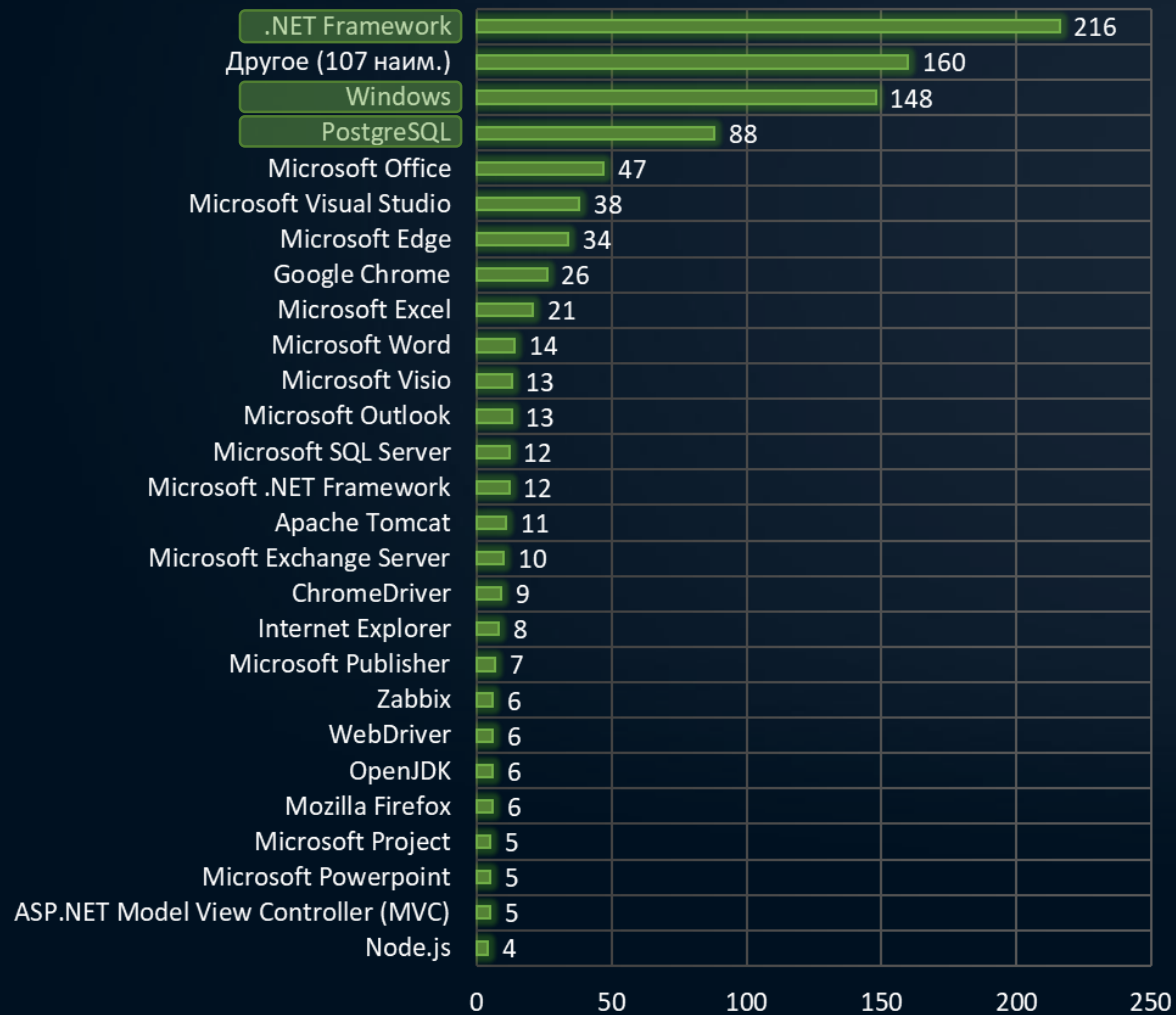
- анализа результатов выполнения системных вызовов обновленного ПО
- анализа получаемых и отправляемых обновленным ПО сетевых пакетов
- анализа состава файловой системы до и после установки обновления ПО
- сигнатурного поиска известных уязвимостей

Выводы:

- не выявлено признаков недеklarированных возможностей
- найлены признаки недеklarированных возможностей, идентифицировать назначение которых не удалось
- найлены признаки недеklarированных возможностей

930

Тестируемое ПО



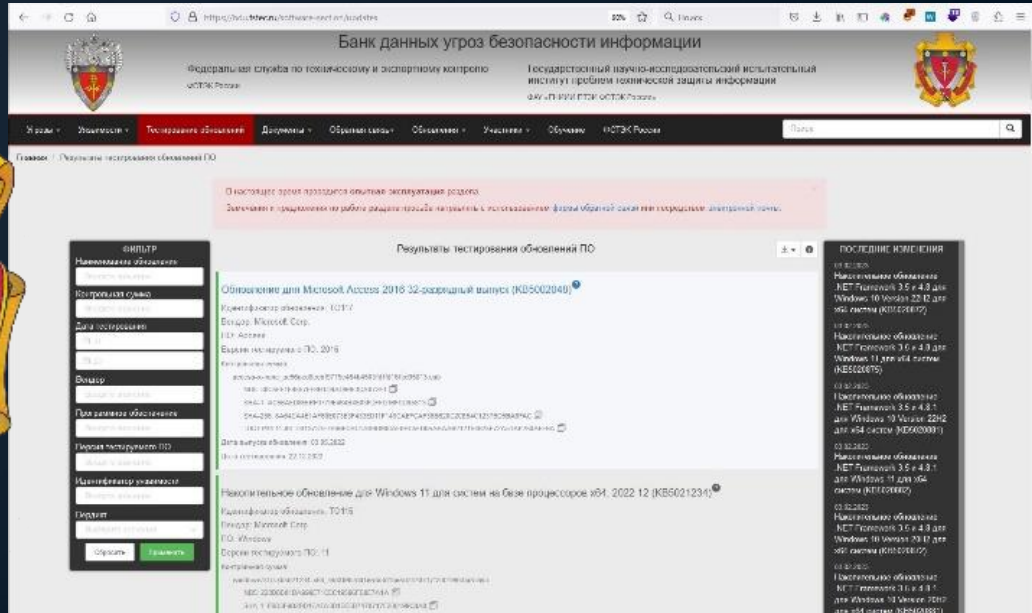
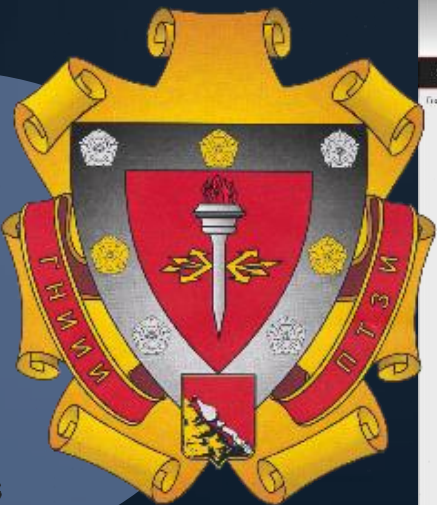
Проводимые тесты



✓ Верификация результатов тестирования

📢 Размещение результатов тестирования обновлений

🔧 Тестирование обновлений



Рабочая группа

ГНИИ ПТЗИ
ФСТЭК России

БДУ ФСТЭК России

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%**.

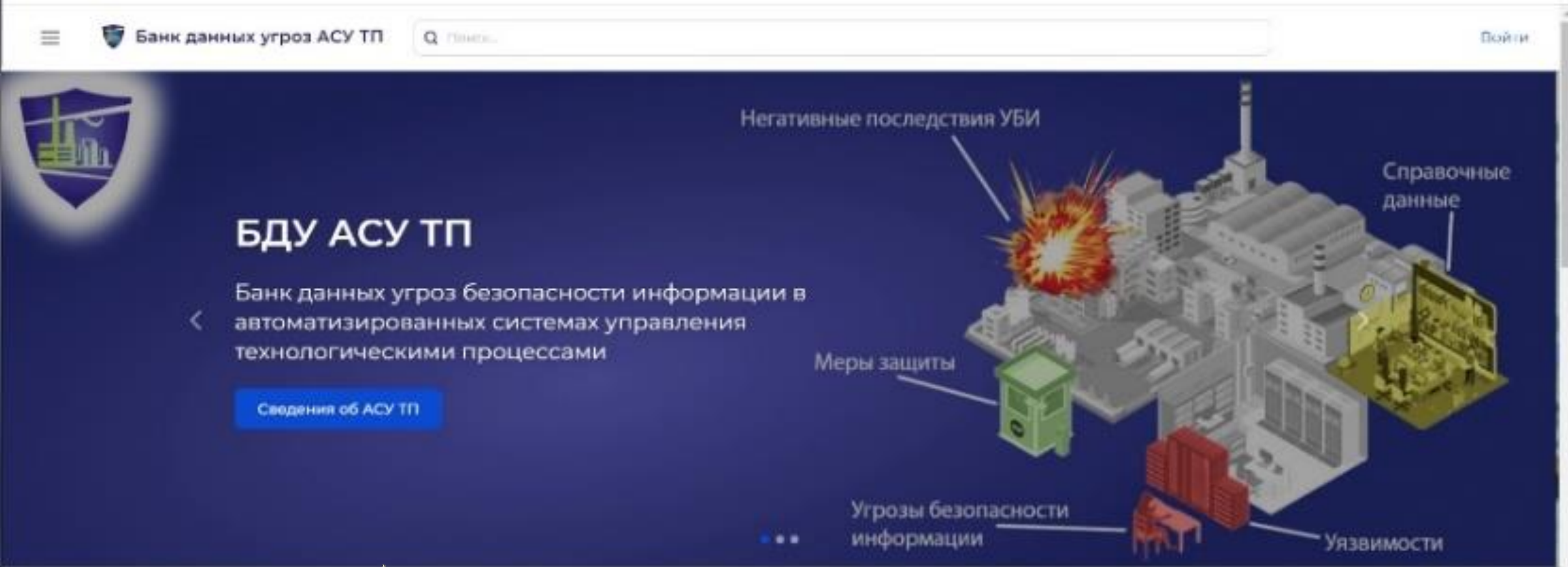
Импортозамещение



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

ЦЕЛЬ СОЗДАНИЯ

Совершенствование системы защиты информации АСУ ТП, повышение качества их ПО



Участники создания:



TELECOM
INTEGRATION



ОСНОВНЫЕ МОДУЛИ БДУ АСУ ТП

1 Модуль уязвимостей

- Уязвимости ПО и промышленных протоколов >
- Уязвимости конфигураций (настройки) >
- Типовые уязвимости web-приложений >

2 Модуль угроз

Угрозы

Типовые сценарии

УТП:01 Угроза утечки информации

УТП:02 Угроза получения информационных ресурсов из недов...

3 Модуль негативных последствий

Транспорт

Энергетика

Топливо-энергетический комплекс

Завод

Негативные последствия: 0

Гидроэлектростанции (ГЭС)

Негативные последствия: 15

4 Модуль мер защиты

Меры защиты

Идентификация и аутентификация (ИАФ)

5 Модуль справочных данных



6 Модуль инфографики

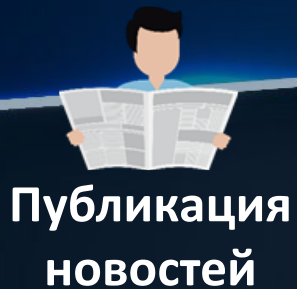


Задачи

- **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**



Сервисы БДУ АСУ ТП



Публикация новостей



Выгрузка сведений



Инфографика



Тестирование



Личные кабинеты



Целевое информирование



Рейтинг исследователей



Предоставление доступа к стенду

Контент БДУ АСУ ТП



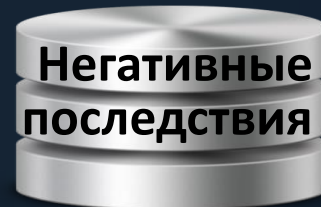
Уязвимости



Угрозы



Меры защиты



Негативные последствия



Справочные сведения



Новости



<https://bduasutp.fstec.ru>

Пользователи

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




Авторизация

Логин или адрес электронной почты

Пароль

Вход

Забыли пароль?



LMS moodle

Повышение квалификации

Тесты

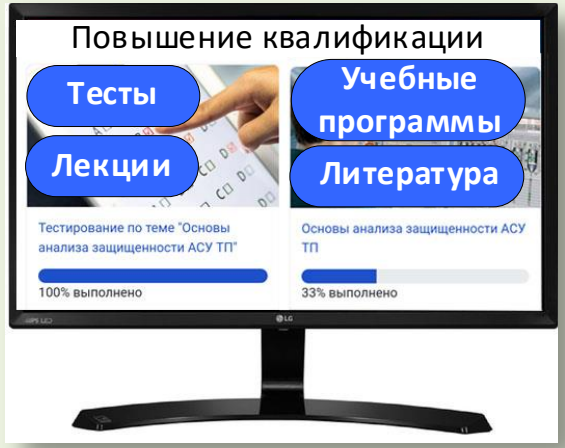
Учебные программы

Лекции

Литература

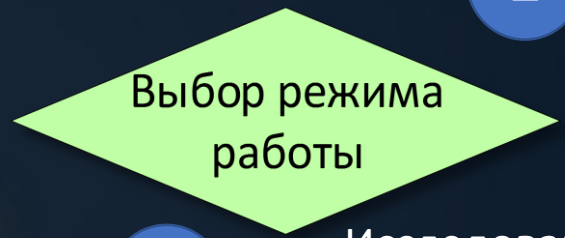
Тестирование по теме "Основы анализа защищенности АСУ ТП" 100% выполнено

Основы анализа защищенности АСУ ТП 33% выполнено




1 Тестирование

2 Получение информации




3 Исследования

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

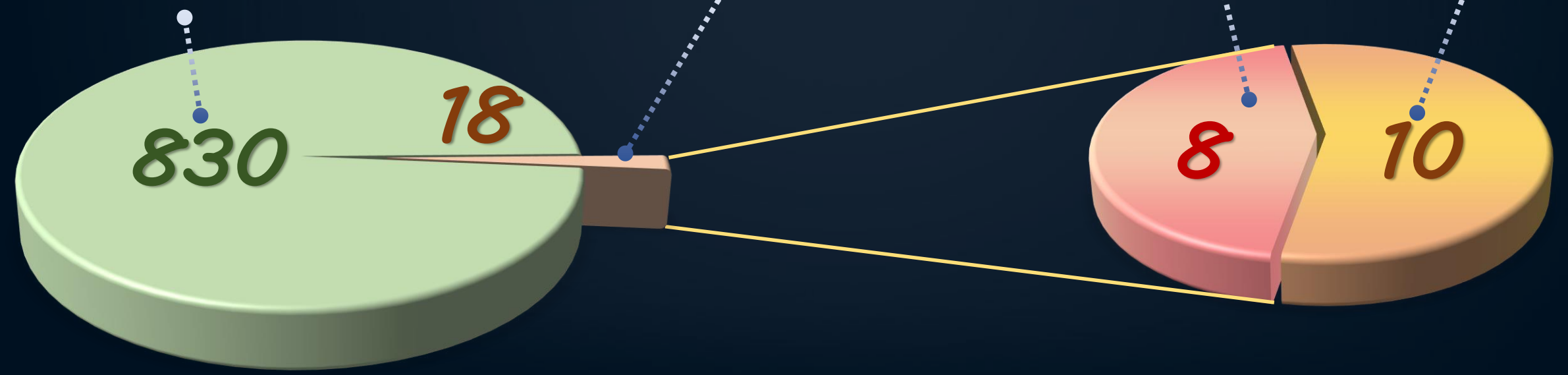
Проведены работы по устранению **830** уязвимостей «нулевого дня»

Устранены и опубликованы
в БДУ

Ведется
взаимодействие

На устранении

Отправлены
уведомления



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