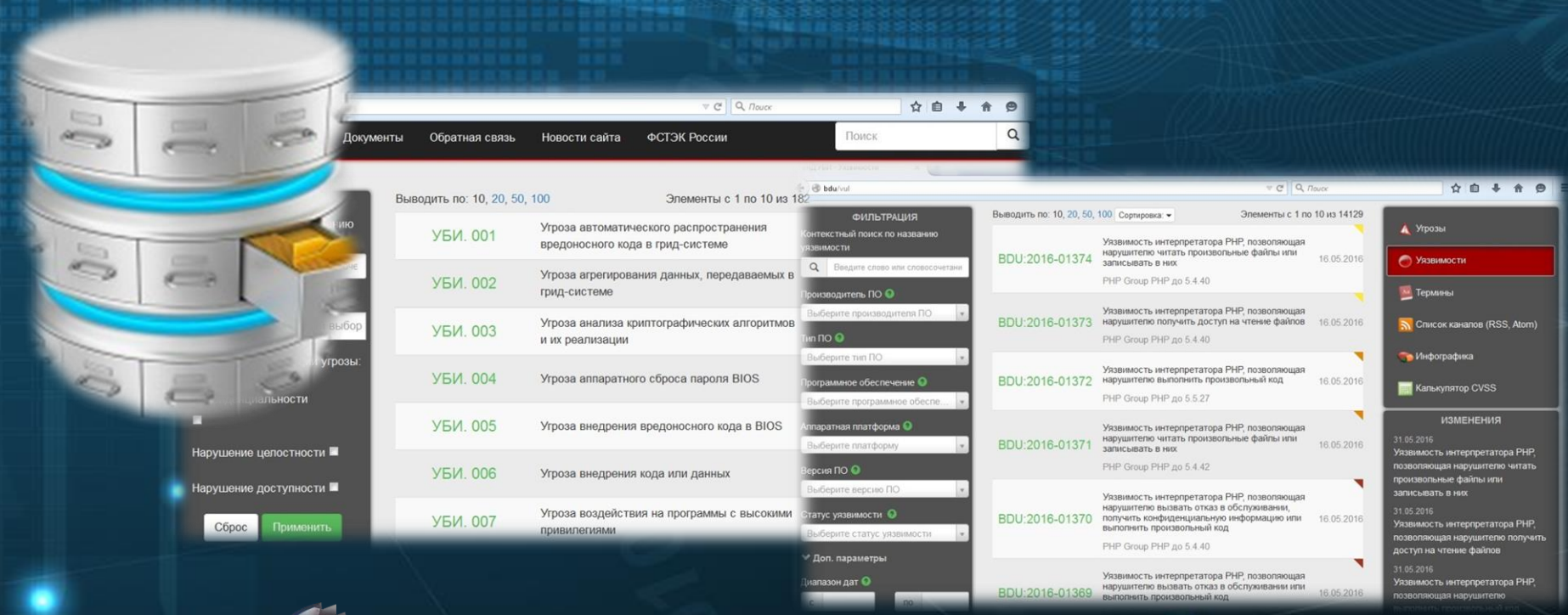
Банк данных угроз безопасности информации как инструмент для разработчика программного обеспечения

Докладчик: Сердечный Алексей

ФАУ «ГНИИИ ПТЗИ ФСТЭК России»

БАНК ДАННЫХ УРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

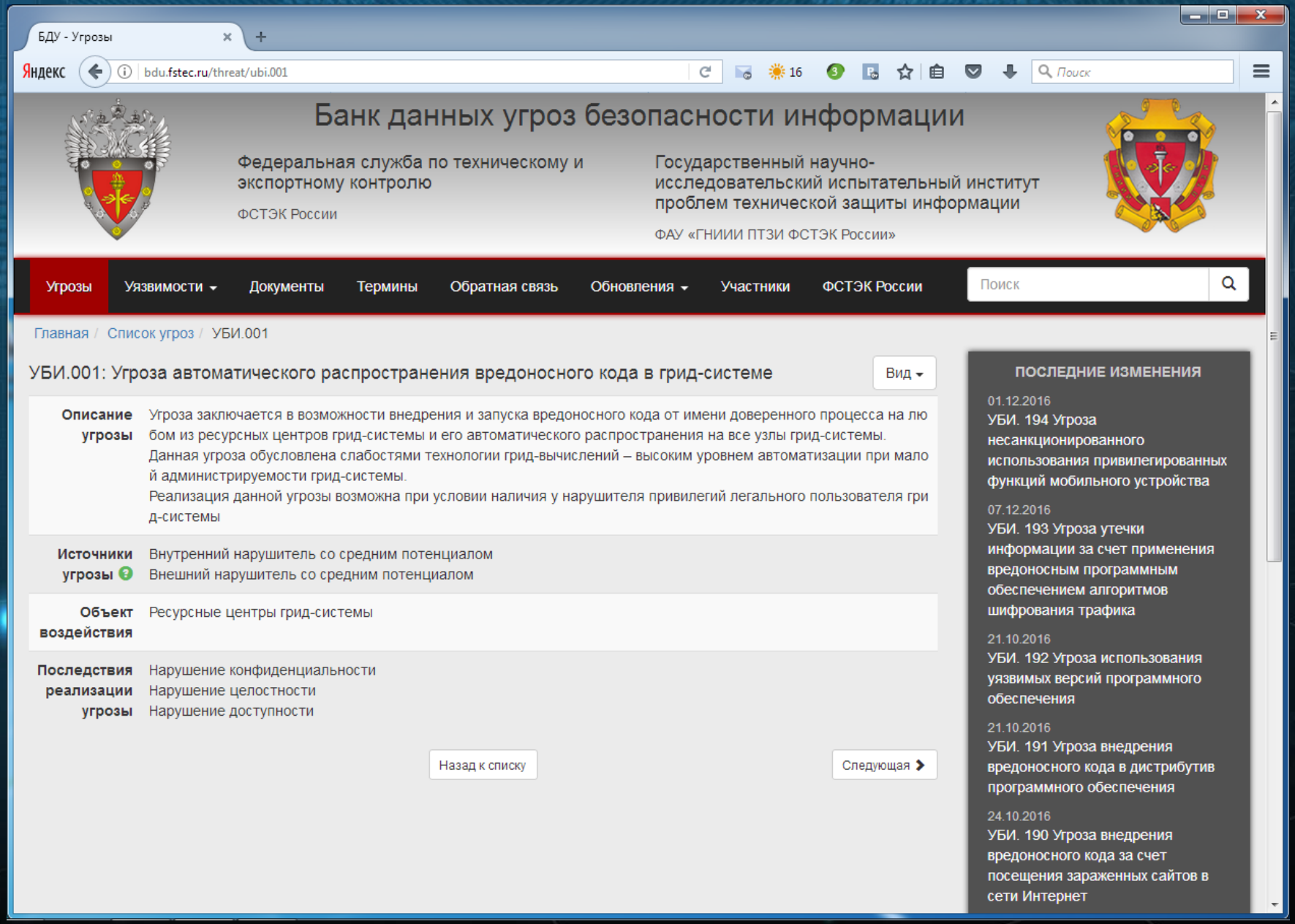


Уязвимости – 16 373

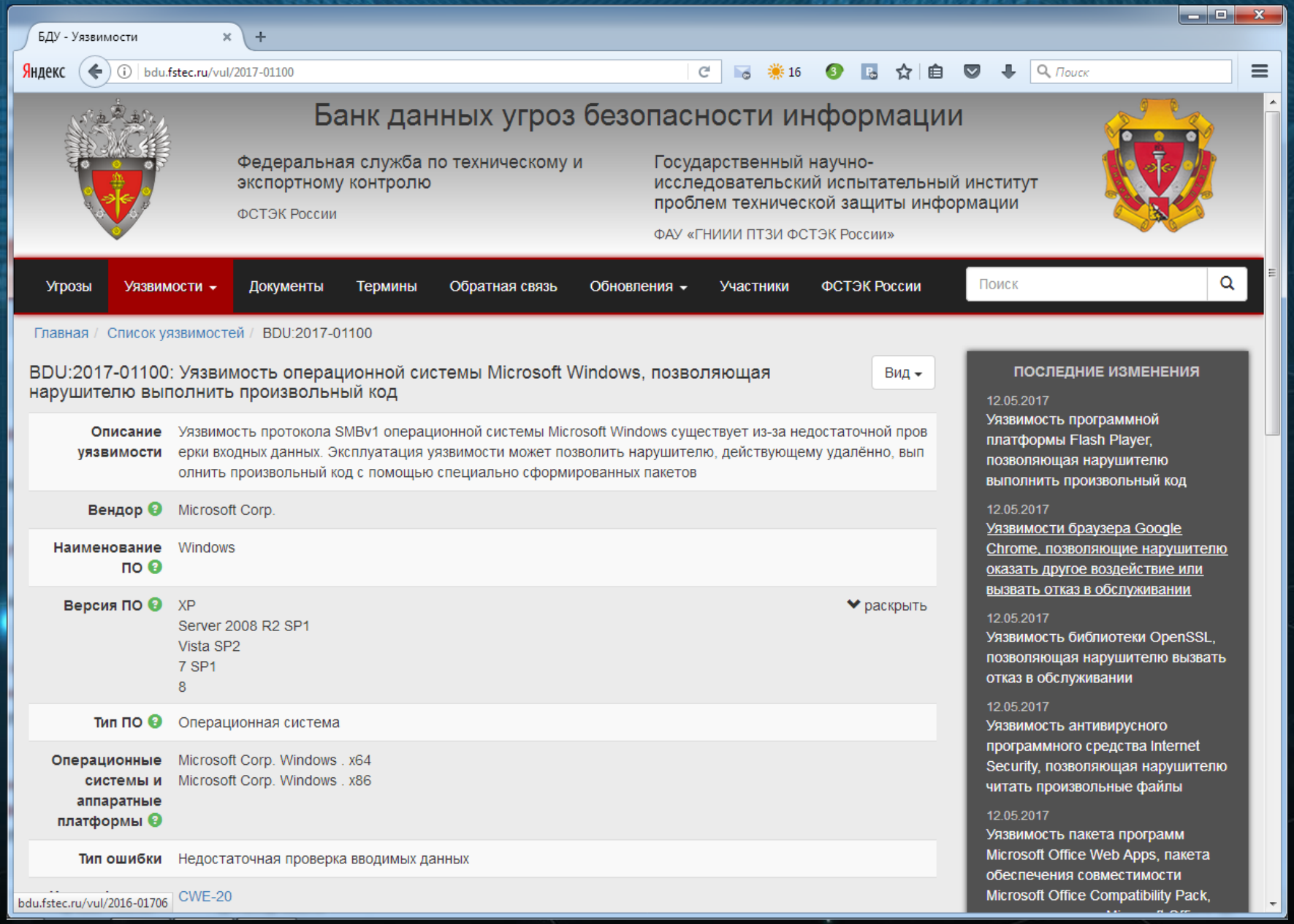
Угрозы – 194

По состоянию на 19.05. 2017

Вкладка «Угрозы»



Вкладка «Уязвимости»



Взаимодействие по БДУ

ИСП РАН

СИНАРА информ защита

Digital Security

ПЕРСПЕКТИВНЫЙ МОНИТОРИНГ

Научно-производственное объединение РусБИТех Открытое акционерное общество

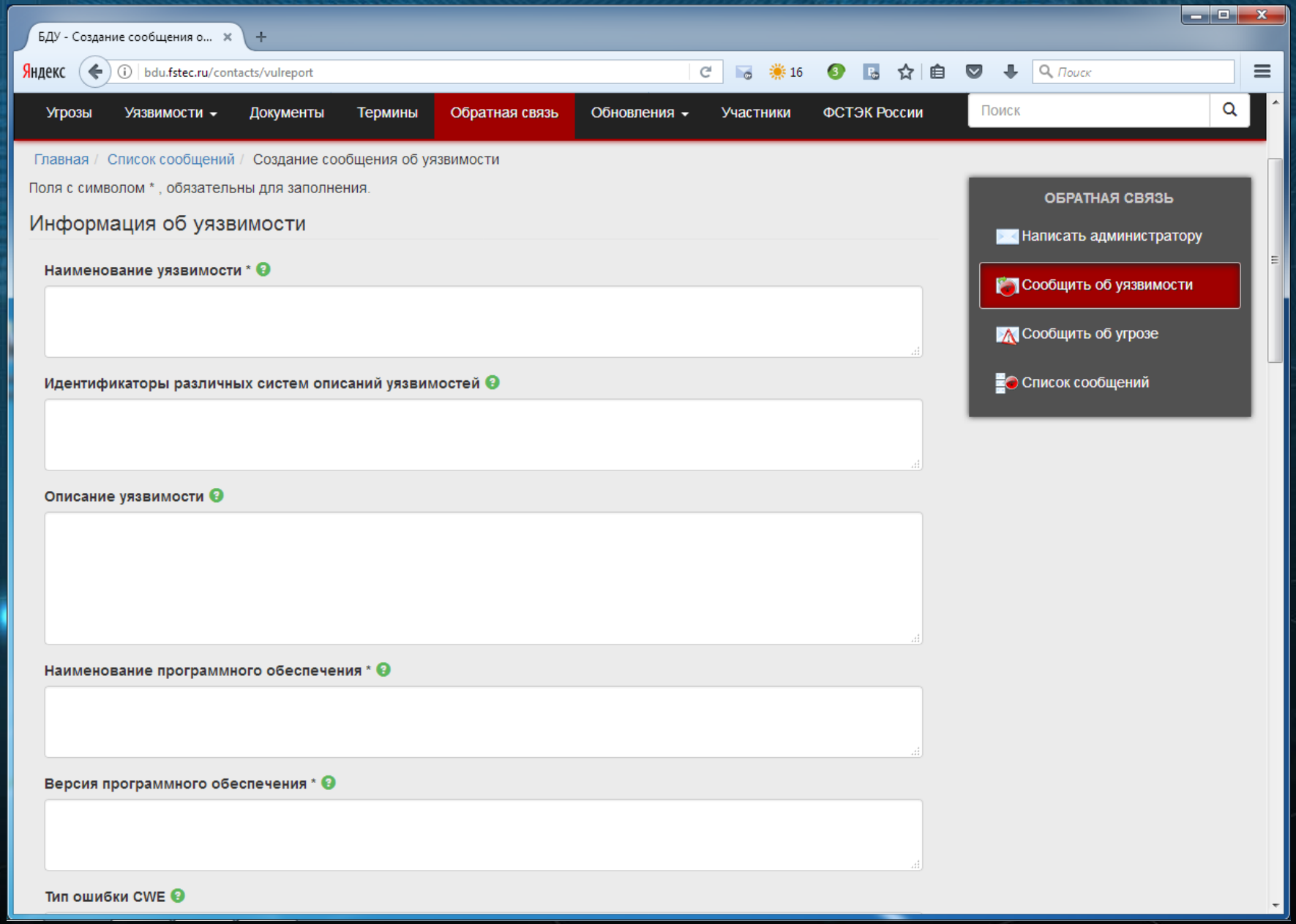
Данные по угрозам ИБ

ГНИИИ ПТЗИ ФСТЭК России

БДУ ФСТЭК России

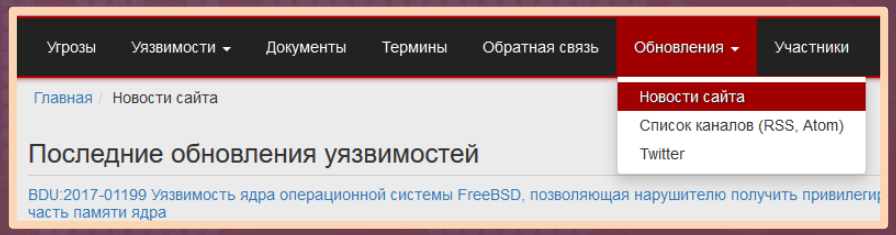
Данные по уязвимостям

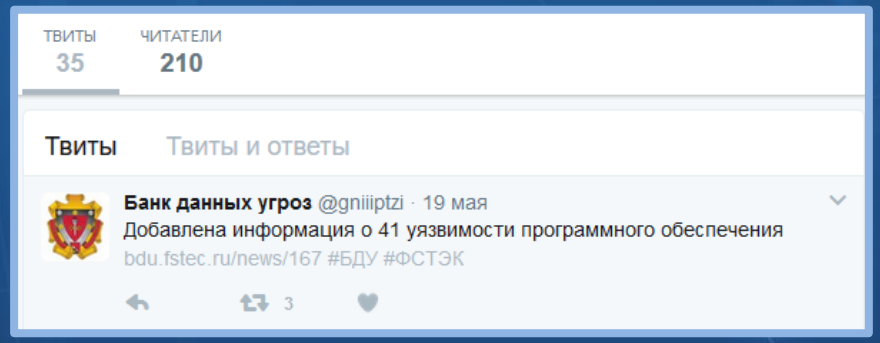
Вкладка «Обратная связь»



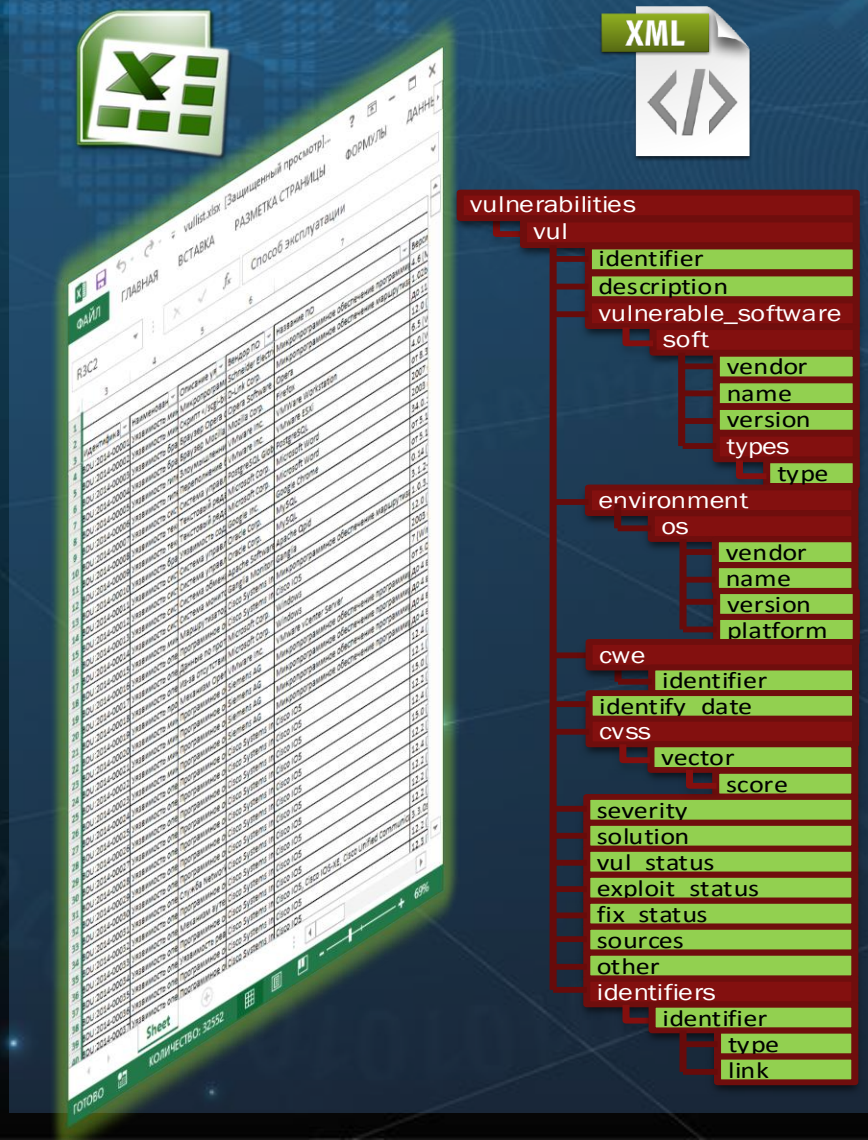
Способы получения сведений об угрозах и уязвимостях

Информирование о появлении новых сведений

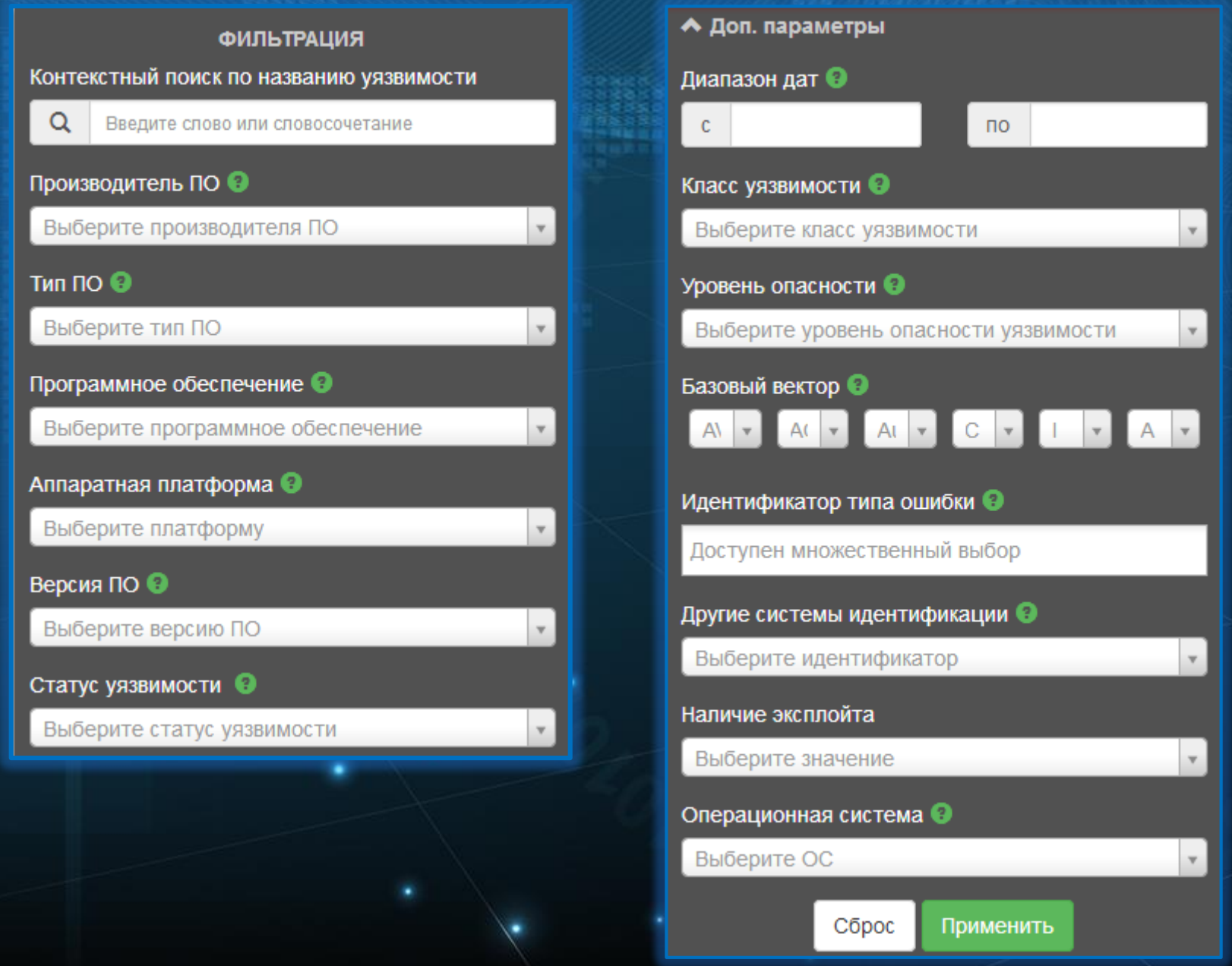




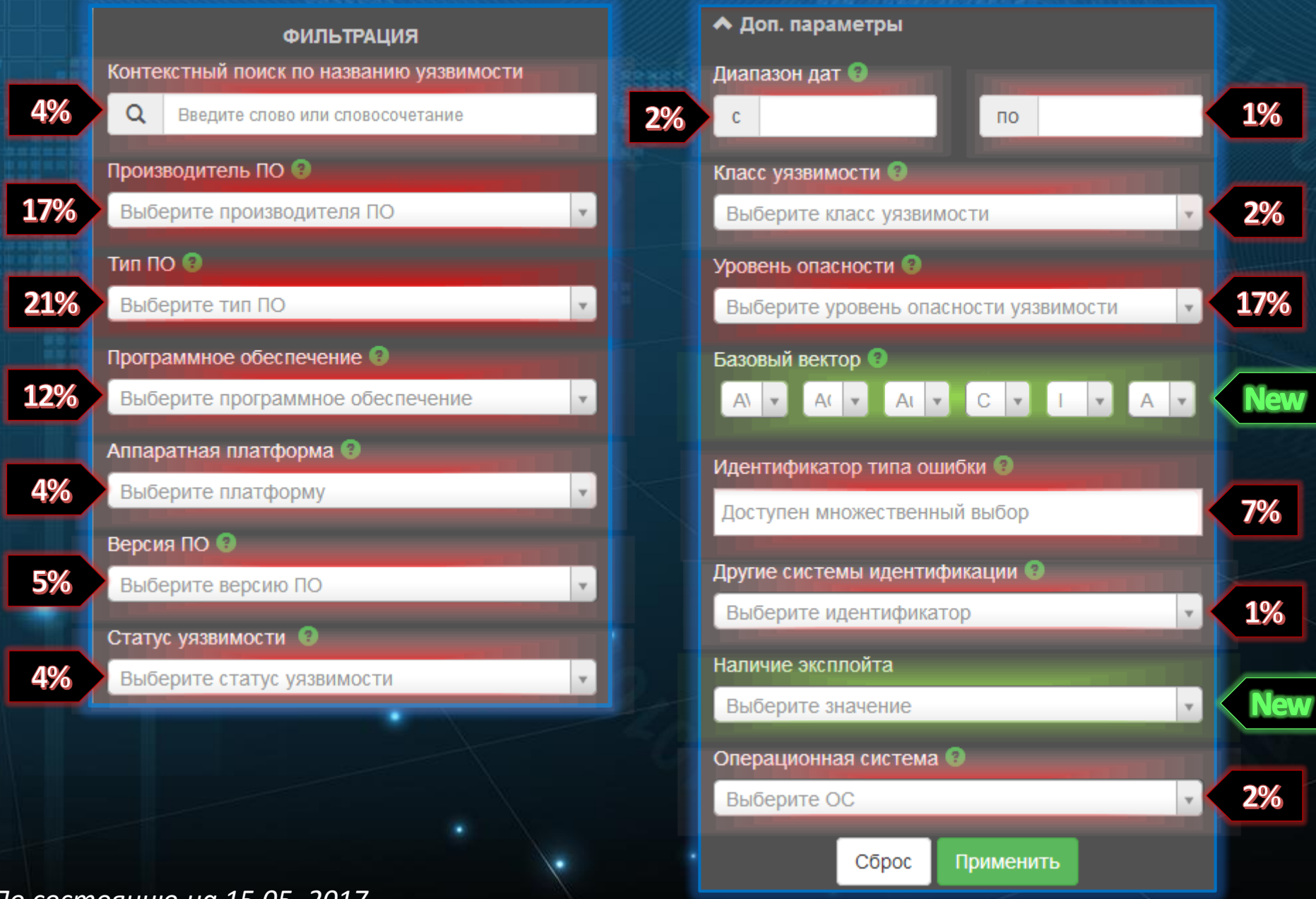
Предоставление сведений



Поиск сведений об уязвимостях



Статистика обращений к фильтрам

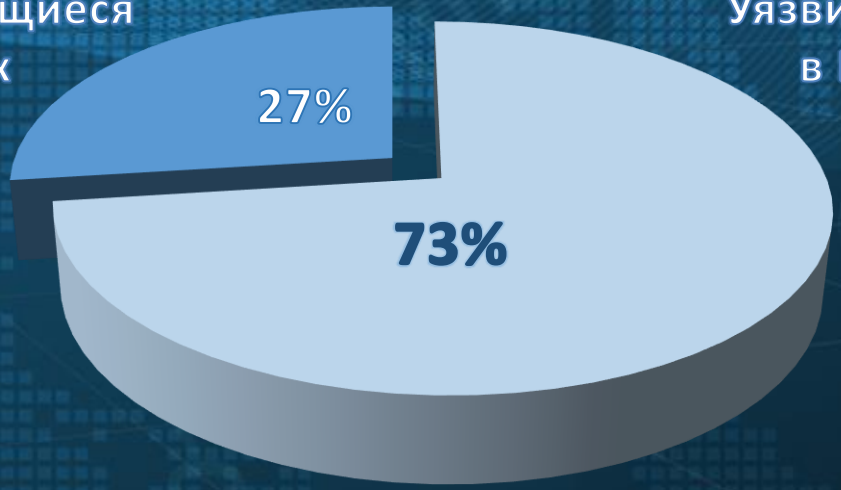


По состоянию на 15.05. 2017

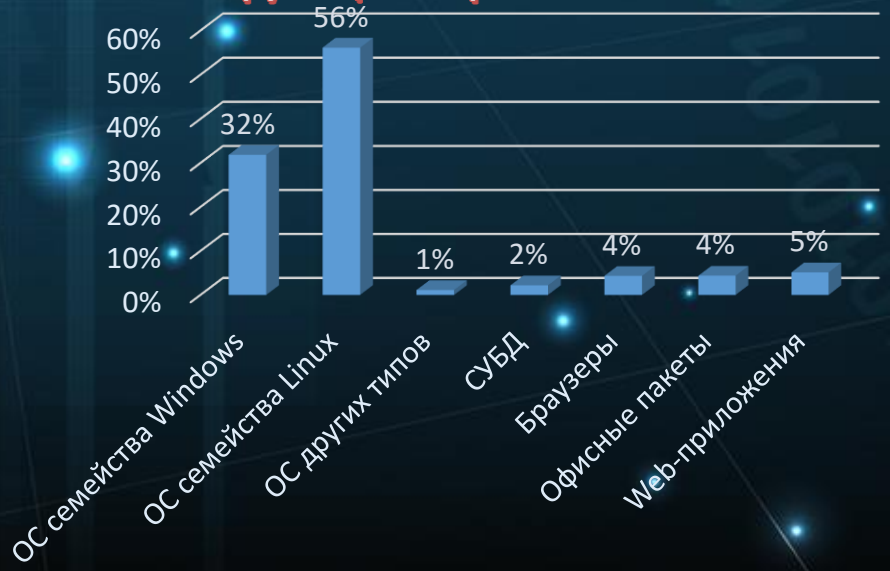
Статистика использования банка данных при сертификации ПО

Уязвимости, содержащиеся только в иностранных источниках

Уязвимости, вошедшие в БДУ ФСТЭК России

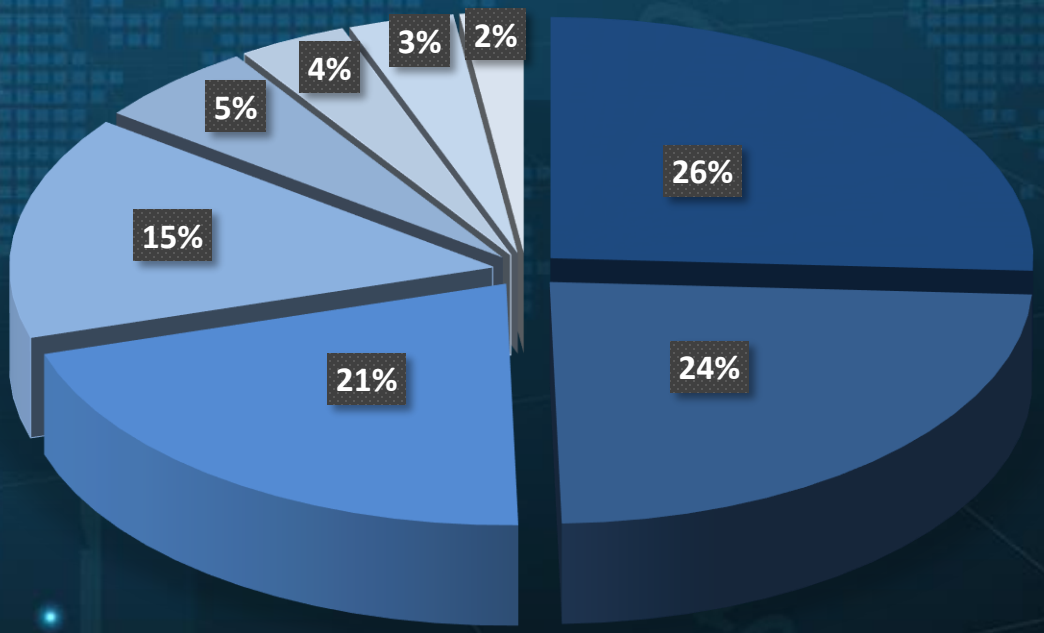


Доля уязвимостей ПО сред функционирования СЗИ



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

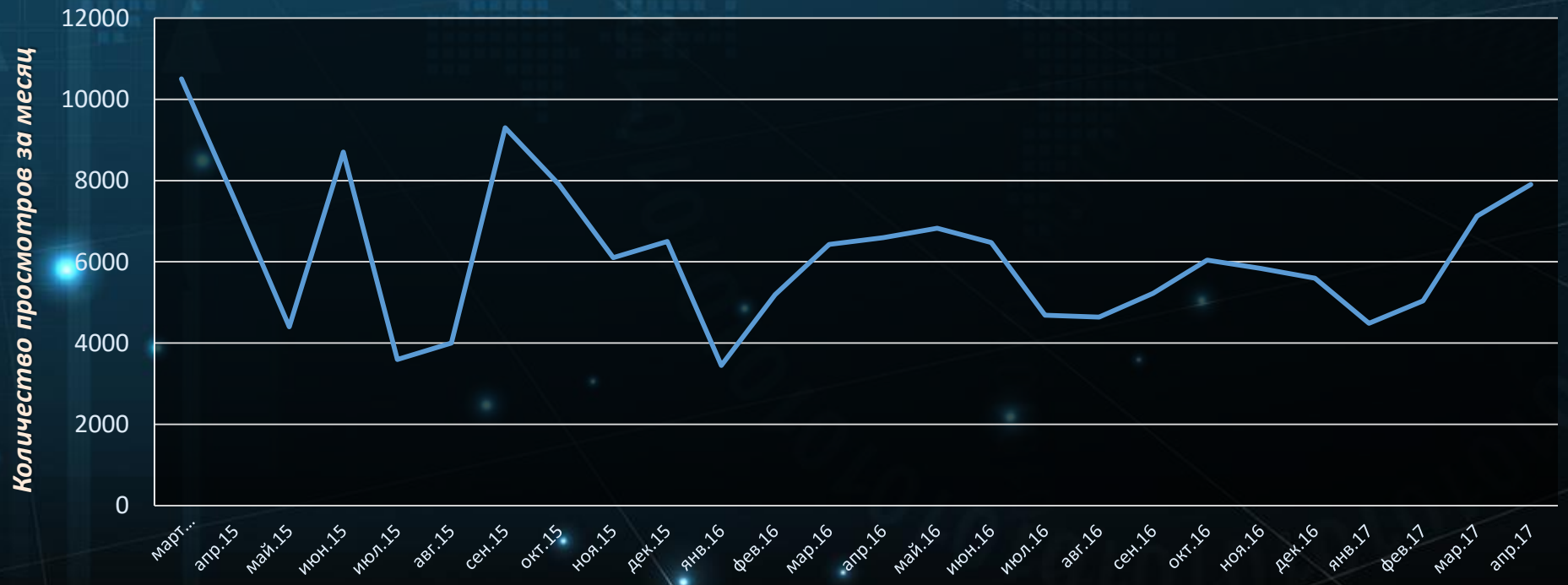
Популярные уязвимости в 2016 году

Статистика посещений БДУ ФСТЭК России

Просмотры страниц – 793 619

Суммарное количество визитов – 160 054

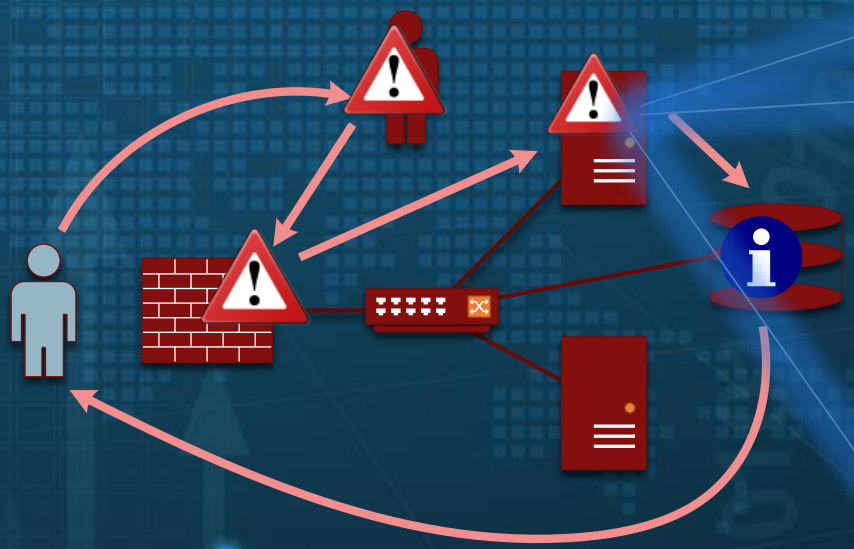
Уникальные посетители – 81 480

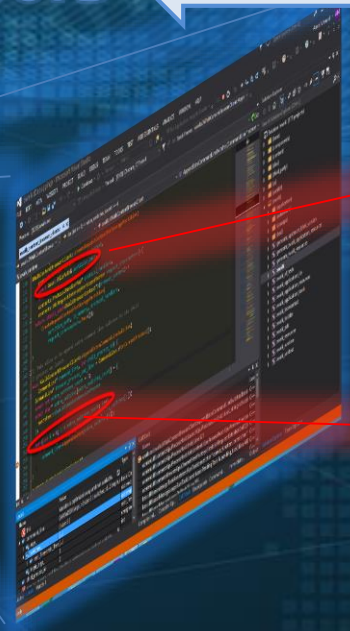


По состоянию на 15.05. 2017

База данных ошибок и ошибочных ситуаций

Угроза ← Уязвимость ← Недостаток (ошибка)





1+1=0

1<4-5

…

array[-1]=5

…

Международный опыт

CWE

CERT C C++ Java

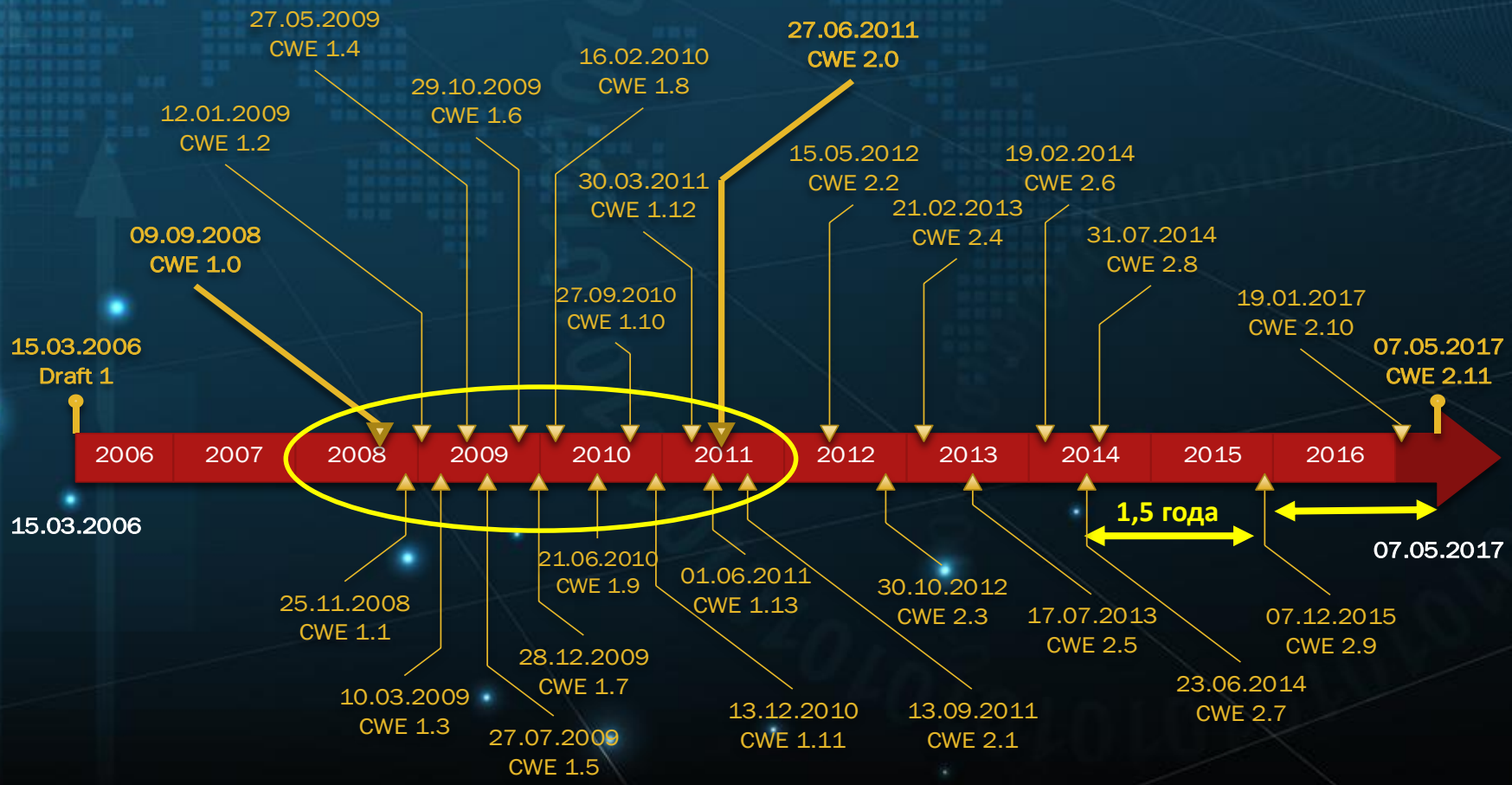
Стандарт CWE

Количество элементов: 1006 (17 устарели)

Крайняя версия: 2.11 (от 7.05.2017)

Участники разработки CWE
(более 50 организаций)

MITRE NIST WASC OWASP IBM Microsoft VERACODE



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:

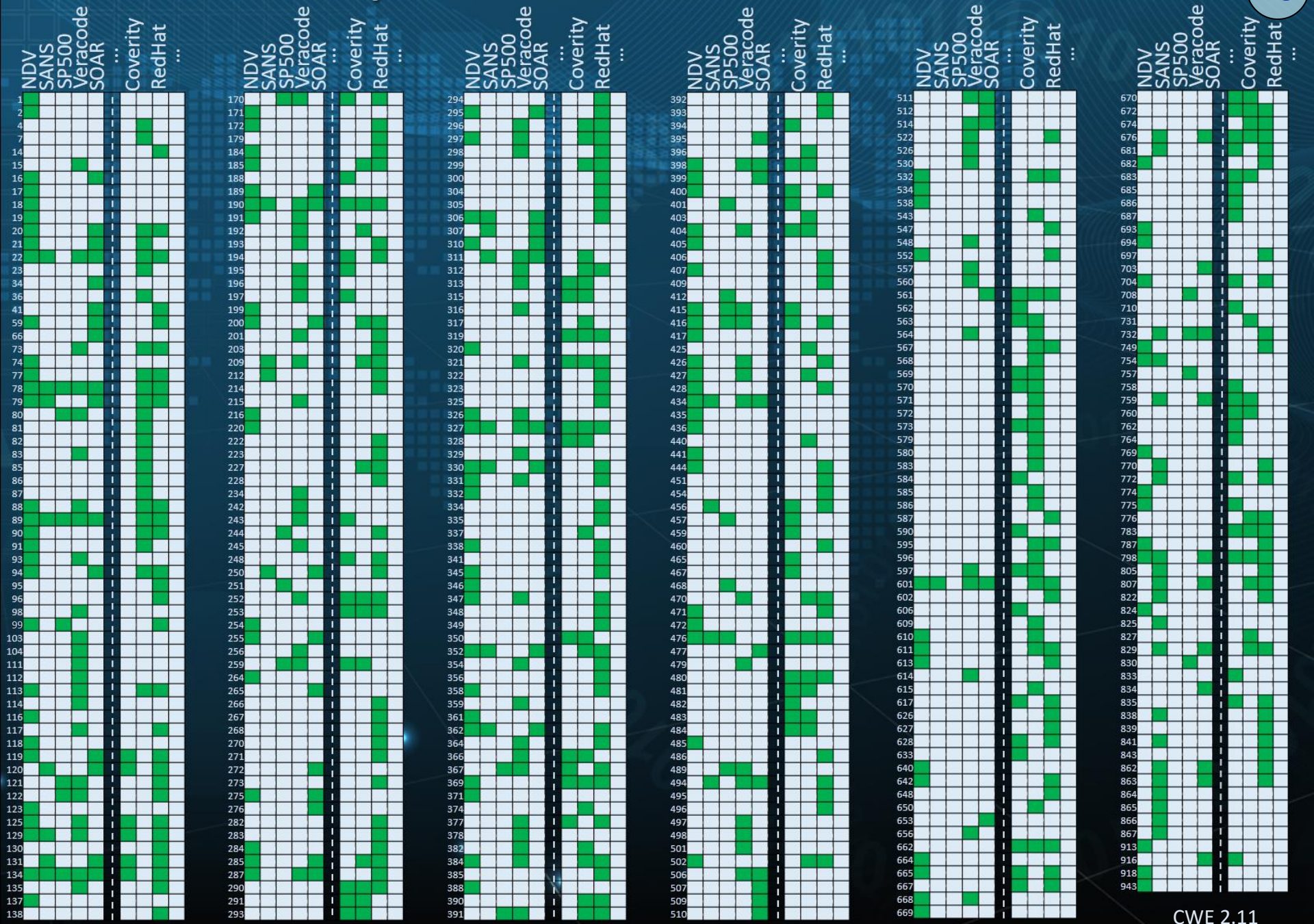
CWE-190 Целочисленное переполнение → **CWE-120** Переполнение буфера

Динамика наполнения стандарта CWE

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	…	…	…	…

Практика использования CWE



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»

- Класс 1
  - Ошибочная ситуация 1.1
  - Ошибочная ситуация 1.2
  - …
  - Ошибочная ситуация 1.n
- Класс 2
  - Ошибочная ситуация 2.1
  - Ошибочная ситуация 2.2
  - …
  - Ошибочная ситуация 2.p
- …
- Класс 1X
  - Ошибочная ситуация 1X.1
  - Ошибочная ситуация 1X.2
  - …
  - Ошибочная ситуация 1X.t

№ 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

C/C++ — Пример 1

C# — Пример 2

Java — Пример 3

PHP — Пример 4

SQL — Пример 5

другие — Примеры

№ 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

Классы «ошибок»

ID	Наименование класса «ошибок»
BDE:01	Переполнение буфера
BDE:02	Разыменование 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