

# Совершенствование банка данных угроз безопасности информации

---

Начальник управления ФАУ «ГНИИИ ПТЗИ ФСТЭК России»

Суховерхов Александр Сергеевич



# Банк данных угроз безопасности информации

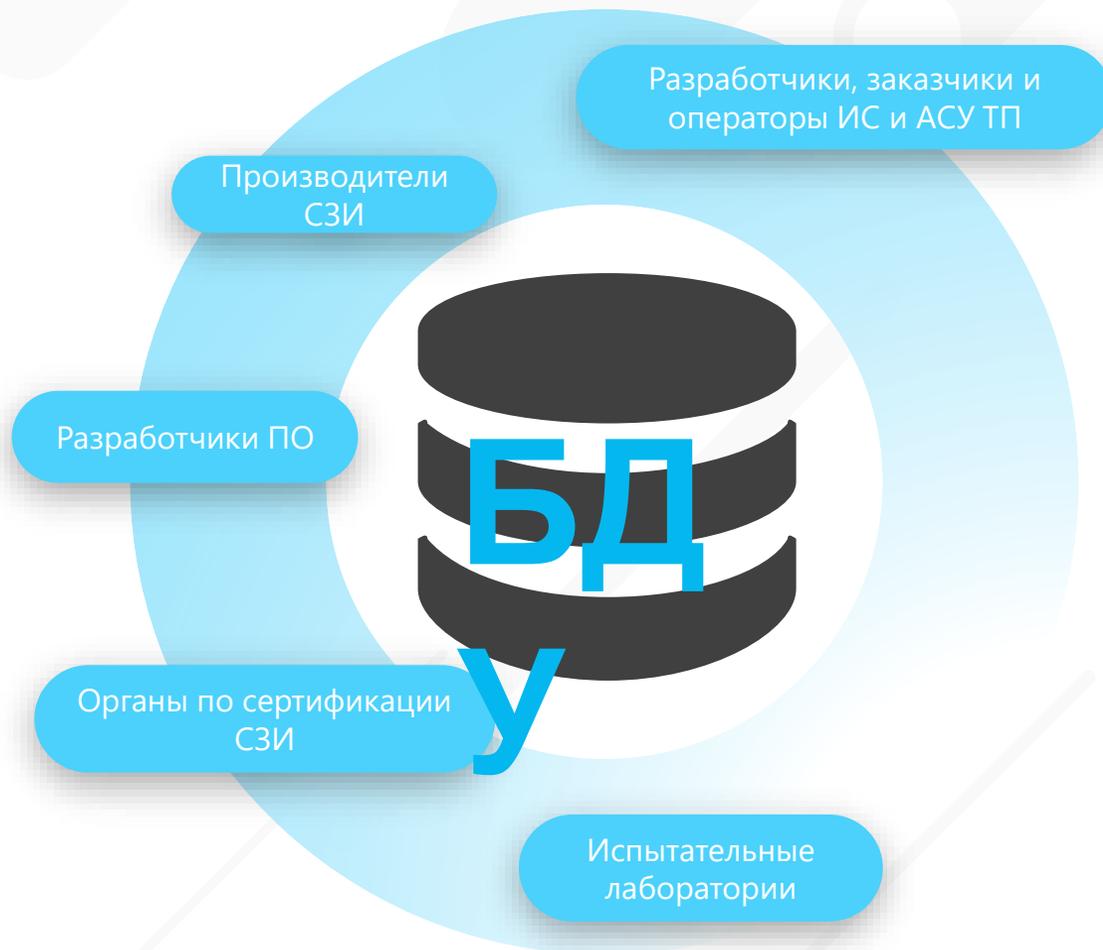
Единый отечественный информационный ресурс, содержащий сведения об угрозах и уязвимостях отечественных и зарубежных программных и программно-аппаратных средств

*определение и оценка угроз*

*выявление, анализ и устранение уязвимостей*

*производство и поддержание в актуальном состоянии СЗИ*

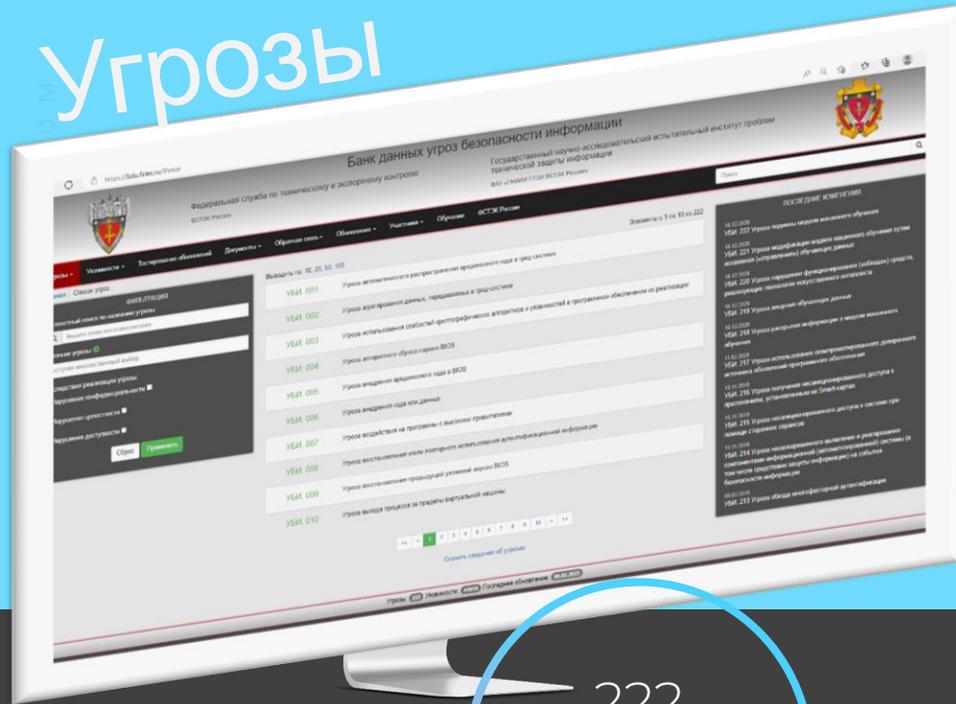
*Информационная и методическая поддержка*



# Банк данных угроз безопасности информации

Введен в эксплуатацию в 2015 году

Угрозы



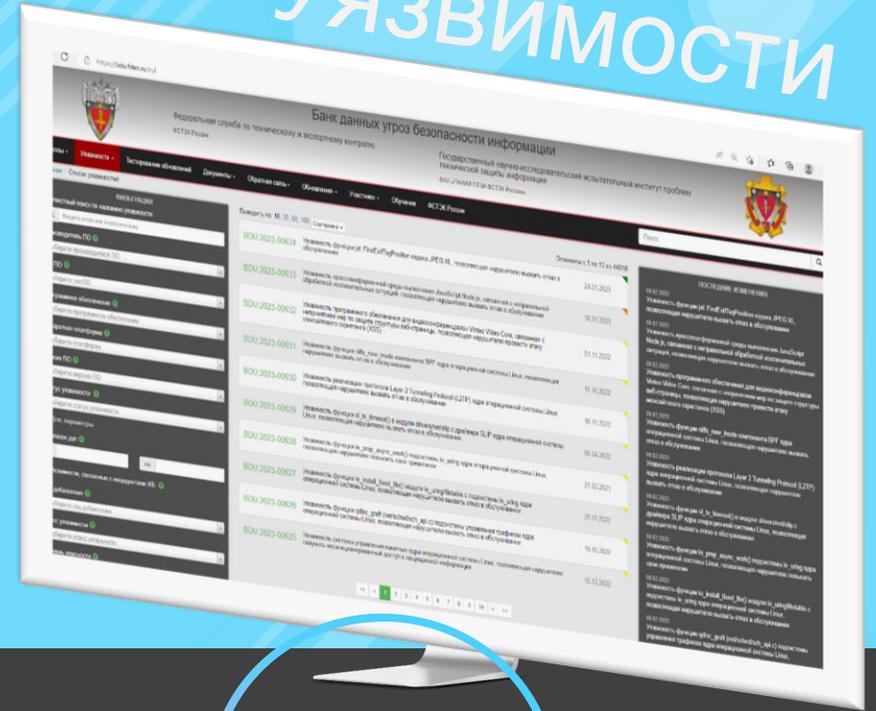
222  
записи



Адрес сайта БДУ:

<https://bdu.fstec.ru>

Уязвимости



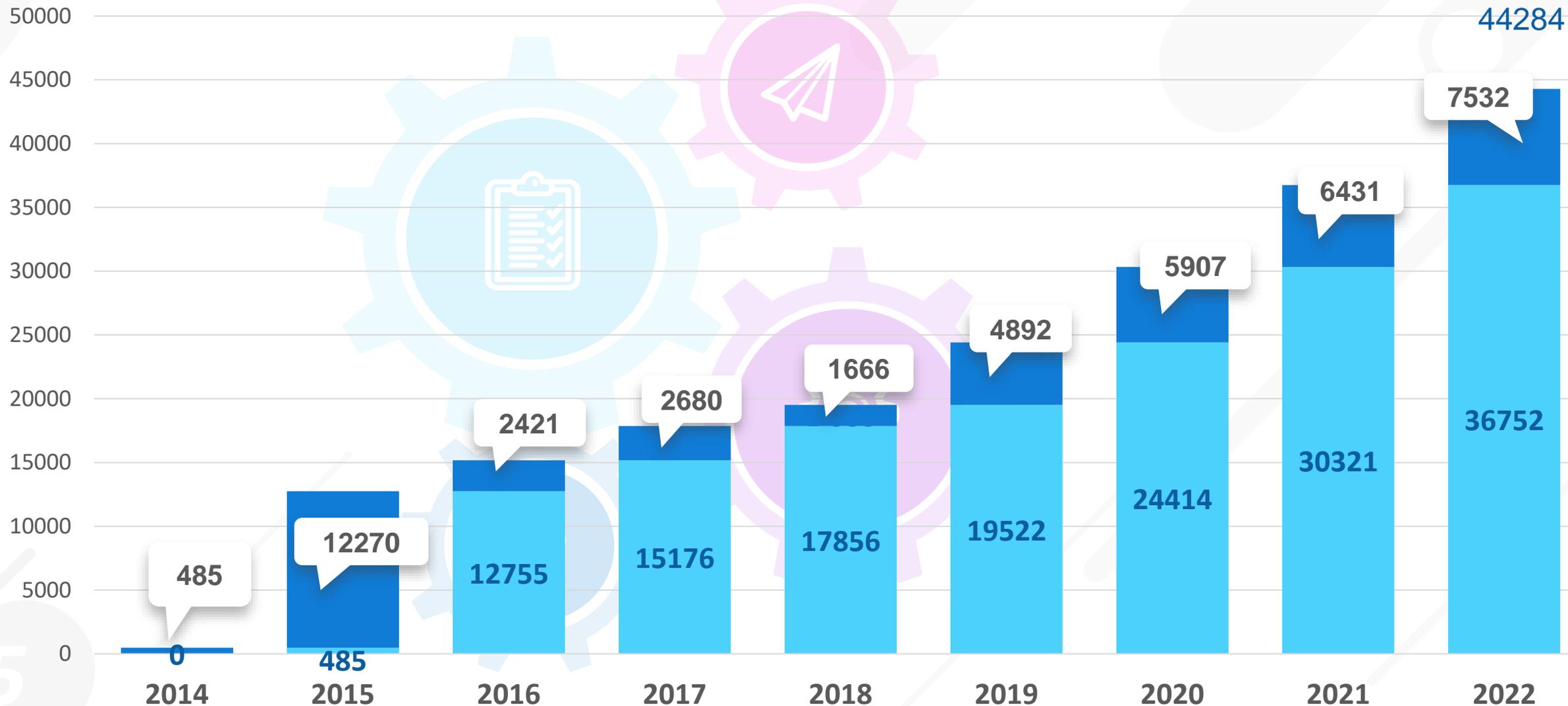
Боле  
44000  
записей



# Банк данных угроз безопасности информации

Характеристика накопленных сведений об уязвимостях.

Включение записей об уязвимостях программного обеспечения по годам



# Уязвимости программного обеспечения

## Сведения об уязвимости

8542: Уязвимость приложения для хранения фотографий Photo Station, связанная с ошибками управления привилегиями, позволяющая нарушителя повысить свои привилегии в системе и выполнить произвольный код

**Описание уязвимости** Уязвимость приложения для хранения фотографий Photo Station связана с ошибками управления привилегиями. Эксплуатация уязвимости может позволить нарушителю действующему пользователю повысить свои привилегии в системе и выполнить произвольный код

**Вендор** QNAP Systems, Inc.

**Наименование ПО** Photo Station

**Версия ПО** до 6.1.2  
до 6.0.22  
до 5.7.18  
до 5.4.15  
до 5.2.14

**Тип ПО** Система средств, Система программного средства

**Имя системы и аппаратные платформы** Данные уточняются

**Тип ошибки** Недостаточная проверка валидных данных, Небезопасное управление привилегиями

**Идентификатор типа ошибки** CVE-20  
CVE-200

**Класс уязвимости** Уязвимость кода

**Дата выявления** 03.09.2022

**Базовый вектор уязвимости** CVESS 2.0: AV/NA/CIAU/NC/CI/CAC  
CVESS 3.0: AV/NA/CIAU/NC/MS/CI/NE/ML/AM

**Уровень опасности уязвимости** Критический уровень опасности (Базовая оценка CVESS 2.0 составляет 10)  
Критический уровень опасности (Базовая оценка CVESS 3.0 составляет 10)

**Компенсационные меры по уязвимости** 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.

**Компенсационные меры:**

- отключение функции перенаправления портов;
- проверка учетной записи пользователя NAS на наличие наданных паролей и их соответствие парольной политике;
- регулярное создание резервных копий данных;
- настройка службы муQMProtocol на сервере критически NAS.

Для настройки службы муQMProtocol на сервере критически NAS необходимо выполнить следующие действия:

- 1) авторизоваться в службе муQMProtocol в качестве администратора;
- 2) отключить перенаправление портов (PNP) в разделе «МуQMP Configuration»;
- 3) включить DNS;
- 4) перейти в раздел «Published Services» и отменить выбор «Publish» для всех служб;
- 5) настроить муQMProtocol Link для обеспечения безопасного удаленного доступа к NAS через SmartURL;
- 6) ограничить доступ к NAS через SmartURL, в разделе «Ключевые Контроли» выбрать «Private или Customized».

Использование рекомендаций производителя:  
<https://www.qnap.com/na/en/security-advisory/ps-22-24>

**Статус уязвимости** Уязвимость исправлена

**Наличие эксплойта** Существует

**Способ эксплуатации** Нарушения авторизации

**Способ устранения** Обновление программного обеспечения

**Информация об уязвимости** Уязвимость устранена

**Ссылка на источник** <https://www.qnap.com/na/en/security-advisory/ps-22-24>

**Источники других систем оценки уязвимостей** CVE: CVE-2022-27593  
OVAL: OVAL-22-24

**Прочая информация** Данные уточняются

Компенсационные меры

## Информационные справки

ИНФОРМАЦИОННАЯ СПРАВКА  
от 15 сентября 2022 г.

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

ИНФОРМАЦИОННАЯ СПРАВКА  
от 9 сентября 2022 г.

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

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 удаленно, оказать воздействие на целостность защищаемой информации или вызвать отказ в обслуживании, путем отправки специально сформированных пакетов на интерфейсы в сети VPN.	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. Компенсационные 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: <a href="https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-vmanage-msg-serv-AqTup7vs">https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-vmanage-msg-serv-AqTup7vs</a>
BDU:2022-05391 CVE-2022-28199 Уязвимость драйвера mlx5 набора библиотек и драйверов для быстрой обработки пакетов frdk связана с неограниченными распределением ресурсов. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, вызвать отказ в обслуживании.	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. Компенсационные 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   include GigabitEthernet.*   rx_errors). Затронутый интерфейс можно восстановить с помощью команд: interface {название} shut no shut. Информация производителя: Для программных продуктов Cisco Systems, Inc. <a href="https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-mlx5-jbPCrQD8">https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-mlx5-jbPCrQD8</a> Для dpdk: <a href="https://git.dpdk.org/dpdk-stable/commit/?id=25c01bd32374b0c3bc260f3e3872408d74">https://git.dpdk.org/dpdk-stable/commit/?id=25c01bd32374b0c3bc260f3e3872408d74</a>

Отправлено порядка 200 информационных справок

# Банк данных угроз безопасности информации

Разделы сайта (2022-2023)

Уязвимости + Тестирование обновлений | Документы + Обратная связь + Обновления + Участники + Обучение | ФСТЭК России

Результаты тестирования обновлений ПО

Фильтр

Наименование обновления

Идентификатор обновления: TC117

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

Идентификатор уязвимости

Идентификатор обновления: TC116

Накопительное обновление для Windows 11 для систем на базе процессоров x64, 2022.12 (KB502123)

ScanOVAL

Идентификатор уязвимости	Результат	Уровень серьезности	Ссылка на описание	Платформа/версия
MS-03-2022-04302	Уязвимость	Высокий	MS-03-2022-04302	Linux
MS-03-2022-04303	Уязвимость	Высокий	MS-03-2022-04303	Linux
MS-03-2022-04304	Уязвимость	Высокий	MS-03-2022-04304	Linux
MS-03-2022-04305	Уязвимость	Высокий	MS-03-2022-04305	Linux
MS-03-2022-04306	Уязвимость	Высокий	MS-03-2022-04306	Linux
MS-03-2022-04307	Уязвимость	Высокий	MS-03-2022-04307	Linux
MS-03-2022-04308	Уязвимость	Высокий	MS-03-2022-04308	Linux
MS-03-2022-04309	Уязвимость	Высокий	MS-03-2022-04309	Linux
MS-03-2022-04310	Уязвимость	Высокий	MS-03-2022-04310	Linux
MS-03-2022-04311	Уязвимость	Высокий	MS-03-2022-04311	Linux
MS-03-2022-04312	Уязвимость	Высокий	MS-03-2022-04312	Linux

**БДУ ФСТЭК России**  
3 016 subscribers  
Новости БДУ ФСТЭК России  
bdu.fstec.ru

VIEW IN TELEGRAM

Preview channel

TELEGRAM-КАНАЛ

Раздел тестирования обновлений безопасности

Пополнение программ ScanOVAL

Список уязвимостей безопасности ПО

Новый раздел угроз

# Угрозы безопасности информации

## Методика оценки угроз безопасности информации



### Этап 1 – Определение негативных последствий

- ✓ Определение негативных последствий, которые могут наступить от реализации УБИ



### Этап 2 – Определение объектов воздействий

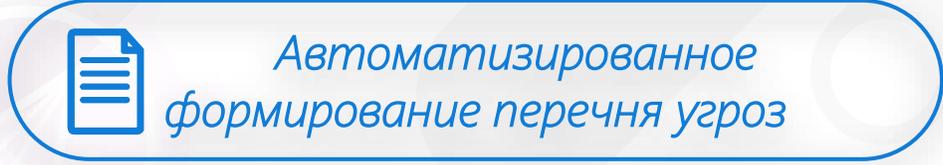
- ✓ Инвентаризация систем и сетей и определение возможных объектов воздействия УБИ



### 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



Перечень компонентов объектов воздействия

Справочники

Негативные последствия

Угрозы

Объекты

**Компоненты**

Способы реализации

Нарушители

Меры защиты

Формирование перечня угроз

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.1.1.1 Прошивка (встроенная микропрограмма)

Тип компонента: Программное обеспечение

**Объекты воздействия, в состав которых может входить К.1.1.1:**

- О.1 Автоматизированное рабочее место
- О.2 Сервер
- О.3 Периферийное оборудование
- О.4 Устройство хранения данных
- О.5 Устройство интернета-вещей
- О.6 Активное сетевое оборудование
- О.7 Обеспечивающие системы
- О.8 Телефония (VoIP, GSM)
- О.9 Средства защиты информации
- О.10 Мобильное устройство

**Способы реализации угроз:**

- 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 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 беспроводных сетей)
- СП.2.10 Использование недостатков конфигурации сетевого оборудования, связанных с отсутствием или некорректной фильтрацией трафика

1 Начальная страница

2 Негативные последствия

3 Угрозы

4 **Объекты воздействия**

5 Компоненты

6 Нарушитель

7 Результат

Раздел предназначен для автоматизации процесса формирования перечня возможных УБИ

Присупить к формированию угроз

**Угрозы безопасности информации**

- УБИ.1 Угроза утечки информации
- УБИ.2 Угроза НСД к информационным ресурсам
- УБИ.11 Угроза несанкционированного массового сбора информации

**Объекты воздействия**

- О.1 АРМ
- О.2 Сервер
- О.12 Физические линии связи

**Компоненты**

- К.1 Программное обеспечение
  - К.1.2 Системное ПО
    - К.1.2.1 Операционная система
- К.2 Программно-аппаратные средства
- К.3 Сетевые компоненты
- К.4 Пользователи

**УБИ.2.1.1 Угроза несанкционированного доступа к автоматизированному рабочему месту за счет эксплуатации уязвимостей**

# Новый раздел угроз безопасности информации

Угрозы | Уязвимости | Документы | Термины | Обратная связь | Обновления | Участники | Обучение | ФСТЭК России

Главная / Раздел угроз

## Угрозы

УБИ.1 Угроза утечки информации	УБИ.2 Угроза несанкционированного доступа	УБИ.3 Угроза несанкционированной модификации (искажения)	УБИ.4 Угроза несанкционированной подмены	УБИ.5 Угроза удаления информационных ресурсов	УБИ.6 Угроза отказа в обслуживании	УБИ.7 Угроза ненадлежащего (нецелевого) использования	УБИ.8 Угроза нарушения функционирования (работоспособности)	УБИ.9 Угроза получения информационных ресурсов из недовверенного или скомпрометированного источника	УБИ.10 Угроза распространения противоправной информации	УБИ.11 Угроза несанкционированного массового сбора информации
--------------------------------	---	--	--	---	------------------------------------	---	---	---	---	---

Способы реализации (возникновения) угроз

СП.1 Эксплуатация уязвимостей > 2	СП.1 Эксплуатация уязвимостей > 2	СП.1 Эксплуатация уязвимостей > 2	СП.2 Использование недостатков конфигурации > 11	СП.1 Эксплуатация уязвимостей > 2	СП.1 Эксплуатация уязвимостей > 2					
СП.2 Использование недостатков конфигурации > 11	СП.2.1 Использование недостатков, связанных с неполнотой проверки вводимых (выходных) данных > 11	СП.2.1 Использование недостатков, связанных с неполнотой проверки вводимых (выходных) данных > 11	СП.2 Использование недостатков конфигурации > 11	СП.3.2 Эксплуатация недостатков, децентрализованного и неконтролируемого подключения к сети Интернет > 11	СП.2 Использование недостатков конфигурации > 11	СП.2 Использование недостатков конфигурации > 11				
СП.3 Использование недостатков архитектуры > 2	СП.2.2 Использование недостатков, связанных с управлением учетными данными > 2	СП.2.2 Использование недостатков, связанных с управлением учетными данными > 2	СП.4 Внедрение вредоносного программного обеспечения > 12	СП.4 Внедрение вредоносного программного обеспечения > 12	СП.3 Использование недостатков архитектуры > 2	СП.3 Использование недостатков архитектуры > 2				
СП.4 Внедрение вредоносного программного обеспечения > 12	СП.2.3 Использование недостатков, связанных с отсутствием проверки достоверности отправителя и/или получателя > 12	СП.2.3 Использование недостатков, связанных с отсутствием проверки достоверности отправителя и/или получателя > 12	СП.5 Внедрение программных и аппаратных закладок > 8	СП.4 Внедрение вредоносного программного обеспечения > 12	СП.4 Внедрение вредоносного программного обеспечения > 12	СП.4 Внедрение вредоносного программного обеспечения > 12				
СП.5 Внедрение программных и аппаратных закладок > 8	СП.5 Внедрение программных и аппаратных закладок > 8	СП.5 Внедрение программных и аппаратных закладок > 8	СП.5 Внедрение программных и аппаратных закладок > 8	СП.5 Внедрение программных и аппаратных закладок > 8	СП.5 Внедрение программных и аппаратных закладок > 8	СП.5 Внедрение программных и аппаратных закладок > 8	СП.6 Использование недеklarированных возможностей > 3	СП.5 Внедрение программных и аппаратных закладок > 8	СП.5 Внедрение программных и аппаратных закладок > 8	СП.5 Внедрение программных и аппаратных закладок > 8
СП.6 Использование недеklarированных возможностей > 3	СП.6 Использование недеklarированных возможностей > 3	СП.7.3 Атаки на уровне каналов и сети, приводящие к изменению маршрутов > 3	СП.6 Использование недеklarированных возможностей > 8	СП.6 Использование недеklarированных возможностей > 3	СП.6 Использование недеklarированных возможностей > 3					

Способы, которыми могут быть реализованы угрозы



# 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 воздействия

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

- К.1.1.1 Пршивка (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)

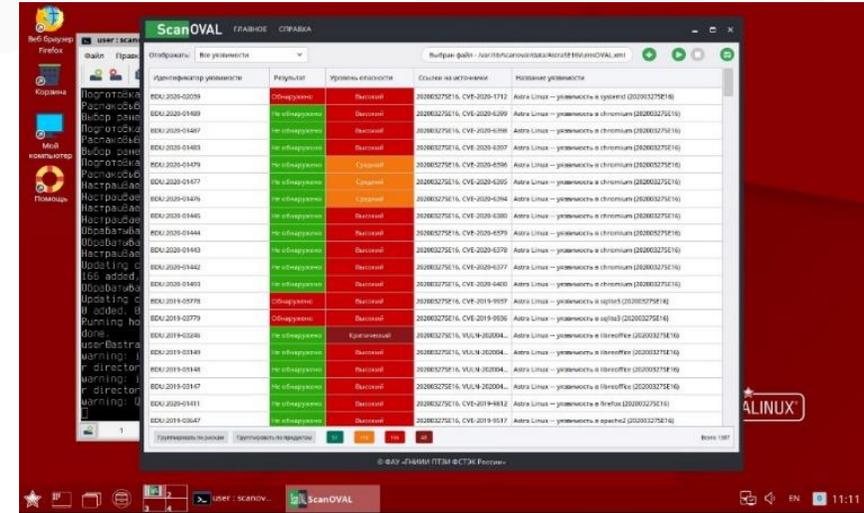
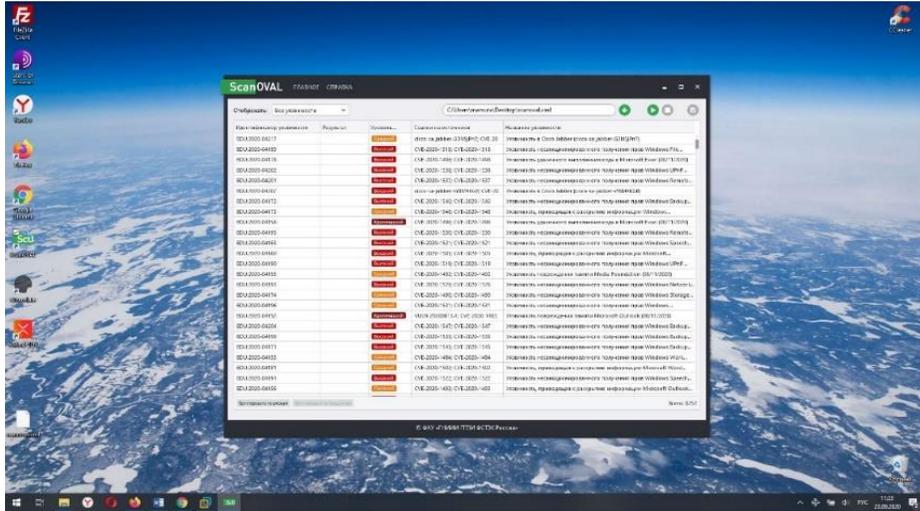
- В.1 Нарушитель, обладающий базовыми возможностями ?
- В.2 Нарушитель, обладающий базовыми повышенными возможностями ?
- В.3 Нарушитель, обладающий средними возможностями ?

# Уязвимости программного обеспечения

## Автоматический поиск уязвимостей. Программы ScanOVAL

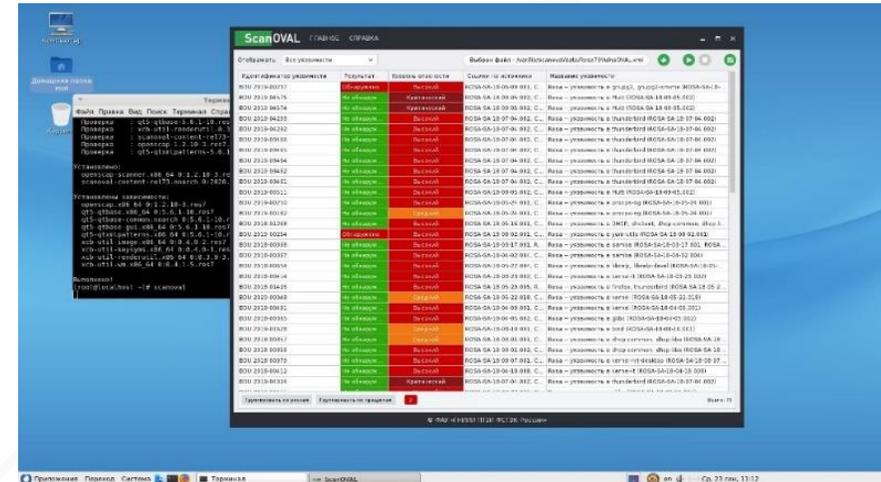
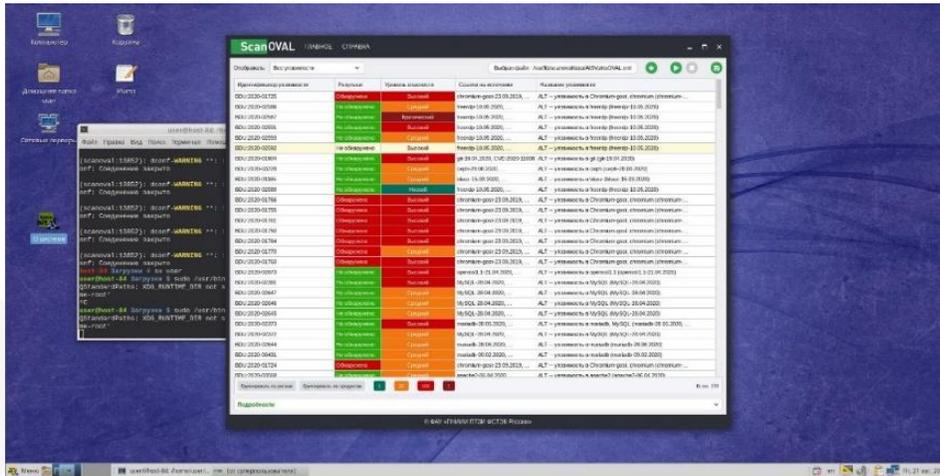
Windows

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*

The screenshot displays the ScanOVAL application interface. The main window shows a table of detected vulnerabilities. Below the table, there is a detailed view for a specific vulnerability (BDU:2022-04769).

Идентификатор уязвимости	Результат	Уровень опасности	Ссылки на источники	Название уязвимости
BDU:2022-05082	Обнаружено	Высокий	2022-1011SE17MD, ...	Astra Linux -- уязвимость в vim (2022-1011SE17MD)
BDU:2022-04066	Обнаружено	Высокий	2022-1011SE17MD, ...	Astra Linux -- уязвимость в vim (2022-1011SE17MD)
BDU:2022-04067	Обнаружено	Высокий	2022-1011SE17MD, ...	Astra Linux -- уязвимость в vim (2022-1011SE17MD)
BDU:2022-04074	Обнаружено	Средний	2022-1011SE17MD, ...	Astra Linux -- уязвимость в vim (2022-1011SE17MD)
BDU:2022-04060	Обнаружено	Высокий	2022-1011SE17MD, ...	Astra Linux -- уязвимость в vim (2022-1011SE17MD)
BDU:2022-04086	Обнаружено	Высокий	2022-1011SE17MD, ...	Astra Linux -- уязвимость в vim (2022-1011SE17MD)
BDU:2022-06481	Обнаружено	Высокий	2022-1011SE17MD, ...	Astra Linux -- уязвимость в vim (2022-1011SE17MD)
BDU:2022-06482	Обнаружено	Высокий	2022-1011SE17MD, ...	Astra Linux -- уязвимость в vim (2022-1011SE17MD)

**Подобности**

Идентификатор уязвимости: [BDU:2022-04769](#)

Результат: **Обнаружено**

Уровень опасности уязвимости: **Критический**

OVAL: [oval:ru.altx-soft.nix:def:1930.40](#) (версия 2)

Название уязвимости: Astra Linux -- уязвимость в firefox, thunderbird (2022-1011SE17MD)

Описание уязвимости: В продуктах firefox, thunderbird обнаружена уязвимость CVE-2022-2505.

Возможные меры по устранению уязвимости: Использование рекомендаций производителя: <https://www.mozilla.org/en-US/security/advisories/mfsa2022-30/>

Ссылки на источники: [VENDOR\\_2022-1011SE17MD](#), [CVE\\_2022-2505](#)

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

Программное обеспечение: cpe:/a:mozilla:thunderbird, cpe:/o:astra\_linux:astralinux\_se:1.7

Детализация: firefox (0:102.0+build2-0ubuntu0.18.04.1+ci202207111653+astral1), firefox-locale-ru (0:102.0+build2-0ubuntu0.18.04.1+ci202207111653+astral1), thunderbird (1:102.0.1+build2-0ubuntu2+ci202207141120+astral1), thunderbird-locale-ru (1:102.0.1+build2-0ubuntu2+ci202207141120+astral1)

Файл: /var/lib/scanoval/data/AstraSE17VulnsOVAL.xml

© ФАУ «ГНИИИ ПТЗИ ФСТЭК России»

# Уязвимости программного обеспечения

## Программы ScanOVAL. Результат сканирования

The screenshot displays the ScanOVAL web interface. At the top, there is a navigation bar with 'ScanOVAL' and 'ГЛАВНОЕ СПРАВКА'. Below it, a search bar contains the file path 'C:\Users\mamuta\Desktop\scanoval.xml'. A dropdown menu is set to 'Только обнаруженные'. The main area features a table of vulnerabilities with columns for 'Идентификатор уязвимости', 'Результат', 'Уровень...', 'Ссылки на источники', and 'Название уязвимости'. The table lists several vulnerabilities, with the last one (BDU:2020-04079) highlighted in yellow. Below the table, there are filters for risk levels and a total count of 274 vulnerabilities. A detailed view of the selected vulnerability (BDU:2020-04079) is shown below, including its result, severity, OVAL definition, name, description, mitigation measures, and references.

Идентификатор уязвимости	Результат	Уровень...	Ссылки на источники	Название уязвимости
BDU:2020-03234	Обнаружена	Средний	CVE-2020-3968; VMSA-2020-0015	Уязвимость в VMware Workstation 15.x до 15.5.5 (VMSA-2020-0015)
BDU:2020-03232	Обнаружена	Низкий	CVE-2020-3970; VMSA-2020-0015	Уязвимость в VMware Workstation 15.x до 15.5.5 (VMSA-2020-0015)
BDU:2020-03515	Обнаружена	Средний	CVE-2020-1342; CVE-2020-1342	Уязвимость, приводящая к раскрытию информации в Microsoft Office...
BDU:2020-03512	Обнаружена	Высокий	CVE-2020-1447; CVE-2020-1447	Уязвимость удаленного выполнения кода Microsoft Word (07/14/2020)
BDU:2020-03499	Обнаружена	Высокий	CVE-2020-1446; CVE-2020-1446	Уязвимость удаленного выполнения кода Microsoft Word (07/14/2020)
BDU:2020-03603	Обнаружена	Средний	CVE-2020-1445; CVE-2020-1445	Уязвимость, приводящая к раскрытию информации в Microsoft Office...
BDU:2020-03498	Обнаружена	Высокий	CVE-2020-1448; CVE-2020-1448	Уязвимость удаленного выполнения кода Microsoft Word (07/14/2020)
BDU:2020-04074	Обнаружена	Высокий	CVE-2020-1583; CVE-2020-1583	Уязвимость, приводящая к раскрытию информации Microsoft Word...
BDU:2020-04079	Обнаружена	Критический	CVE-2020-1563; CVE-2020-1563	Уязвимость удаленного выполнения кода Microsoft Office...

Группировать по рискам | Группировать по продуктам | 26 168 74 6 | Всего: 274

**Подробности**

Идентификатор уязвимости: [BDU:2020-04079](#)

Результат: **Обнаружена**

Уровень опасности уязвимости: **Критический**

OVAL: [oval:ru.altx-soft.win:def:70705](#) (версия 5)

Название уязвимости: Уязвимость удаленного выполнения кода Microsoft Office (BDU:2020-04079)

Описание уязвимости: Уязвимость удаленного выполнения кода в Microsoft Office позволяет злоумышленникам выполнить произвольный код в контексте текущего пользователя. Если текущий пользователь имеет административные привилегии, злоумышленник получит контроль над уязвимой системой, после чего злоумышленник сможет устанавливать программы; просматривать, изменять или удалять данные;

Возможные меры по устранению уязвимости: Использование рекомендаций: <https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1563>

Ссылки на источники: Microsoft [CVE-2020-1563](#)  
CVE [CVE-2020-1563](#)

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

Программное обеспечение: cpe:/a:microsoft:office:2016

Детализация: C:\Program Files\Common Files\Microsoft Shared\OFFICE16\ACEEXCL.DLL (16.0.4266.1001)

Файл: C:\Users\mamuta\Desktop\scanoval.xml

Кнопка запуска проверки

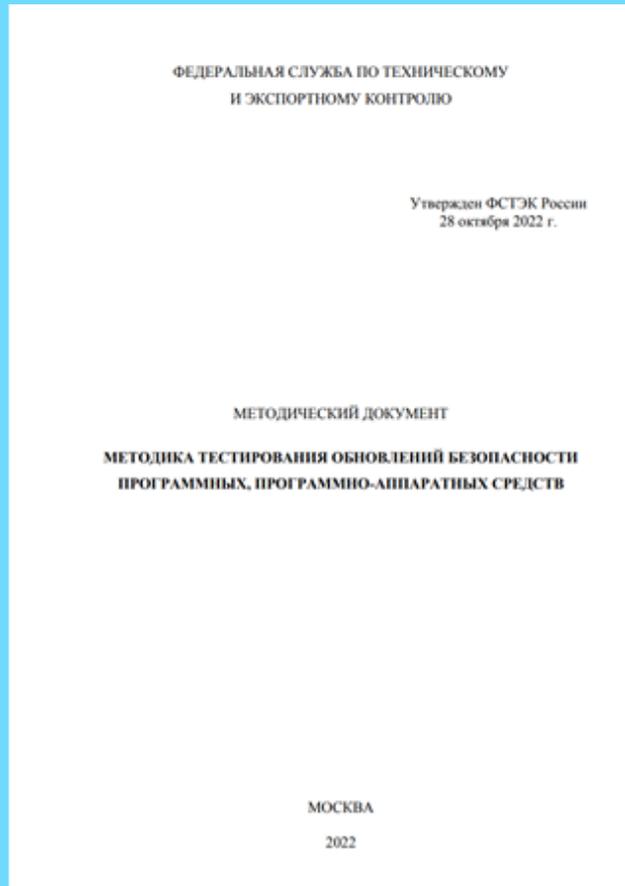
Обнаруженные уязвимости

Количество обнаруженных уязвимостей

Детализированная информация по выбранной записи

# Уязвимости программного обеспечения

Методика тестирования обновлений безопасности программных, программно-аппаратных средств



**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



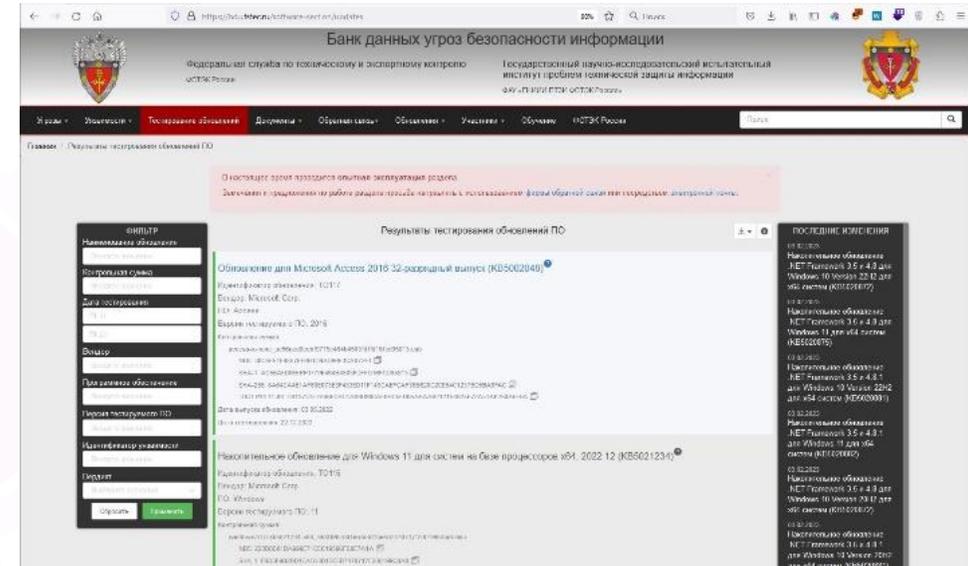
ДЕПАРТАМЕНТ  
ИНФОРМАЦИОННЫХ  
ТЕХНОЛОГИЙ  
ГОРОДА МОСКВЫ



ИСП РАН



ГНИИИ ПТЗИ  
ФСТЭК России



БДУ ФСТЭК России

Рабочая группа

# Уязвимости программного обеспечения

## Раздел тестирования обновлений БДУ

[bdu.fstec.ru/software-section/updates](https://bdu.fstec.ru/software-section/updates)

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

Поиск

Результаты тестирования обновлений ПО

**ФИЛЬТР**

Наименование обновления

Контрольная сумма

Дата тестирования  
от   
до

Вендор

Программное обеспечение

Версия тестируемого ПО

Идентификатор уязвимости

Вердикт

**Обновление для Microsoft Access 2016 32-разрядный выпуск (KB5002048)**<sup>2</sup>

Идентификатор обновления: TO117  
Вендор: Microsoft Corp.  
ПО: Access  
Версии тестируемого ПО: 2016  
Контрольная сумма:  
access-x-none\_ac56aed8eebf9779e464b4503fdffd16fcd95813.cab  
MD5: 30C5FE1F9557FF8B1D9AD96E3CA072E1   
SHA-1: AC56AED8EEBF9779E464B4503FDFFD16FCD95813   
SHA-256: 8A64CA4E1AF69E073E3F433ED11F149CAEFCFAF36B620C2CE54C1237BD5BA6FAC   
ГОСТ P34.11-94: 4D3137F1B764CECBA1989D00EAB05CDE50BAAA26215164527EA213EA52A0FEA6

Дата выпуска обновления: 03.05.2022  
Дата тестирования: 22.12.2022

**Накопительное обновление для Windows 11 для систем на базе процессоров x64, 2022 12 (KB5021234)**<sup>2</sup>

Идентификатор обновления: TO116  
Вендор: Microsoft Corp.  
ПО: Windows  
Версии тестируемого ПО: 11  
Контрольная сумма:  
windows10.0-kb5021234-x64\_16d3f9b2dd1eafa3d1be5d7470717f230199c0a8.msu  
MD5: 223B8B01DA999E71CEC19596FB0E7A1A   
SHA-1: F6D3F9B2DD1EAF3D1BE5D7470717F230199C0A8   
SHA-256: CF25B8772623402EF84982B05A7E5E48D653F7CDF0B49A19AC91DA3E18D460F   
ГОСТ P34.11-94: C49D6104FF8AC8C47A2F679F16FFB9A8692FFB5D2D088C83714CD4DDE5ABCA1

Дата выпуска обновления: 13.12.2022  
Дата тестирования: 15.12.2022

**ПОСЛЕДНИЕ ИЗМЕНЕНИЯ**

03.02.2023  
Накопительное обновление .NET Framework 3.5 и 4.8 для Windows 10 Version 22H2 для x64 систем (KB5020872)

03.02.2023  
Накопительное обновление .NET Framework 3.5 и 4.8 для Windows 11 для x64 систем (KB5020875)

03.02.2023  
Накопительное обновление .NET Framework 3.5 и 4.8.1 для Windows 10 Version 22H2 для x64 систем (KB5020881)

03.02.2023  
Накопительное обновление .NET Framework 3.5 и 4.8 для Windows 10 Version 20H2 для x64 систем (KB5020872)

03.02.2023  
Накопительное обновление .NET Framework 3.5 и 4.8.1 для Windows 10 Version 20H2 для x64 систем (KB5020881)

03.02.2023  
Накопительное обновление .NET Framework 3.5 и 4.8 для Windows 10 Version 21H2 на базе процессоров x86 (KB5020872)

02.02.2023  
Накопительное обновление .NET Framework 3.5 и 4.8.1 для Windows 10 Version 21H2 на базе процессоров x86

# 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:	<a href="https://support.microsoft.com/help/5002286">https://support.microsoft.com/help/5002286</a>
URI:	<a href="https://catalog.s.download.windowsupdate.com/c/msdownload/update/software/secur/2022/11/visio-x-none_80d9120cdce1d2bcd022fa5c1217663379a8ae50.cab">https://catalog.s.download.windowsupdate.com/c/msdownload/update/software/secur/2022/11/visio-x-none_80d9120cdce1d2bcd022fa5c1217663379a8ae50.cab</a> <a href="https://www.catalog.update.microsoft.com/Search.aspx?q=5002286">https://www.catalog.update.microsoft.com/Search.aspx?q=5002286</a>
Контрольная сумма:	visio-x-none_80d9120cdce1d2bcd022fa5c1217663379a8ae50.cab: MD5: 8AF40BAD0C4F27301F9FC3FEB8C5CC61 SHA-1: 80D9120CDCE1D2BCD022FA5C1217663379A8AE50 SHA-256: B5A15CC1F3B29DF70F6D451796D7C52B63B9AD56986C48F219C4B176220D9A40 ГОСТ P34.11-94: 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)	<u>Не выявлено признаков не декларированных возможностей или деструктивного функционала</u>	Исследовательский стенд
Ручной анализ обновления (T006)	Не проводился	-

# Уязвимости программного обеспечения

## Раздел тестирования обновлений БДУ ФСТЭК России

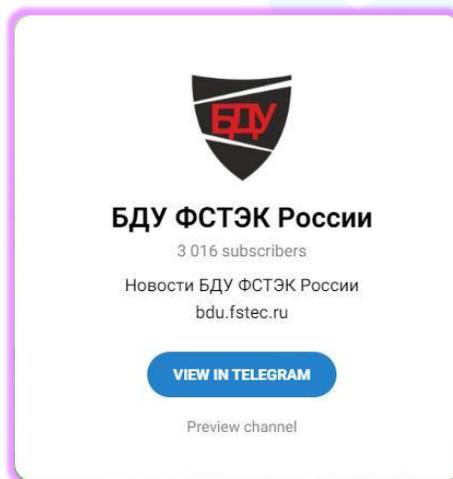
### Сведения о результатах тестирований в описаниях уязвимостей

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 ▾
<b>Описание уязвимости</b>	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	
<b>Вендор</b>	Microsoft Corp.	
<b>Наименование ПО</b>	Microsoft Office, Microsoft Visio, 365 Apps for Enterprise	
<b>Версия ПО</b>	2019 (Microsoft Office) 2013 SP1 (Microsoft Visio) 2016 (Microsoft Visio) - (365 Apps for Enterprise) LTSC 2021 (Microsoft Office)	
<b>Тип ПО</b>	Прикладное ПО информационных систем	
<b>Операционные системы и аппаратные платформы</b>	Данные уточняются	
<b>Тип ошибки</b>	Использование после освобождения	
<b>Идентификатор типа ошибки</b>	CWE-416	
<b>Класс уязвимости</b>	Уязвимость кода	
<b>Дата выявления</b>	13.12.2022	
<b>Базовый вектор уязвимости</b>	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:A/N	
<b>Уровень опасности уязвимости</b>	Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,2) Высокий уровень опасности (базовая оценка CVSS 3.0 составляет 7,8)	
<b>Возможные меры по устранению уязвимости</b>	Использование рекомендаций производителя: <a href="https://more-microsoft.com/update-guide/en_USA/vulnerability/CVE-2022-14605">https://more-microsoft.com/update-guide/en_USA/vulnerability/CVE-2022-14605</a> 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)	
<b>Статус уязвимости</b>	Подтверждена производителем	
<b>Наличие эксплойта</b>	Данные уточняются	

# Новые возможности банка данных угроз безопасности информации

Telegram-канал и БОТ с возможностью подписки на рассылку

[t.me/bdufstecru](https://t.me/bdufstecru)



## БДУ ФСТЭК России

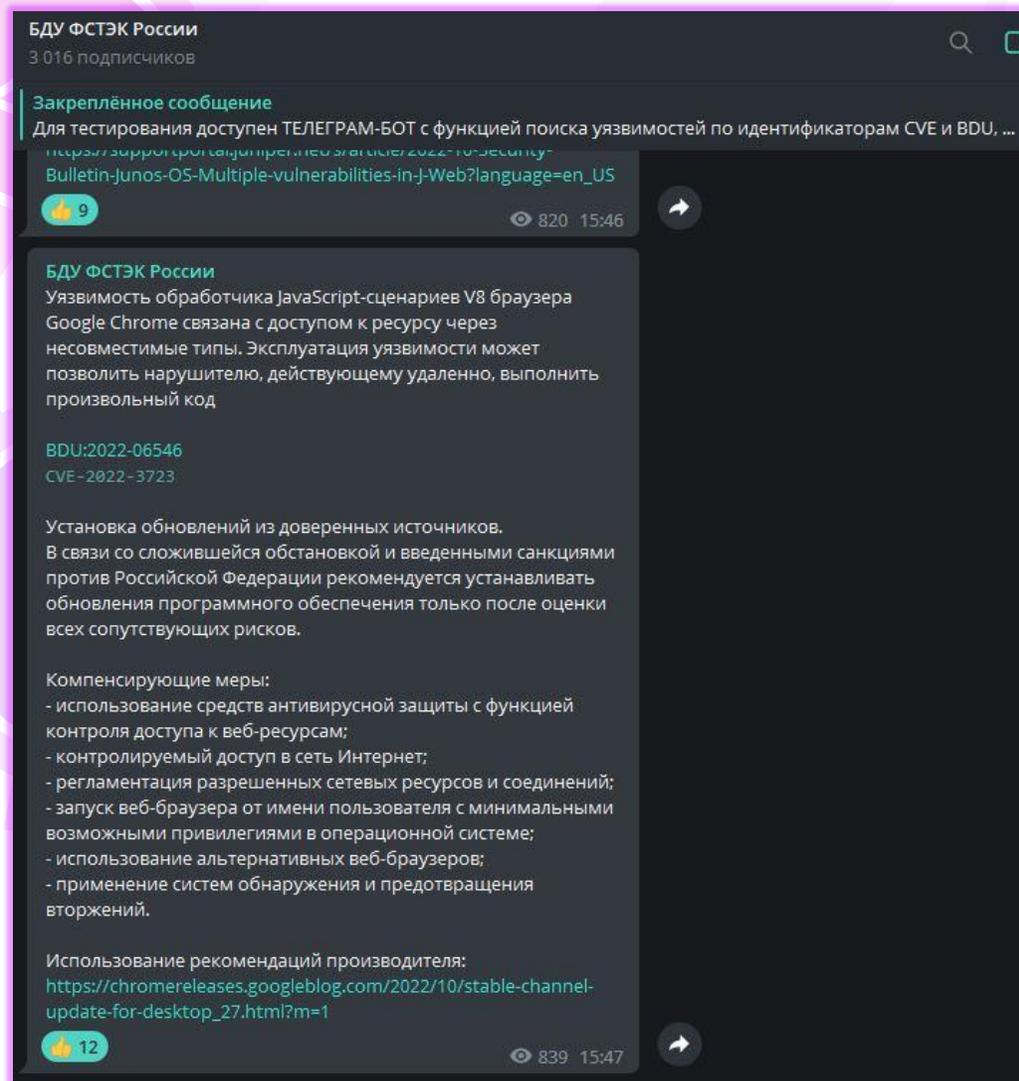
Для тестирования доступен ТЕЛЕГРАМ-БОТ с функцией поиска уязвимостей по идентификаторам CVE и BDU, а также с возможностью подписаться на обновления БДУ; мгновенно получить топ 10 уязвимостей: по вендорам, по АСУ ТП и т.д.

Ссылка на бота:

[@BDU\\_HELPbot](https://t.me/@BDU_HELPbot)

👍 6 🍌 3 ❤️ 2 🤖 1

👁 9432 ⚡ изменено 16:59



# 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