



СОВЕРШЕНСТВОВАНИЕ БАНКА ДАННЫХ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

**Заместитель начальника отдела
управления ФСТЭК России
Гефнер Ирина Сергеевна**

Создание банка данных угроз безопасности информации



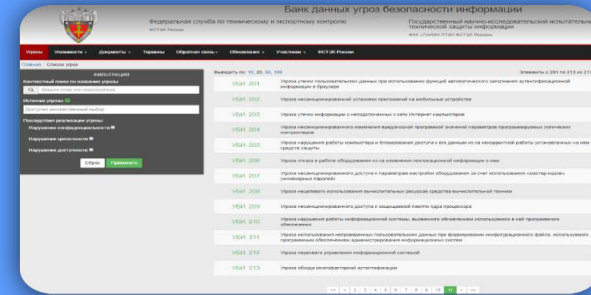
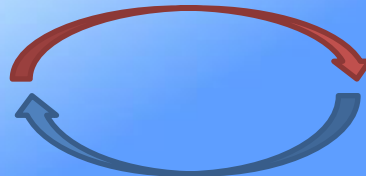
213 угроз безопасности

Более 20 000 уязвимостей

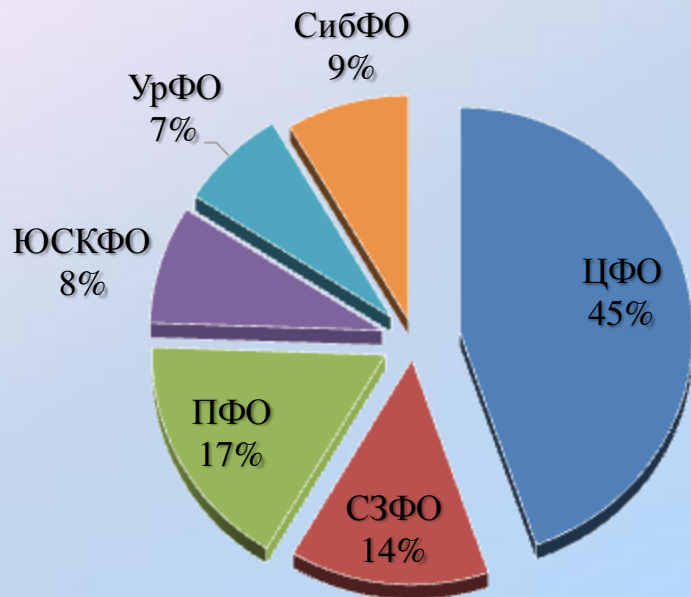
Статистика посещения сайта банка угроз безопасности информации



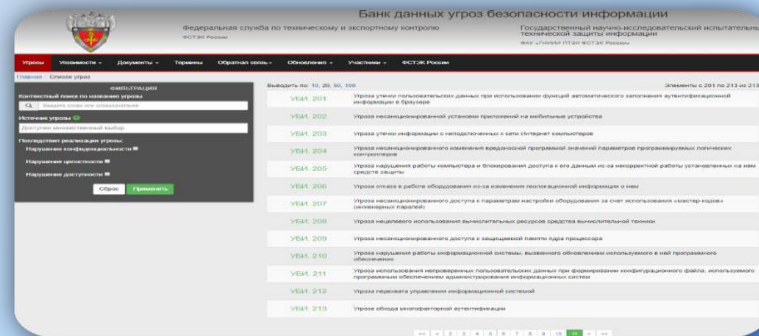
■ 2015 ■ 2016 ■ 2017 ■ 2018



Статистика посещения сайта банка угроз безопасности информации



Статистика посещений сайта пользователями из различных федеральных округов



Термины 6822

Документы 14761

Уязвимости 133239

Угрозы 361813

Статистика просмотра популярных разделов

Статистика посещения сайта банка угроз безопасности информации



Статистические данные по использованию компонента фильтрации в разделе «Уязвимости»

Угрозы безопасности информации 2018 года

Новые технологии

Уязвимости

Эксплойты

Новые способы реализации угроз

Новые угрозы безопасности информации

УБИ.208

Угроза нецелевого использования вычислительных ресурсов средства вычислительной техники

УБИ.209

Угроза несанкционированного доступа к защищаемой памяти ядра процессора

УБИ.210

Угроза нарушения работы информационной системы, вызванного обновлением используемого в ней программного обеспечения

УБИ.211

Угроза использования непроверенных пользовательских данных при формировании конфигурационного файла, используемого программным обеспечением администрирования информационных систем

УБИ.212

Угроза перехвата управления информационной системой

УБИ.213

Угроза обхода многофакторной аутентификации

Появление новых угроз безопасности информации в банке данных

Угрозы новых
технологий

Угрозы АСУ ТП

Угрозы ЧПУ

Угрозы SCADA



Классификация угроз безопасности информации

Банк данных угроз безопасности информации

Федеральная служба по техническому и экспортному контролю
ФСТЭК России

Государственный научно-исследовательский испытательный
технической защиты информации
ФГУП «Центр ПТЗИ ФСТЭК России»

Угрозы Уязвимости Документы Термины Обратная связь Обсуждение Участники ФСТЭК России

Главная / Список угроз

Фильтрация

Контекстный поиск по названию угрозы

Источники угроз

Последствия реализации угрозы

Нарушение конфиденциальности

Нарушение целостности

Нарушение доступности

Обновить

Выборить по: 10, 20, 50, 100

Элементы с 201 по 213 из 213

УБИ.201	Угроза утечки пользовательских данных при использовании функций автоматического заполнения идентификационной информации в браузере
УБИ.202	Угроза несанкционированной установки приложений на мобильные устройства
УБИ.203	Угроза утечки информации с подключенными к сети Интернет компьютеров
УБИ.204	Угроза несанкционированного изменения вредоносной программой значений параметров программируемых логических контроллеров
УБИ.205	Угроза нарушения работы компьютера и блокирования доступа к его данным из-за неисправной работы установленных на нем средств защиты
УБИ.206	Угроза отказа в работе оборудования из-за изменения неоплаченной информации о нем
УБИ.207	Угроза несанкционированного доступа к параметрам настройки оборудования за счет использования его интерфейсов
УБИ.208	Угроза нецелевого использования вычислительных ресурсов средства вычислительной техники
УБИ.209	Угроза несанкционированного доступа к защищаемой памяти ядра процессора
УБИ.210	Угроза нарушения работы информационной системы, вызванного обновлением используемого в ней программного обеспечения
УБИ.211	Угроза использования непроверенных пользователем данных при формировании конфигурационного файла, используемого программным обеспечением администрирования информационных систем
УБИ.212	Угроза

Главная / Список угроз / УБИ.213

Детальная
классификация?

ОБЪЕКТ ВОЗДЕЙСТВИЯ

ИСТОЧНИКИ УГРОЗ

**ПОСЛЕДСТВИЯ РЕАЛИЗАЦИИ
УГРОЗЫ**

ОПИСАНИЕ УГРОЗЫ

факторной аутентификации

содержится в возможности обхода многофакторной аутентификации путем внедрения вредоносного кода.

Угроза обусловлена:

уязвимостей программного обеспечения;
отсутствием мер антивирусной защиты и разграничения доступа.

Последствия данной угрозы возможна:

работы дискредитируемого пользователя с файлами, поступающими из недоверенных источников;
утраты им привилегий установки программного обеспечения

Угроза реализуется злоумышленником с высоким потенциалом

Объект воздействия: Системное программное обеспечение, микропрограммное обеспечение, учетные данные пользователя

конфиденциальности
целостности
доступности

Тестовая версия классификации угроз безопасности информации

УГРОЗЫ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

ИНЦИДЕНТЫ

- Отказ в обслуживании
- Нарушение функционирования (работоспособности) технических средств и систем
- Утечка данных
- Модификация (подмена) данных
- Несанкционированный доступ
- Несанкционированное использование вычислительных ресурсов

ОБЪЕКТЫ ВОЗДЕЙСТВИЯ

- Человек
- Процессы разработки, производства, поставки
- Каналы связи (передачи) данных
- Технические средства
- Программное обеспечение (программы)
- Аппаратное устройство (компонент)

СПОСОБ (МЕТОДЫ) РЕАЛИЗАЦИИ УГРОЗ

- Несанкционированный сбор информации
- Исчерпание ресурсов
- Инъекция
- Подмена при взаимодействии
- Манипулирование сроками и состоянием
- Злоупотребление функционалом
- Вероятностные методы
- Нарушение аутентификации
- Нарушение авторизации
- Манипулирование структурами данных
- Анализ целевого объекта
- Манипулирование ресурсами
- Использование технических отказов, ошибок
- Получение физического доступа
- Использование слабостей в организации

ИСТОЧНИК

- Нарушитель
 - ТИП НАРУШИТЕЛЯ
 - Внешний
 - Внутренний
- ПОТЕНЦИАЛ
 - Базовый
 - Базовый повышенный
 - Высокий
- ТИП ДОСТУПА
 - Физический доступ
 - Локальный доступ
 - Удаленный доступ
- Вредоносный код (программная закладка)
- Аппаратное устройство (аппаратная закладка)
- Техногенные источники

Выбор угроз по заданному
классификационному признаку

Удобство при моделировании
угроз безопасности информации

Тестовая версия классификации угроз безопасности информации

УГРОЗЫ БЕЗОПАСНОСТИ ИНФОРМАЦИИ



УГРОЗЫ БЕЗОПАСНОСТИ ИНФОРМАЦИИ, СВЯЗАННЫЕ С ОТКАЗОМ В ОБСЛУЖИВАНИИ

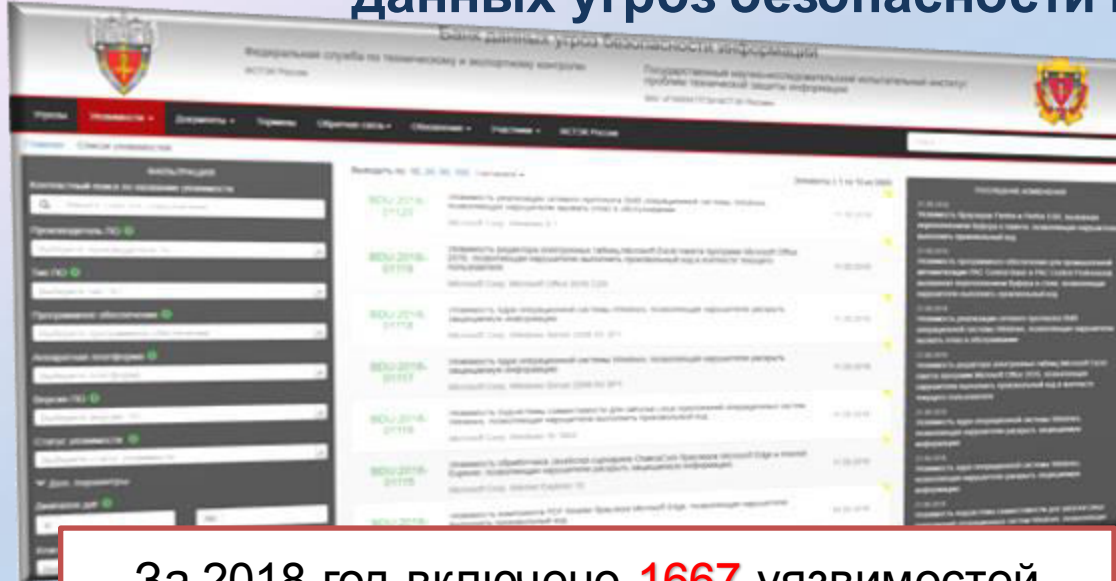
Под угрозами безопасности информации, связанными с отказом в обслуживании, понимаются угрозы, реализация которых может привести к частичной или полной неспособности системы, сервисов или сетей продолжать функционирование

Элементы 1—10 из 25

УБИ. 006	Угроза внедрения кода или данных
УБИ. 011	Угроза деавторизации санкционированного клиента беспроводной сети
УБИ. 014	Угроза длительного удержания вычислительных ресурсов пользователями
УБИ. 022	Угроза избыточного выделения оперативной памяти
УБИ. 024	Угроза изменения режимов работы аппаратных элементов компьютера
УБИ. 026	Угроза искажения XML-схемы
УБИ. 038	Угроза истощения вычислительных ресурсов хранилища больших данных
УБИ. 040	Угроза конфликта юрисдикций различных стран
УБИ. 043	Угроза нарушения доступности облачного сервера
УБИ. 046	Угроза нарушения процедуры аутентификации субъектов виртуального информационного взаимодействия

Выбор угроз по заданному классификационному признаку

Сведения об уязвимостях, содержащихся в банке данных угроз безопасности информации



За 2018 год включено **1667** уязвимостей

Содержит сведения о более **20 000** уязвимостей

Еженедельное наполнение сведениями об уязвимостях (сейчас в среднем **100** уязвимостей/неделя)



Статистика по уязвимостям

Распределение уязвимостей по уровням опасности



Статистика уязвимостей отечественного программного обеспечения

Распределение по производителям



Распределение уязвимостей по уровням опасности



Средство автоматизации ScanOval

Банк данных угроз безопасности информации

Федеральная служба по техническому и экспортному контролю
встрах.России

Государственный научно-исследовательский испытательный институт
проблем технической защиты информации
ФНИИ ИТЗИ встрах.России

Угрозы Уязвимости Документы Топологии Обратная связь Обновления Участники встрах.России

Главная Список уязвимостей Информации Кабинет CVSS V2 Кабинет CVSS V3 ScanOval

Программа ScanOval для автоматизированных проверок наличия уязвимостей программного обеспечения

Программа ScanOval предназначена для оперативного автоматизированного обнаружения уязвимостей программного обеспечения на уровне операционной системы, программных пакетов, установленных на уровне операционной системы Microsoft Windows. В настоящее время проводится анализ эксплуатационных систем ScanOval. Задачами и предложения по работе программы ScanOval, просьба направлять в письменной или электронной форме по адресу: info@fntsi.vestrah.ru

Ввиду использования программы, пользователь, ознакомившись с условиями (агрегированного соглашения) о конфиденциальности информации ScanOval, в файле Readme.txt соглашается с условиями использования информации ScanOval.

Программа ScanOval обеспечивает выполнение следующих основных функций:

- загрузка XML-файлов с OVAL, описанием уязвимостей, выходящих из стандарта «The OVAL Language Specification» версии не ниже 5.10.1, описанием на основании обработки данных, представленных в XML-файлах, уязвимостей программного обеспечения, установленного на рабочей ПДМ, работающей под управлением операционной системы семейства Microsoft Windows;

Для работы в рамках ScanOval, необходимы конфигурации клиента данных соответствующие следующим минимальным требованиям:

- 32-разрядный (x86) или 64-разрядный (x64) процессор с тактовой частотой 1 ГГц или выше;
- 1 Гб (для 32-разрядной системы) или 2 Гб (для 64-разрядной системы) оперативной памяти;
- 6.5 Гб свободного места на жестком диске;
- графическое устройство DirectX 9 с драйвером WDDM 1.0 или более поздней версии.



Размещено на сайте
банка данных
18 сентября 2018 г.

5878 просмотров

Автоматизированная проверка уязвимостей ПО,
работающего под управлением ОС Windows

База уязвимостей, состоящая из
3 767 уязвимостей на языке OVAL

Формирование отчета по результатам анализа

ScanOVAL ГЛАВНОЕ СПРАВКА

Идентификатор уязвимости: Все уязвимости Результат: Уровни... Ссылка на источник: Название уязвимости

BDU-2014-00004	Уязвимость	CVE-2012-1944; mfa2012-36	Уязвимость в реализации CSP в Mozilla Firefox 4.x по 12.0, Firefox ESR...
BDU-2014-00005	Уязвимость	CVE-2014-1732; MS14-017	Уязвимость, позволяющая форматировать файлы Microsoft Office (MS14-017)
BDU-2014-00184	Уязвимость	CVE-2014-1506; MS14-026	Уязвимость TypeLibrary (MS14-026)
BDU-2015-00281	Уязвимость	CVE-2014-0516; arpit14-14	Уязвимость в Adobe Flash Player до 13.0.0.214, Adobe AIR SDK до...
BDU-2015-00277	Уязвимость	CVE-2014-0516; arpit14-14	Уязвимость в Adobe Flash Player до 13.0.0.214, Adobe AIR SDK до...
BDU-2014-00364	Уязвимость	CVE-2014-1809; MS14-024	Уязвимость ASLR в MSOSCT (MS14-024)
BDU-2015-00280	Уязвимость	CVE-2014-0516; arpit14-14	Уязвимость в Adobe Flash Player до 13.0.0.214, Adobe AIR SDK до...
BDU-2015-00306	Уязвимость	CVE-2014-0516; arpit14-14	Уязвимость в Adobe Flash Player до 13.0.0.214, Adobe AIR SDK до...
BDU-2014-00363	Уязвимость	CVE-2014-1809; MS14-023	Уязвимость в Microsoft Office, связанная с проверкой документов...
BDU-2015-00278	Уязвимость	CVE-2014-0517; arpit14-14	Уязвимость в Adobe Flash Player до 13.0.0.214, Adobe AIR SDK до...
BDU-2014-00362	Уязвимость	CVE-2014-1746; MS14-023	Уязвимость в Adobe Flash Player до 13.0.0.214, Adobe AIR SDK до...
BDU-2015-00279	Уязвимость	CVE-2014-0520; arpit14-14	Уязвимость в Google Chrome до 34.0.1847.137 (stable-channel-update)
BDU-2014-00167	Уязвимость	CVE-2014-1741; stable-channel-up	Уязвимость в Google Chrome до 34.0.1847.137 (stable-channel-update)
BDU-2014-00199	Уязвимость	CVE-2014-1742; stable-channel-up	Уязвимость в Google Chrome до 34.0.1847.137 (stable-channel-update)
BDU-2014-00212	Уязвимость	CVE-2014-1743; stable-channel-up	Уязвимость в Google Chrome до 34.0.1847.137 (stable-channel-update)
BDU-2014-00330	Уязвимость	CVE-2014-1743; stable-channel-up	Уязвимость в Google Chrome до 34.0.1847.137 (stable-channel-update)
BDU-2014-00332	Уязвимость	CVE-2014-1743; stable-channel-up	Уязвимость в Google Chrome до 34.0.1847.137 (stable-channel-update)
BDU-2014-00195	Уязвимость	CVE-2014-1746; stable-channel-up	Уязвимость в Google Chrome до 34.0.1847.137 (stable-channel-update)
BDU-2014-00137	Уязвимость	CVE-2014-1744; stable-channel-up	Уязвимость в Google Chrome до 34.0.1847.137 (stable-channel-update)
BDU-2014-00193	Уязвимость	CVE-2014-1747; stable-channel-up	Уязвимость в Google Chrome до 34.0.1847.137 (stable-channel-update)
BDU-2014-00157	Уязвимость	CVE-2014-1746; stable-channel-up	Уязвимость в Google Chrome до 34.0.1847.137 (stable-channel-update)
BDU-2014-00382	Уязвимость	CVE-2014-1813; MS14-022	Уязвимость Web Applications, связанная с содержимым страниц...
BDU-2015-00374	Уязвимость	CVE-2014-4247; cveid2014-19729	Неопределенная уязвимость в Oracle Java SE 6u75, 7u60, и 8u...
BDU-2015-00452	Уязвимость	CVE-2014-4255; cveid2014-19729	Неопределенная уязвимость в Oracle Java SE 6u75, 7u60, и 8u...
BDU-2015-00540	Уязвимость	CVE-2014-4219; cveid2014-19729	Неопределенная уязвимость в Oracle Java SE 6u75, 7u60, и 8u...

Дополнительно по результатам: Всего: 3321

Загрузка OVAL-описаний

СканOVAL ГЛАВНОЕ СПРАВКА

Отображать: Только обнаруженные E:\scanoval.xml

Идентификатор уязвимости	Результат	Уровень...	Ссылки на источники	Название уязвимости
16	Обнаружена	Критический	CVE-2017-11937; CVE-2017-11937	Уязвимость в Microsoft Malware Protection Engine до 1.1.14405.2...
15	Обнаружена	Высокий	CVE-2018-0986; CVE-2018-0986	Уязвимость в Microsoft Malware Protection Engine до 1.1.14700.5...
13	Обнаружена	Высокий	CVE-2018-8161; CVE-2018-8161	Уязвимость удаленного выполнения кода Microsoft Office (08/05/2018)
19	Обнаружена	Высокий	MS16-107; CVE-2016-3360	Уязвимость повреждения памяти в Microsoft Office (MS16-107)
16	Обнаружена	Средний	MS16-088; CVE-2016-3279	Уязвимость обхода функций безопасности Microsoft (MS16-088)
16	Обнаружена	Средний	MS16-004; CVE-2016-0012	Уязвимость обхода ASLR в Microsoft Office (MS16-004)

The screenshot shows the ScanOVAL application interface. At the top, there is a header bar with the 'ScanOVAL' logo on the left and the word 'ОТЧЁТ' (Report) on the right. Below the header, there is a table with five columns: '№ от' (Scan ID), '№ ск' (Scan Number), 'Прод' (Duration), 'Нача' (Start Time), and 'Форм' (Format). The table contains five rows of scan results. A blue callout box with the text 'Фильтрация результатов сканирования' (Filtering of scan results) points to the table. Below the table, there is a summary table with three columns: 'Уровень опасности' (Danger Level), 'Найдено' (Found), and 'Всего' (Total). The summary table has five rows, including a total row at the bottom.

№ от	№ ск	Прод	Нача	Форм
				b086d5d4-9af1-4e68-b03f-86c5191e2af2
				5a52388a-cacc-45d0-bb54-6b1db1510463
				Уязвимости
				26.09.2018 12:21:44 / 26.09.2018 12:26:08
				26.09.2018 12:28:51

Уровень опасности	Найдено	Всего
Критический	1	773
Высокий	3	1475
Средний	2	1053
Низкий	0	20
Всего	6	3321

Сканирование

Идентификатор уязвимости	Результат	Уровень...	Ссылки на источники	Название уязвимости
BDU-2014-00004	Сканировано	Высокий	CVE-2012-1944; mfsa2012-36	Уязвимость в реализации CSP в Mozilla Firefox 4.x по 12.0, Firefox ESR...
BDU-2014-00008	Высокий	Высокий	CVE-2014-1757; MS15-017	Уязвимость конвертера форматов файлов
BDU-2014-00184	Сканировано	Высокий	CVE-2014-1806; MS14-026	Уязвимость TrueTypeFont (MS15-026)
BDU-2015-00281	Высокий	Высокий	CVE-2014-0516; apris-14-14	Уязвимость в Adobe Flash Player до 13.1
BDU-2015-00277	Высокий	Высокий	CVE-2014-0518; apris-14-14	Уязвимость в Adobe Flash Player до 13.1
BDU-2014-00364	Высокий	Высокий	CVE-2014-1809; MS14-024	Уязвимость ASLR в MSCOMCTL (MS14-0...
BDU-2015-00280	Высокий	Высокий	CVE-2014-0519; apris-14-14	Уязвимость в Adobe Flash Player до 13.1
BDU-2015-00266	Высокий	Высокий	CVE-2014-0510; apris-14-14	Переполнение кучи в Adobe Flash Play
BDU-2014-00363	Сканировано	Высокий	CVE-2014-1808; MS14-023	Уязвимость повторного использования
BDU-2015-00278	Высокий	Высокий	CVE-2014-0517; apris-14-14	Уязвимость в Adobe Flash Player до 13.1
BDU-2014-00362	Высокий	Высокий	CVE-2014-1807; MS14-022	Уязвимость Microsoft Office, casual...
BDU-2015-00279	Высокий	Высокий	CVE-2014-0520; apris-14-14	Уязвимость в Adobe Flash Player до 13.0.0.214, Adobe AIR SDK до...
BDU-2014-00167	Высокий	Высокий	CVE-2014-1741; stable-channel-u...	Уязвимость в Google Chrome до 34.0.1847.137 (stable-channel-update)
BDU-2014-00169	Высокий	Высокий	CVE-2014-1740; stable-channel-u...	Уязвимость в Google Chrome до 34.0.1847.137 (stable-channel-update)
BDU-2014-00212	Высокий	Высокий	CVE-2014-1742; stable-channel-u...	Уязвимость в Google Chrome до 34.0.1847.137 (stable-channel-update)
BDU-2014-00330	Высокий	Высокий	CVE-2014-1745; stable-channel-u...	Уязвимость в Google Chrome до 35.0.1916.114 (stable-channel-update)_20
BDU-2014-00332	Высокий	Высокий	CVE-2014-1743; stable-channel-u...	Уязвимость в Google Chrome до 35.0.1916.114 (stable-channel-update)_20
BDU-2014-00195	Сканировано	Высокий	CVE-2014-1748; stable-channel-u...	Уязвимость в Google Chrome до 35.0.1916.114 (stable-channel-update)_20
BDU-2014-00197	Сканировано	Высокий	CVE-2014-1747; stable-channel-u...	Уязвимость в Google Chrome до 35.0.1916.114 (stable-channel-update)_20
BDU-2014-00155	Сканировано	Высокий	CVE-2014-1747; stable-channel-u...	Уязвимость в Google Chrome до 35.0.1916.114 (stable-channel-update)_20
BDU-2014-00157	Сканировано	Высокий	CVE-2014-1746; stable-channel-u...	Уязвимость в Google Chrome до 35.0.1916.114 (stable-channel-update)_20
BDU-2014-00382	Высокий	Высокий	CVE-2014-1813; MS15-022	Уязвимость Web Applications, связанная с содержанием страниц...
BDU-2015-00574	Высокий	Высокий	CVE-2014-4247; cpeuj2014-19729?	Неопределенная уязвимость в Oracle Java SE BuS (cpeuj2014-1972956)
BDU-2015-00542	Сканировано	Высокий	CVE-2014-4265; cpeuj2014-19729?	Неопределенная уязвимость в Oracle Java SE BuS 6u75, 7u60, и BuS...
BDU-2015-00410	Высокий	Высокий	CVE-2014-4241; cpeuj2014-19729?	Неопределенная уязвимость в Oracle Java SE BuS 6u75, 7u60, и BuS...

Обратная связь



Банк данных угроз безопасности информации

Федеральная служба по техническому и экспортному контролю

ФСТЭК России

Государственный научно-исследовательский испытательный институт проблем технической информации

ФАУ «ГНИИИ ПТЗИ ФСТЭК России»

Угрозы Уязвимости ▾ Документы ▾ Термины Обратная связь ▾ Обновления ▾ Участники ▾ ФСТЭК России

Главная / Список угроз

ФИЛЬТРАЦИЯ

Контекстный поиск по названию угрозы

Введите слово или словосочетание

Источник угрозы

Доступен множественный выбор

Последствия реализации угрозы:

Нарушение конфиденциальности ☐

Нарушение целостности ☐

Нарушение доступности ☐

Сброс

Применить



Написать
администратору



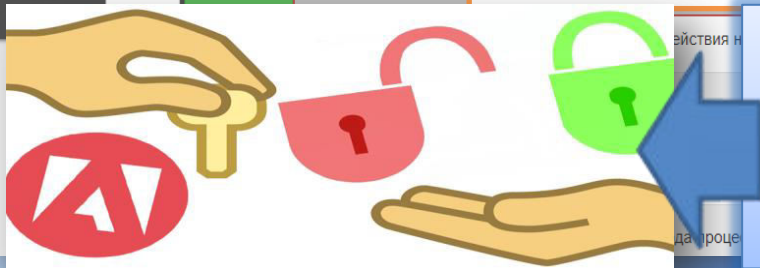
Электронная
почта



Сообщить об
уязвимости



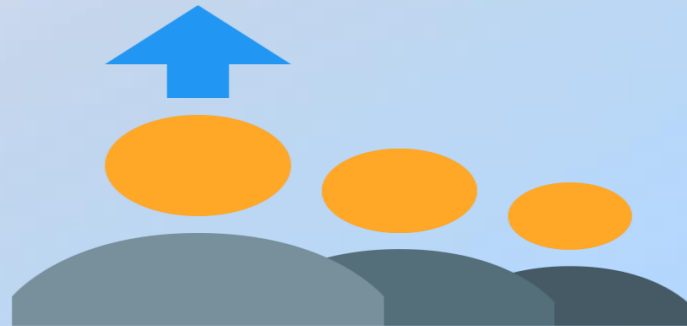
Сообщить об
угрозе



PGP ключ

Отпечаток ключа: **2C0C ECDB F42D 4009 3F62**
C17E 924D 91FE F309 92A2

Инициативные исследователи



Банк данных угроз безопасности информации

Федеральная служба по техническому и экспортному контролю
ФСТЭК России

Государственный научно-исследовательский испытательный институт
проблем технической защиты информации
ФГУП «НИИ ИТЗИ ФСТЭК России»

Угрозы · Уязвимости · Документы · Термины · Обратная связь · Обновления · Участники · ФСТЭК России

Главная · Участники · Исследователи

Сведения об уязвимостях, поступившие от исследователей через раздел "Обратная связь"

Описание уязвимости

уязвимость операционной системы FortiOS, позволяющая осуществлять мейсайтовые сценарные атаки	Статус уязв.
уязвимость системы управления бизнес-процессами, связанная с недостаточной защитой структуры веб-страницы	Принята
уязвимость механизма загрузки DLL-файлов системы управления	Принята
уязвимость, связанная с наличием предустановленных учетных данных системы управления	Принята
уязвимость автоматизированной системы управления, позволяющая осуществлять мейсайтовые сценарные атаки	Принята
уязвимость механизма загрузки DLL-файлов автоматизированной системы управления	Принята
уязвимость автоматизированной системы управления, связанная с переполнением буфера в памяти	Принята
уязвимость системы управления обучением и развитием, позволяющая нарушителю выполнить вредоносный код в браузере пользователя	Рассматривается
уязвимость системы управления обучением и развитием, позволяющая нарушителю получить доступ к файловым хранилищам других пользователей	Рассматривается
уязвимость системы управления обучением и развитием, позволяющая нарушителю изменить содержимое чужого портфолио	Рассматривается

Количество уязвимостей: 46
Добавлено в очередь: 22
Добавлено в банк данных: 18

Количество угроз: 17
Принято: 4

Регламент включения информации об уязвимостях

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ
(ФСТЭК РОССИИ)

УТВЕРЖДЕН
ФСТЭК России 26 июня 2018 г.

МЕТОДИЧЕСКИЙ ДОКУМЕНТ

РЕГЛАМЕНТ
ВКЛЮЧЕНИЯ ИНФОРМАЦИИ ОБ УЯЗВИМОСТЯХ ПРОГРАММНОГО
ОБЕСПЕЧЕНИЯ И ПРОГРАММНО-АППАРАТНЫХ СРЕДСТВ В БАНК
ДАННЫХ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ ФСТЭК РОССИИ

2018

Оператор сайта
БДУ

Исследователи

Разработчики



Порядок обработки
и устранения
уязвимостей



Порядок раскрытия
информация об
уязвимости в БДУ



<https://bdu.fstec.ru/site/regulations> 

Работы по Регламенту

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ТЕХНИЧЕСКОМУ ИЭКСПОРТНОМУ КОНТРОЛЮ
(ФСТЭК РОССИИ)

УТВЕРЖДЁН
ФСТЭК России 26 июня 2018 г.

МЕТОДИЧЕСКИЙ ДОКУМЕНТ

РЕГЛАМЕНТ
ВКЛЮЧЕНИЯ ИНФОРМАЦИИ ОБ УЯЗВИМОСТЯХ ПРОГРАММНОГО
ОБЕСПЕЧЕНИЯ И ПРОГРАММНО-АППАРАТНЫХ СРЕДСТВ В БАНК
ДАННЫХ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ ФСТЭК РОССИИ



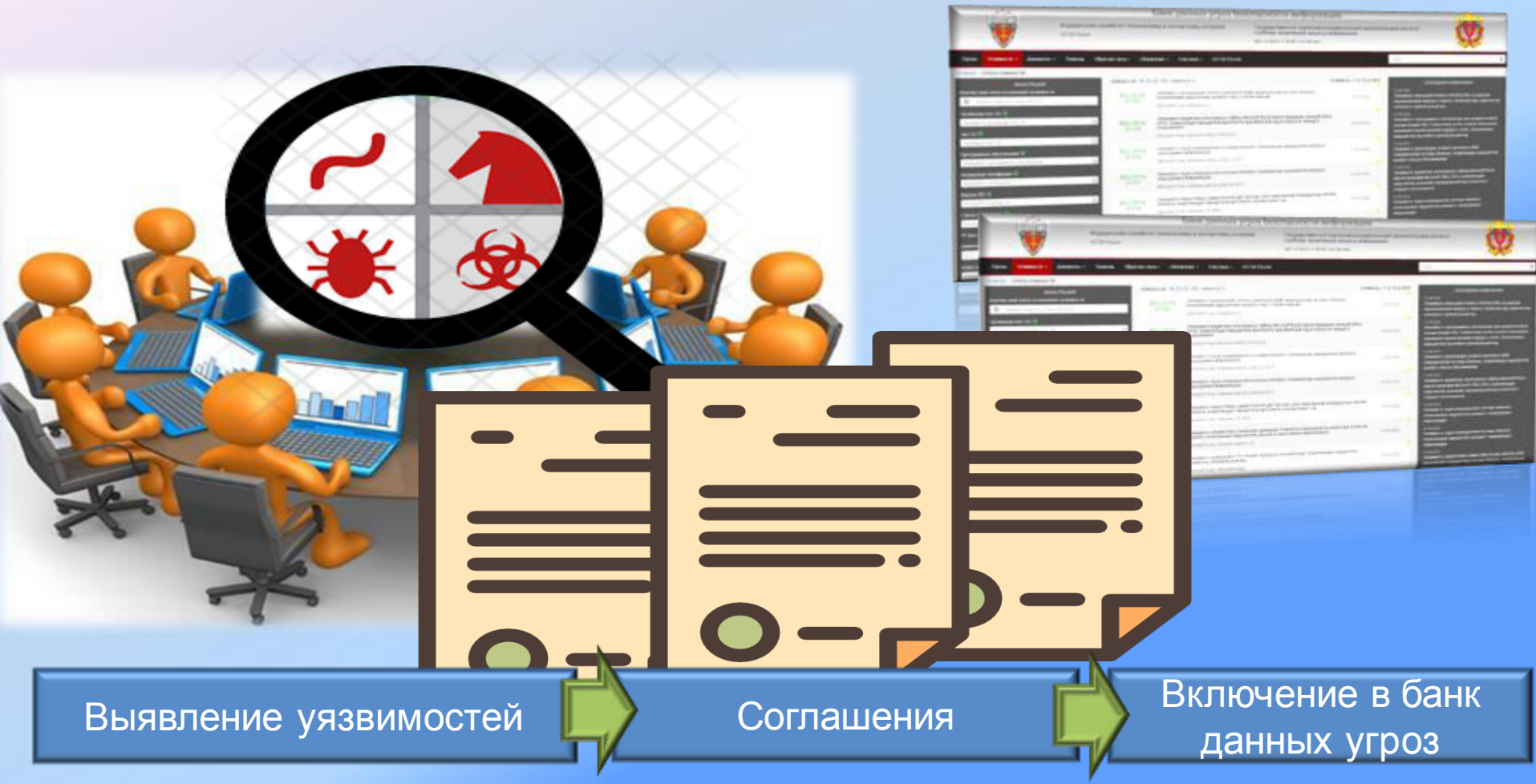
Включены **25**
уязвимостей

10 исследователей

8 организаций



Взаимодействие с исследователями (соглашения)



Рейтинг исследователей

Рейтинг исследователей, предоставивших сведения об уязвимостях программного обеспечения

Благодарим исследователей за предоставленную информацию об уязвимостях программного обеспечения!

Рейтинг исследователя определяется суммированием всех рейтинговых баллов, полученных исследователями за предоставленные сведения об уязвимостях программного обеспечения. Рейтинговые баллы рассчитываются в соответствии с [Порядком определения рейтинга](#), установленным в соответствии с [Регламентом включения уязвимостей](#).

Позиция в рейтинге	Исследователь	Кол-во 	Важность 	Качество 	Критичность 	Рейтинг
1.	Владислав Саиченко	7	7.14	3.00	5.71	104.00
2.	Андрей Лосьяников	3	10.00	1.00	4.67	44.00
3.	Георгий Бирюзов	3	5.00	3.00	4.00	33.00

Приложение № 2
к Регламенту включения информации
об уязвимостях программного обеспечения
и программно-аппаратных средств
в банк данных угроз безопасности
информации ФСТЭК России

Определение рейтинга исследователей, предоставивших информацию об уязвимостях в Банк данных угроз

Исследователь получает рейтинговые баллы за предоставленные сведения об уязвимостях в Банк данных угроз безопасности при выполнении следующих условий:

- сведения об уязвимости не опубликованы ранее в Банке данных угроз или других общедоступных источниках;
- исследователем представлены информация об уязвимости и контактная информация исследователя в соответствии с Регламентом обращения с информацией об уязвимостях программного обеспечения и программно аппаратных средств в Банке данных угроз безопасности информации ФСТЭК России.

Количество рейтинговых баллов за выявленную -уязвимость определяется по следующей формуле:

$$A = (T + P + R) * C, \text{ где}$$

T – показатель, характеризующий объект исследований (выбирается тип программного обеспечения с максимальным значением);

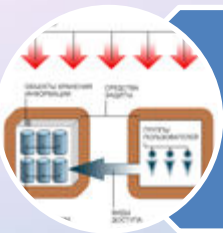
P – показатель, характеризующий алгоритм проверки уязвимости и подтверждающие материалы;

R – показатель, характеризующий уровень опасности уязвимости;

C – показатель, характеризующий количество затрагиваемого программного обеспечения.

Общий рейтинг исследователя определяется простым суммированием всех рейтинговых баллов, полученных исследователем за информацию об уязвимостях, сведения о которых были представлены в Банк данных угроз.

Средство автоматизации по определению угроз безопасности информации



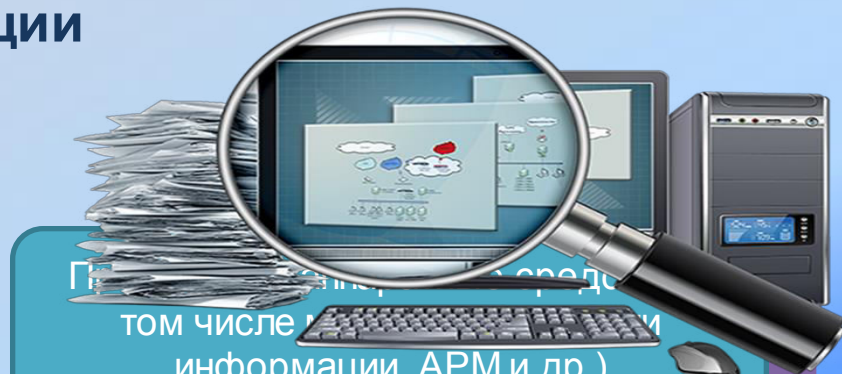
Задание структурно-функциональных характеристик информационных систем



Обнаружение на основе заданных классификационных признаков вероятных угроз безопасности информации



Формирование отчета о вероятных угрозах безопасности информации



Где хранятся данные (в том числе и в среде информации, АРМ и др.)

(микропрограммное обеспечение, общесистемное ПО, прикладное ПО)

Архитектура и конфигурация

телекоммуникационное оборудование

Перечень возможных угроз безопасности информации

Выявление уязвимостей в информационных системах под управлением операционных систем Linux



Федеральная служба
по техническому регулированию
и метрологии
ФСТЭК России

Государственный
технический университет
«Специальный техникум»
г. Москва

Федеральный испытательный институт
по метрологии, стандартизации и
техническому регулированию

Угрозы Уязвимости Документы Термины Обратная связь Обновления Участники ФСТЭК России

Поиск

Главная / Программа ScanOVAL

Программа **ScanOVAL** для автоматизированных проверок наличия уязвимостей программного обеспечения

Программа ScanOVAL предназначена для оперативного автоматизированного обнаружения уязвимостей программного обеспечения на рабочих станциях и серверах, функционирующих под управлением операционных систем семейства Microsoft Windows. В настоящее время проводится **опытная эксплуатация** программы ScanOVAL.

Замечания и предложения по работе программы ScanOVAL принимаются с использованием **формы обратной связи** или посредством **электронной почты**.

Перед использованием программы, пожалуйста, ознакомьтесь с **настройками Лицензионным соглашением** с конечным пользователем программы ScanOVAL, а также **Руководством оператора**.

Программа ScanOVAL обеспечивает выполнение следующих основных функций:

- загрузка XML-файлов с OVAL-описаниями уязвимостей, выполненными в соответствии со стандартом «The OVAL Language Specification» версии не ниже 5.10.1;
- обнаружение на основании обработки данных, представленных в XML-файлах, уязвимостей программного обеспечения, установленного на локальной ПЭВМ, работающей под управлением операционной системы семейства Microsoft Windows.

Для работы программы ScanOVAL аппаратная конфигурация компьютера должна соответствовать следующим минимальным требованиям.

- 32-разрядный (x86) или 64-разрядный (x64) процессор с тактовой частотой 1 ГГц или выше;
- 1 Гб (для 32-разрядной системы) или 2 Гб (для 64-разрядной системы) оперативной памяти;
- 0,5 Гб свободного места на жестком диске;
- графическое устройство DirectX 9 с драйвером WDDM 1.0 или более поздней версии.

для Linux



Спасибо за внимание!

Гефнер Ирина Сергеевна
otd22@fstec.ru
www.fstec.ru