

Банк данных угроз безопасности информации как инструмент для разработчика программного обеспечения



Докладчик: Сердечный Алексей

ФАУ «ГНИИИ ПТЗИ ФСТЭК России»



БАНК ДАННЫХ УРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ



2



Выводить по: 10, 20, 50, 100 Элементы с 1 по 10 из 182

Идентификатор	Описание угрозы
УБИ. 001	Угроза автоматического распространения вредоносного кода в грид-системе
УБИ. 002	Угроза агрегирования данных, передаваемых в грид-системе
УБИ. 003	Угроза анализа криптографических алгоритмов и 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

ФИЛЬТРАЦИЯ

- Контекстный поиск по названию уязвимости
- Производитель ПО
- Тип ПО
- Программное обеспечение
- Аппаратная платформа
- Версия ПО
- Статус уязвимости
- Доп. параметры
- Диапазон дат

Выводить по: 10, 20, 50, 100 Элементы с 1 по 10 из 14129

Идентификатор	Описание уязвимости	Дата
BDU:2016-01374	Уязвимость интерпретатора PHP, позволяющая нарушителю читать произвольные файлы или записывать в них	16.05.2016
BDU:2016-01373	Уязвимость интерпретатора PHP, позволяющая нарушителю получить доступ на чтение файлов	16.05.2016
BDU:2016-01372	Уязвимость интерпретатора PHP, позволяющая нарушителю выполнить произвольный код	16.05.2016
BDU:2016-01371	Уязвимость интерпретатора PHP, позволяющая нарушителю читать произвольные файлы или записывать в них	16.05.2016
BDU:2016-01370	Уязвимость интерпретатора PHP, позволяющая нарушителю вызвать отказ в обслуживании, получить конфиденциальную информацию или выполнить произвольный код	16.05.2016
BDU:2016-01369	Уязвимость интерпретатора PHP, позволяющая нарушителю вызвать отказ в обслуживании или выполнить произвольный код	16.05.2016

ИЗМЕНЕНИЯ

- 31.05.2016 Уязвимость интерпретатора PHP, позволяющая нарушителю читать произвольные файлы или записывать в них
- 31.05.2016 Уязвимость интерпретатора PHP, позволяющая нарушителю получить доступ на чтение файлов
- 31.05.2016 Уязвимость интерпретатора PHP, позволяющая нарушителю вызвать отказ в обслуживании или выполнить произвольный код



Уязвимости – 16 373



Угрозы – 194

По состоянию на 19.05. 2017

Вкладка «Угрозы»

БДУ - Угрозы x +

Яндекс bdu.fstec.ru/threat/ubi.001 16 Поиск



Банк данных угроз безопасности информации

Федеральная служба по техническому и экспортному контролю
ФСТЭК России

Государственный научно-исследовательский испытательный институт проблем технической защиты информации
ФАУ «ГНИИИ ПТЗИ ФСТЭК России»



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

Поиск

[Главная](#) / [Список угроз](#) / УБИ.001

УБИ.001: Угроза автоматического распространения вредоносного кода в грид-системе Вид ▾

Описание угрозы	Угроза заключается в возможности внедрения и запуска вредоносного кода от имени доверенного процесса на любом из ресурсных центров грид-системы и его автоматического распространения на все узлы грид-системы. Данная угроза обусловлена слабостями технологии грид-вычислений – высоким уровнем автоматизации при мало й администрируемости грид-системы. Реализация данной угрозы возможна при условии наличия у нарушителя привилегий легального пользователя грид-системы
Источники угрозы	Внутренний нарушитель со средним потенциалом Внешний нарушитель со средним потенциалом
Объект воздействия	Ресурсные центры грид-системы
Последствия реализации угрозы	Нарушение конфиденциальности Нарушение целостности Нарушение доступности

Назад к списку
Следующая ➔

ПОСЛЕДНИЕ ИЗМЕНЕНИЯ

01.12.2016
УБИ. 194 Угроза несанкционированного использования привилегированных функций мобильного устройства

07.12.2016
УБИ. 193 Угроза утечки информации за счет применения вредоносным программным обеспечением алгоритмов шифрования трафика

21.10.2016
УБИ. 192 Угроза использования уязвимых версий программного обеспечения

21.10.2016
УБИ. 191 Угроза внедрения вредоносного кода в дистрибутив программного обеспечения

24.10.2016
УБИ. 190 Угроза внедрения вредоносного кода за счет посещения зараженных сайтов в сети Интернет

Вкладка «Уязвимости»

БДУ - Уязвимости x +

Яндекс | bdu.fstec.ru/vul/2017-01100

16 | Поиск



Банк данных угроз безопасности информации

Федеральная служба по техническому и экспортному контролю
ФСТЭК России

Государственный научно-исследовательский испытательный институт проблем технической защиты информации
ФАУ «ГНИИИ ПТЗИ ФСТЭК России»



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

Поиск

Главная / Список уязвимостей / BDU:2017-01100

BDU:2017-01100: Уязвимость операционной системы Microsoft Windows, позволяющая нарушителю выполнить произвольный код Вид ▾

Описание уязвимости	Уязвимость протокола SMBv1 операционной системы Microsoft Windows существует из-за недостаточной проверки входных данных. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, выполнить произвольный код с помощью специально сформированных пакетов	
Вендор	Microsoft Corp.	
Наименование ПО	Windows	
Версия ПО	XP Server 2008 R2 SP1 Vista SP2 7 SP1 8	раскрыть
Тип ПО	Операционная система	
Операционные системы и аппаратные платформы	Microsoft Corp. Windows . x64 Microsoft Corp. Windows . x86	
Тип ошибки	Недостаточная проверка вводимых данных	

ПОСЛЕДНИЕ ИЗМЕНЕНИЯ

12.05.2017
Уязвимость программной платформы Flash Player, позволяющая нарушителю выполнить произвольный код

12.05.2017
[Уязвимости браузера Google Chrome, позволяющие нарушителю оказать другое воздействие или вызвать отказ в обслуживании](#)

12.05.2017
Уязвимость библиотеки OpenSSL, позволяющая нарушителю вызвать отказ в обслуживании

12.05.2017
Уязвимость антивирусного программного средства Internet Security, позволяющая нарушителю читать произвольные файлы

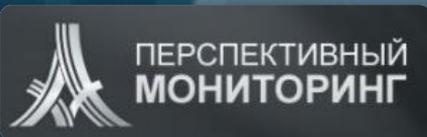
12.05.2017
Уязвимость пакета программ Microsoft Office Web Apps, пакета обеспечения совместимости Microsoft Office Compatibility Pack,

bdu.fstec.ru/vul/2016-01706 **CWE-20**

Взаимодействие по БДУ

Данные по угрозам ИБ

ИСПРАН



ГНИИ ПТЗИ
ФСТЭК России



БДУ ФСТЭК России

Данные по уязвимостям

Вкладка «Обратная связь»

БДУ - Создание сообщения о... x +

Яндекс | bdu.fstec.ru/contacts/vulreport

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

Главная / Список сообщений / Создание сообщения об уязвимости

Поля с символом *, обязательны для заполнения.

Информация об уязвимости

Наименование уязвимости * ?

Идентификаторы различных систем описаний уязвимостей ?

Описание уязвимости ?

Наименование программного обеспечения * ?

Версия программного обеспечения * ?

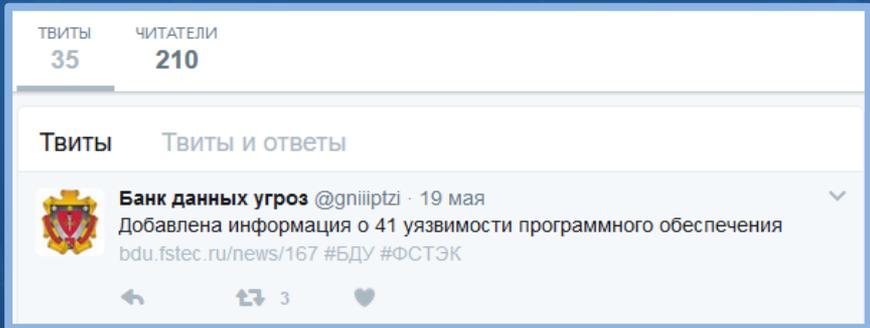
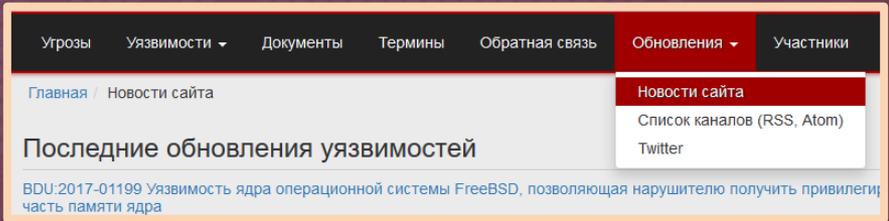
Тип ошибки CWE ?

ОБРАТНАЯ СВЯЗЬ

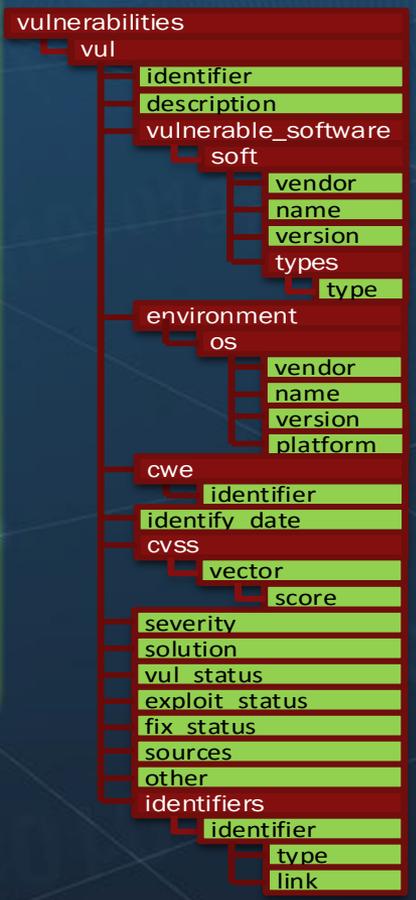
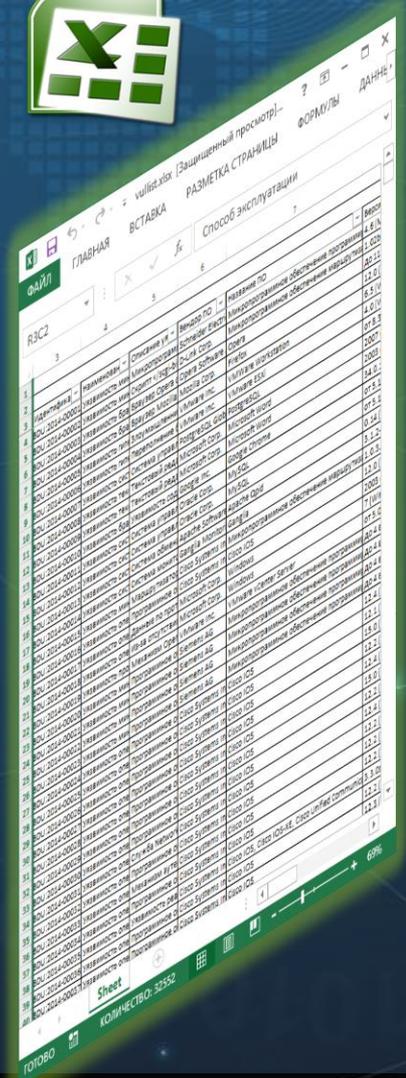
- Написать администратору
- Сообщить об уязвимости**
- Сообщить об угрозе
- Список сообщений

Способы получения сведений об угрозах и уязвимостях

Информирование о появлении новых сведений



Предоставление сведений



Поиск сведений об уязвимостях

ФИЛЬТРАЦИЯ

Контекстный поиск по названию уязвимости

Производитель ПО ?

Тип ПО ?

Программное обеспечение ?

Аппаратная платформа ?

Версия ПО ?

Статус уязвимости ?

Доп. параметры

Диапазон дат ?

Класс уязвимости ?

Уровень опасности ?

Базовый вектор ?

Идентификатор типа ошибки ?

Другие системы идентификации ?

Наличие эксплойта

Операционная система ?

Статистика обращений к фильтрам

ФИЛЬТРАЦИЯ

Контекстный поиск по названию уязвимости

4%

Производитель ПО ?

17%

Тип ПО ?

21%

Программное обеспечение ?

12%

Аппаратная платформа ?

4%

Версия ПО ?

5%

Статус уязвимости ?

4%

Доп. параметры

2% Диапазон дат ?

с по 1%

Класс уязвимости ?

2%

Уровень опасности ?

17%

Базовый вектор ?

New

Идентификатор типа ошибки ?

7%

Другие системы идентификации ?

1%

Наличие эксплойта

New

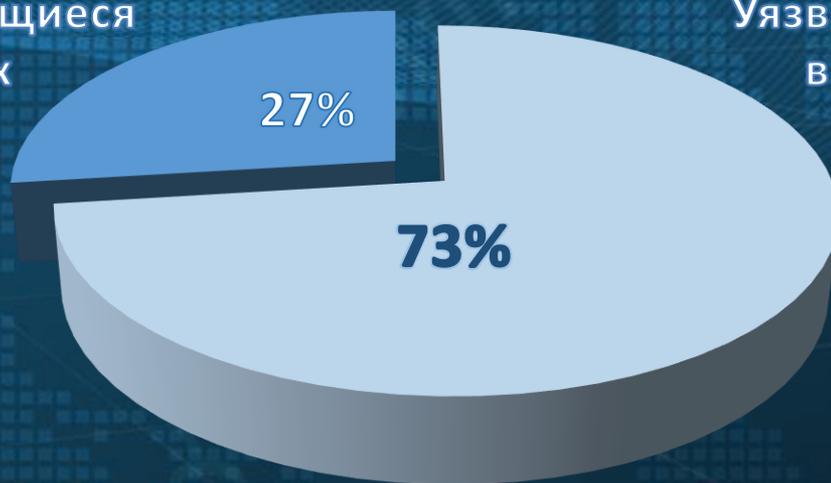
Операционная система ?

2%

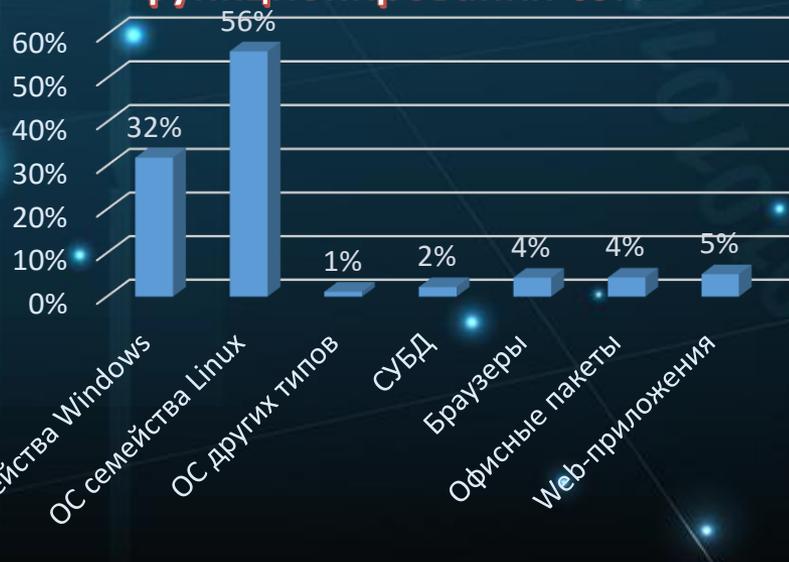
Статистика использования банка данных при сертификации ПО

Уязвимости, содержащиеся только в иностранных источниках

Уязвимости, вошедшие в БДУ ФСТЭК России



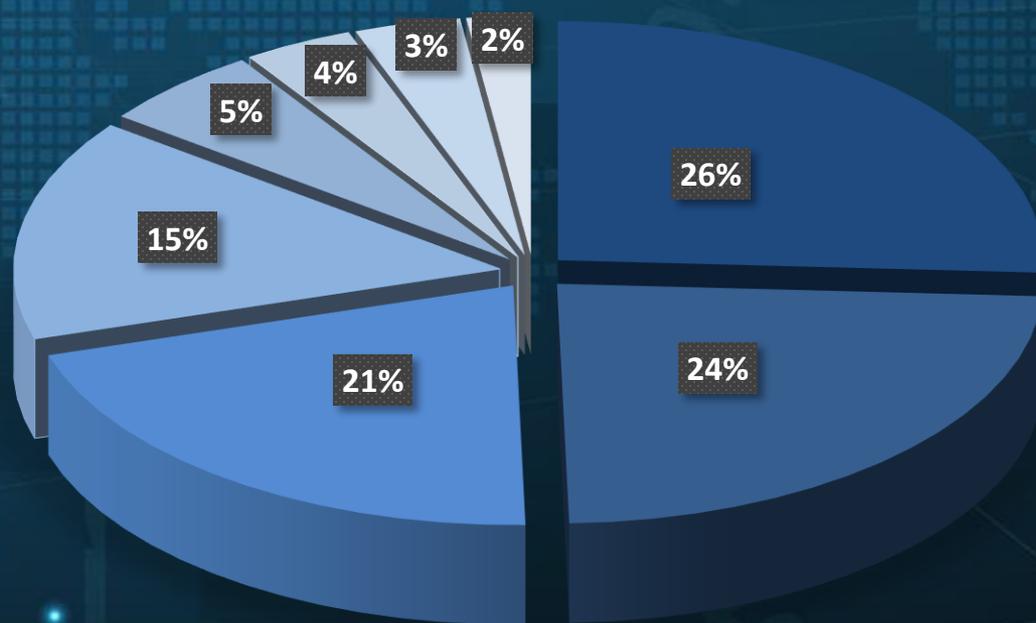
Доля уязвимостей ПО сред функционирования СЗИ



Доля уязвимостей объектов сертификации



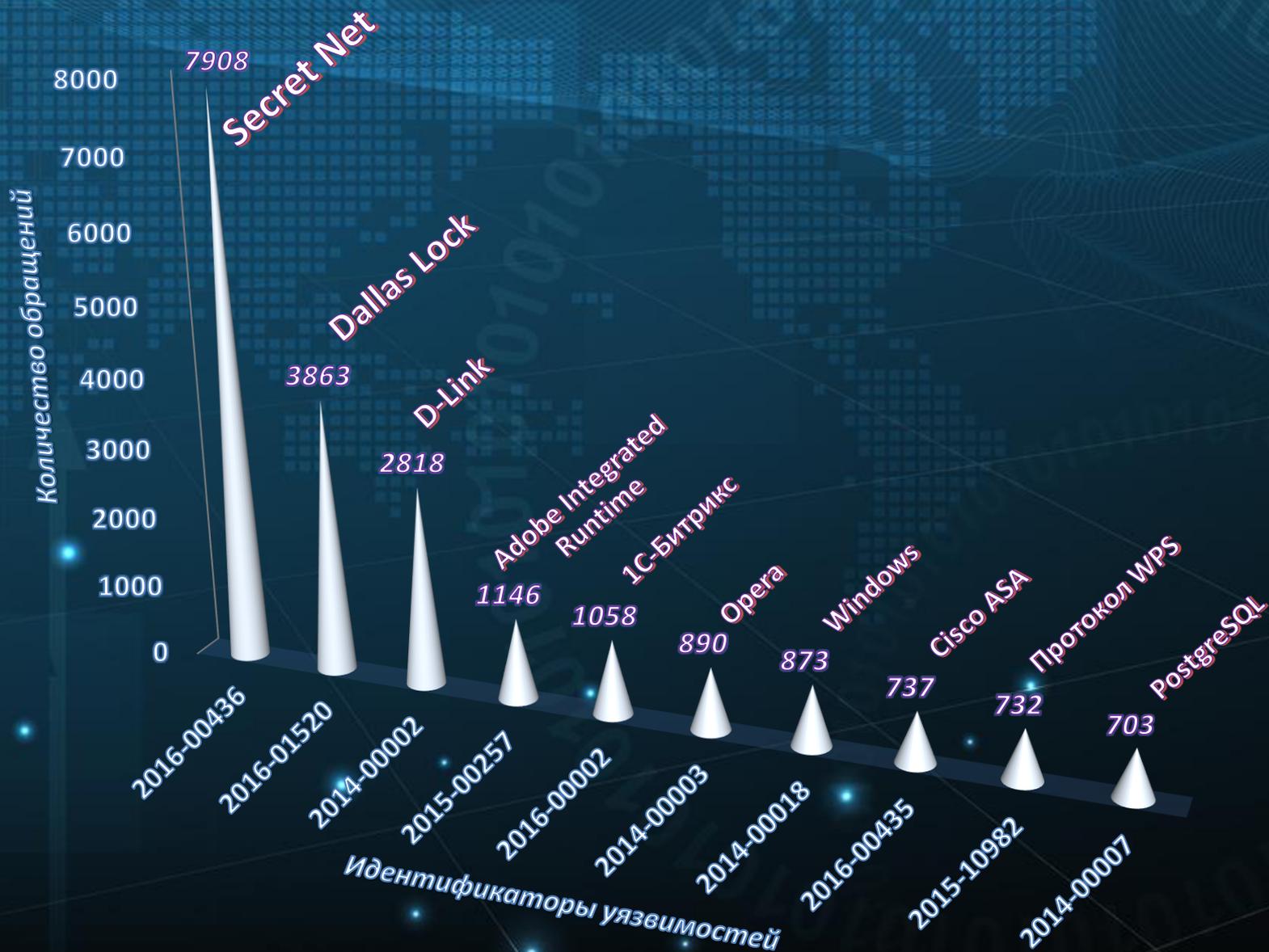
Количество уязвимостей в ПО различных производителей



Google Inc.	678
Adobe Systems Inc.	624
Microsoft Corp.	543
Apple Inc.	392
Oracle Corp.	144
Mozilla Corp.	95
Cisco Systems Inc.	93
PHP Group	56

Уязвимости внесены в Банк данных угроз
в период с 01.01.2016 – по 19.05.2017

Популярные уязвимости в 2016 году



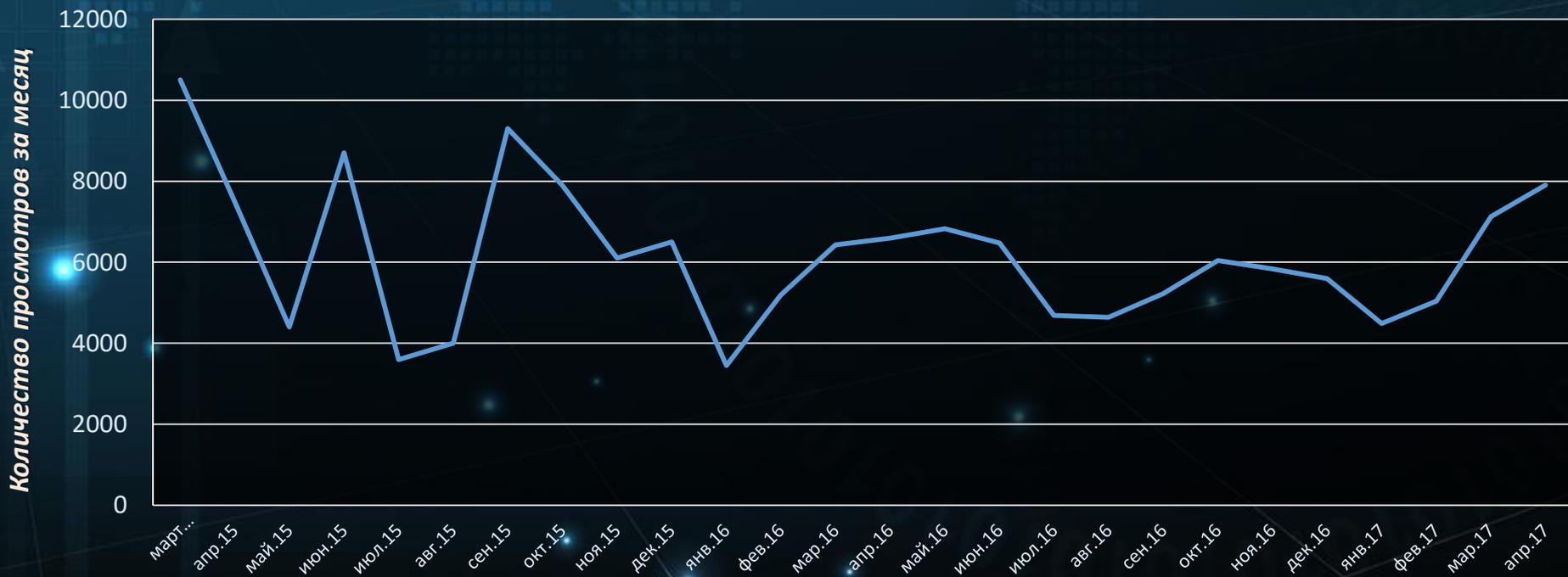
Статистика посещений БДУ ФСТЭК России



Просмотры страниц – 793 619

Суммарное количество визитов – 160 054

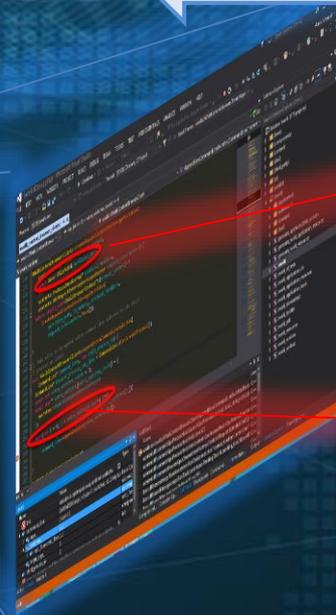
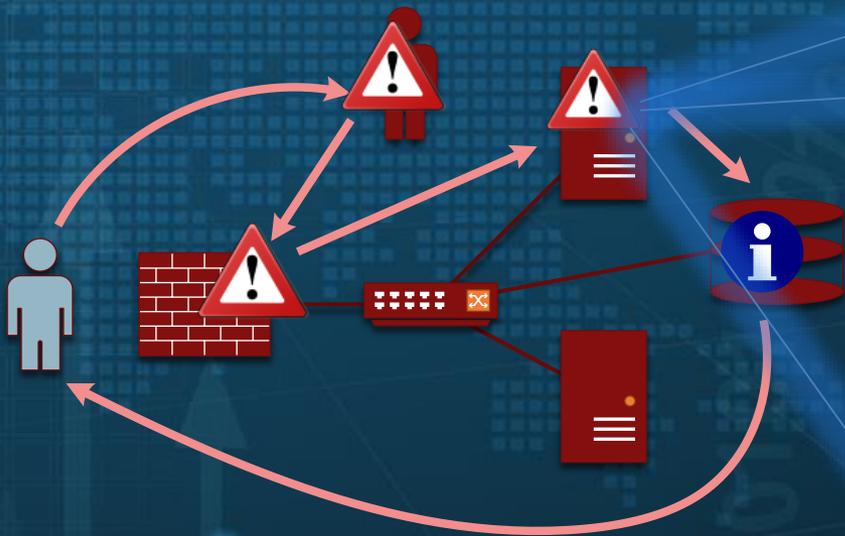
Уникальные посетители – 81 480



По состоянию на 15.05. 2017

База данных ошибок и ошибочных ситуаций

Угроза ← Уязвимость ← Недостаток (ошибка)



1+1=0
1<4-5
...
array[-1]=5
...

Международный опыт



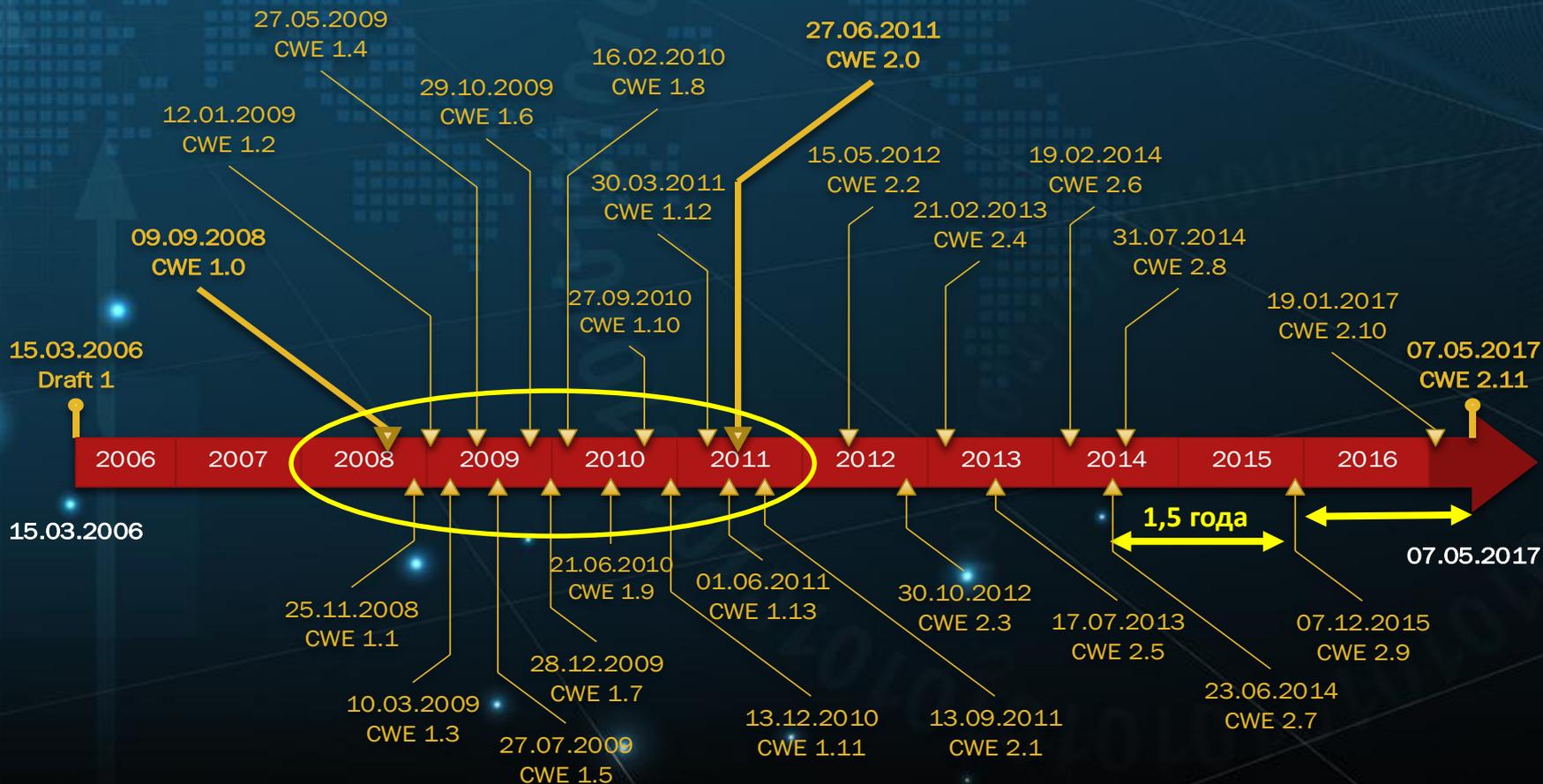
Стандарт CWE



Количество элементов: 1006 (17 устарели)

Крайняя версия: 2.11 (от 7.05.2017)

Участники разработки CWE
(более 50 организаций)



Типы элементов стандарта CWE

Коллекция
«View»

Категория
«Category»

Слабость
«Weakness»

Составной элемент
«Compound Elements»

CWE-699: Концепции разработки



CWE-189: Ошибки чисел



CWE-190:

CWE-191: Обратное целочисленное переполнение

CWE-680:

CWE-190: Целочисленное переполнение



CWE-120: Переполнение буфера

Динамика наполнения стандарта CWE

Количество добавленных элементов



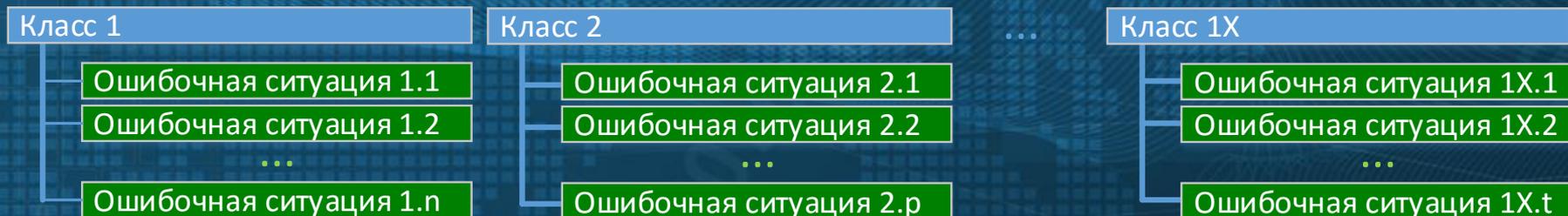
Поля описания элементов CWE

Название поля	Количество заполненных элементов (CWE 2.11)			
	Коллекция	Категория	Слабость	Сост. эл.
Идентификатор	33	243	705	8
Название				
Тип				
Описание				
Статус (готов/проект/в разработке)	0/14/19	0/48/195	4/387/314	0/6/2
Этап появления	-	4	664	5
Причина появления	-	1	75	1
Условия эксплуатации	-	0	23	0
Вероятность эксплуатации	-	2	185	3
Последствия от эксплуатации	-	2	698	8
Меры противодействия	-	6	522	4
Методы обнаружения	-	6	77	3
Пример кода с недостатком	-	4	370	8
Пример CVE	-	3	353	6
Языки программирования	-	22	554	8
Связанные шаблоны атак (CAPEC)	-	23	204	7
Связи	19	239	705	8
другие поля

Трудности использования стандарта CWE

- сложная структура стандарта;
- недостаточная детализация элементов для задач статического анализа;
- отсутствие удобных инструментов работы с базой данных CWE;
- отсутствие перевода на русский язык

Двухуровневая модель описания «ошибок» и «ошибочных ситуаций»



№ п/п	Название поля паспорта класса «ошибки»
1	Идентификатор класса «ошибки»
2	Наименование класса «ошибки»
3	Описание класса «ошибки»
4	Дата публикации сведений
5	Идентификаторы «ошибочных ситуаций»
6	Идентификаторы CWE

№ п/п	Название поля паспорта «ошибочной ситуации»
1	Идентификатор «ошибочной ситуации»
2	Наименование «ошибочной ситуации»
3	Описание «ошибочной ситуации»
4	Дата публикации сведений
5	Идентификаторы классов «ошибок»
6	Языки программирования
7	Примеры «ошибочной ситуации»
8	Идентификаторы CWE
9	Рекомендации по устранению «ошибочной ситуации»
10	Требования к методу выявления «ошибочной ситуации»
11	Уровень опасности «ошибочной ситуации»
12	Прочая информация

C/C++

Пример 1

PHP

Пример 4

C#

Пример 2

SQL

Пример 5

Java

Пример 3

другие

Примеры

Классы «ошибок»

ID	Наименование класса «ошибок»
BDE:01	Переполнение буфера
BDE:02	Разыменованное нулевого указателя
BDE:03	Утечка памяти или других ресурсов
BDE:04	Использование знаковых и беззнаковых чисел
BDE:05	Деление на ноль
BDE:06	Наличие мёртвого или недостижимого кода
BDE:07	Использование неинициализированных переменных
BDE:08	Непроверенное использование ввода пользователя
BDE:09	Некорректное использование многопоточных примитивов
BDE:10	Некорректное использование интерфейсов стандартных библиотек
BDE:11	Ошибки управления выделенной динамической памятью
BDE:12	Недостаточная обработка исключительных ситуаций
BDE:13	Некорректная реализация функций безопасности
BDE:14	Ошибки компиляции

Переполнение буфера



```

a=(c+i)*d;   for (i=1; i<1000; i++) {   a=func(...);
...          a=i*d+c;                 ...   b=func(...);
...                                     ...   ...
}                                           func(buf,...);

```

```

buf[a]=c;
...
int *buff = new[b];
...
c_func (buf, a, b);

```

индекс адрес размер

ID	Ошибочные ситуации, связанные с классом ошибок «Переполнение буфера»
001	Переполнение буфера с использованием размера и индекса буфера константного размера (внутри одной функции)
002	Переполнение буфера с использованием адреса, размера или индекса буфера, полученного как параметр функции или как результат вызова функции
003	Переполнение буфера с использованием размера или индекса буфера, полученного в результате арифметических вычислений
004	Переполнение буфера после предварительных сравнений индекса буфера с размером или основанными на нем вычислениями
005	Переполнение буфера после вычисления индекса, размера или адреса буфера в цикле
006	Переполнение буфера в результате передачи неверных значений размера, индекса или адреса буфера в стандартные библиотечные функции
007	Переполнение буфера в результате использования индекса или размера буфера, зависящего от ввода пользователя

Спасибо за внимание !

Использованные источники:

1. <http://bdu.fstec.ru> – Банк данных угроз безопасности информации
2. <https://cwe.mitre.org> –Общий перечень недостатков
3. <https://www.securecoding.cert.org> – Стандарты безопасного кодирования
4. <https://samate.nist.gov/BF/> - Bugs Framework