

# Банк данных угроз безопасности информации: реалии и перспективы

Докладчик:  
начальник отдела  
ФАУ «ГНИИИ ПТЗИ ФСТЭК России»  
Владимир Минаков

# Вопросы доклада

1. Текущее состояние информационных ресурсов банка данных угроз безопасности информации
2. Банк данных угроз безопасности информации в сравнении с мировыми аналогами
3. Перспективы развития банка данных угроз безопасности информации

Текущее состояние  
информационных ресурсов банка  
данных угроз безопасности  
информации

# Годовой отчёт

4

Изменения с 10 марта 2015 по настоящее время

## Банк данных угроз безопасности информации



### Базы данных

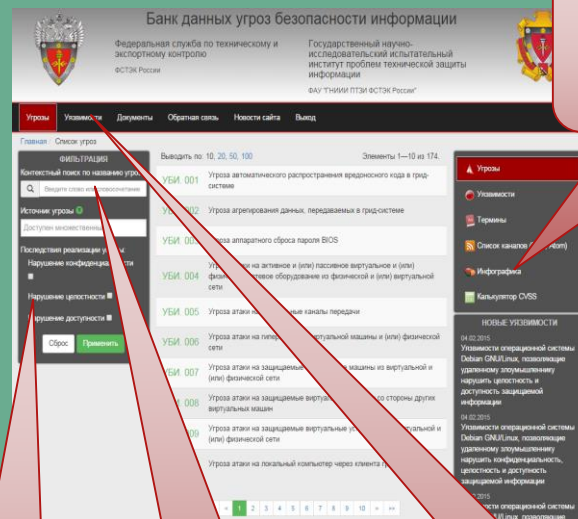
+20 угроз

База  
данных  
угроз

База  
данных  
уязвимостей

### Web-интерфейс

Изменена  
Инфографика



+2774  
уязвимости

термины и определения

Изменено  
1774  
уязвимости

Калькулятор CVSS

Документы

RSS/Atom

Еженедельные  
новостные  
сообщения

+2 фильтра

+контекстный  
поиск

+сортировка  
уязвимостей

# Банк данных в цифрах

5



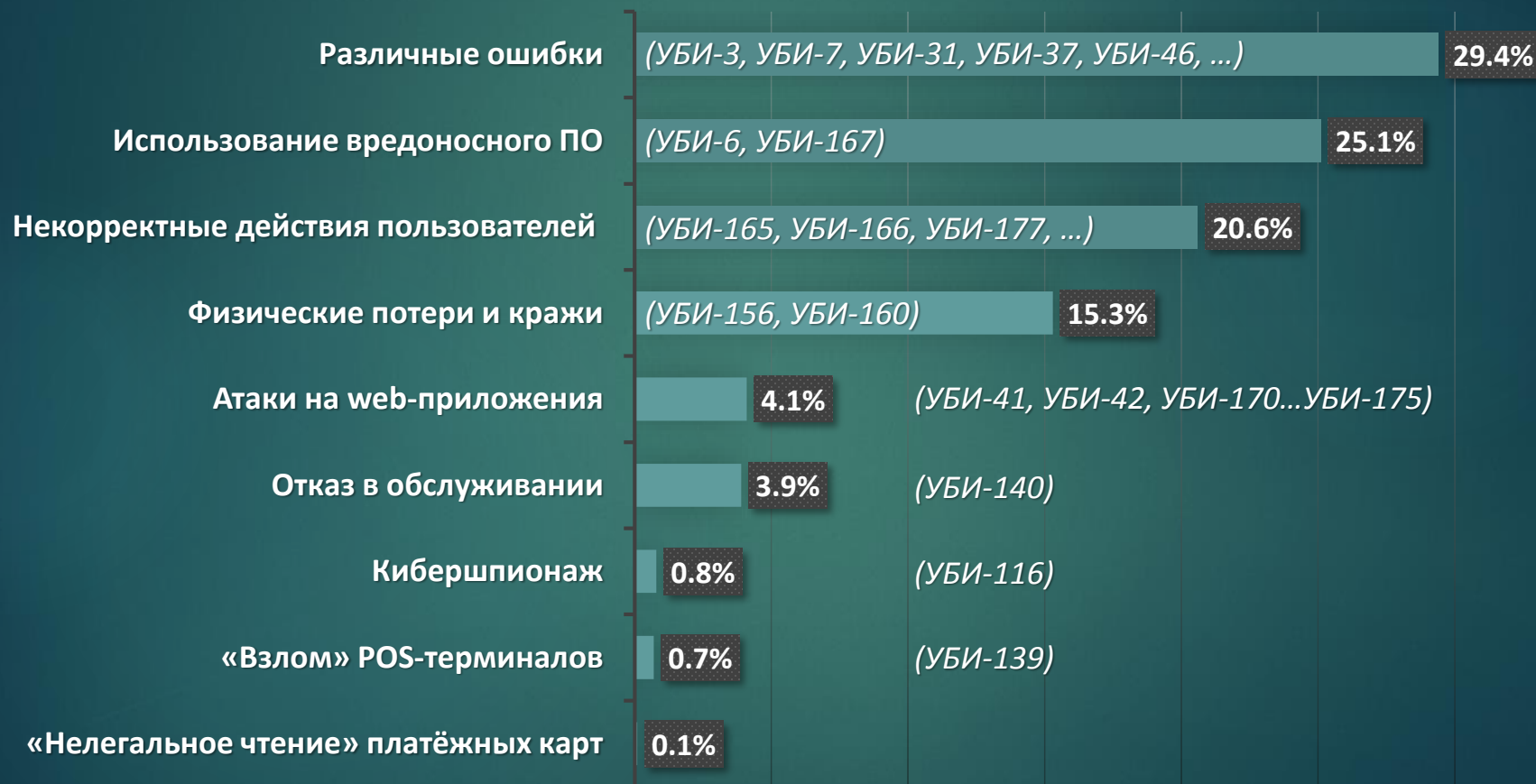
Данные актуальны по состоянию на 25.01.2016 г.

# Динамика угроз

6

## Распределение инцидентов по шаблонам атак

### Нарушение безопасности информации



# Динамика угроз



## Распределение инцидентов по шаблонам атак

**Нарушение только конфиденциальности информации**



# Динамика угроз



## Распределение инцидентов по шаблонам атак и нарушителям

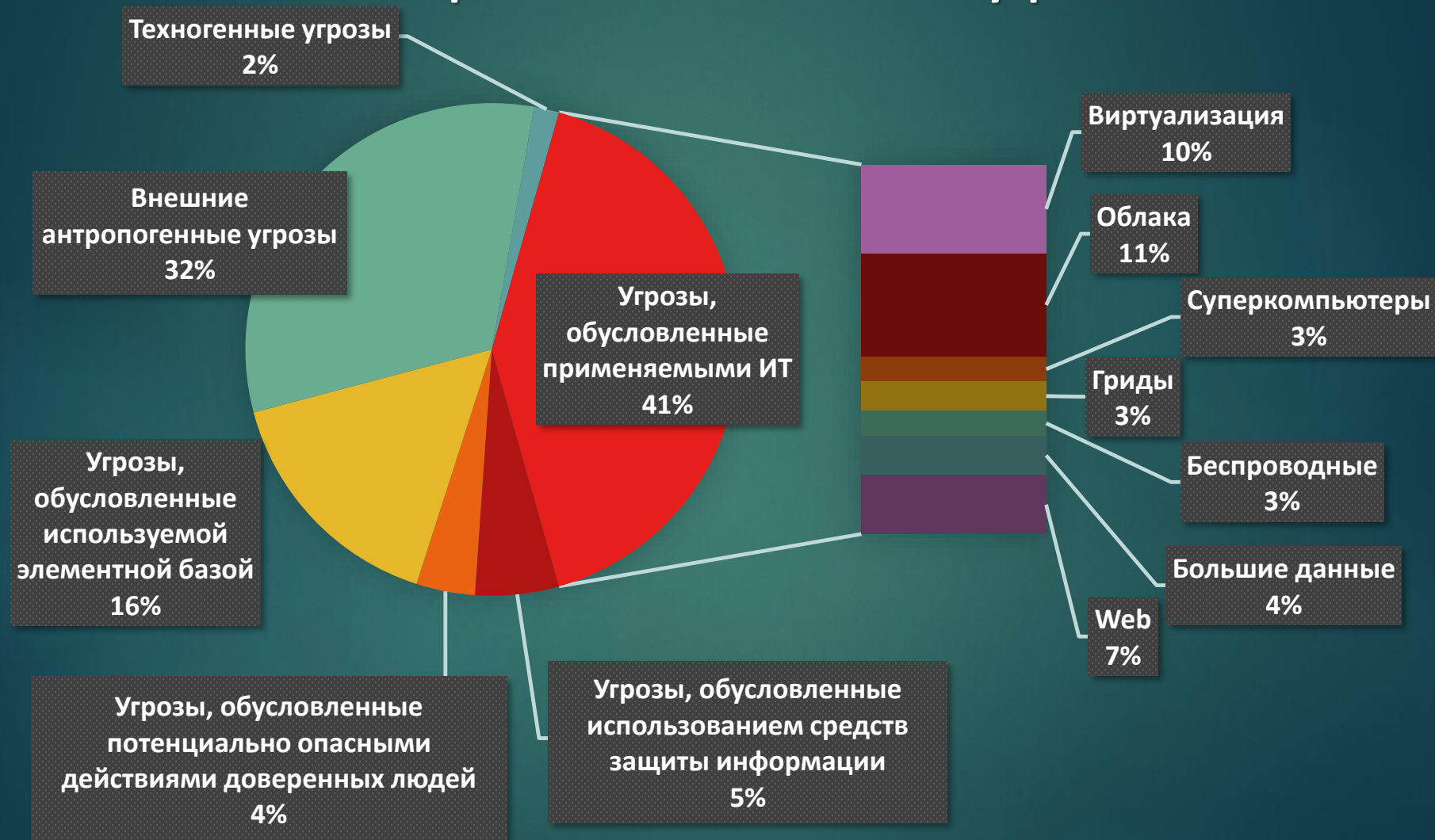
	Использование вредоносного ПО	Кибершпионаж	Отказ в обслуживании	Физические потери и кражи	Различные ошибки	«Незаконное чтение» платёжных карт	«Взлом» POS-терминалов	Некорректные действия пользователей	Атаки на web-приложения
Активисты	3%	5%	31%						61%
Организации	73%						6%		20%
Государства		97%							3%
Нет данных	41%	3%	5%	18%	2%	6%	1%	3%	22%



# Угрозы в цифрах

9

## Причины возникновения угроз



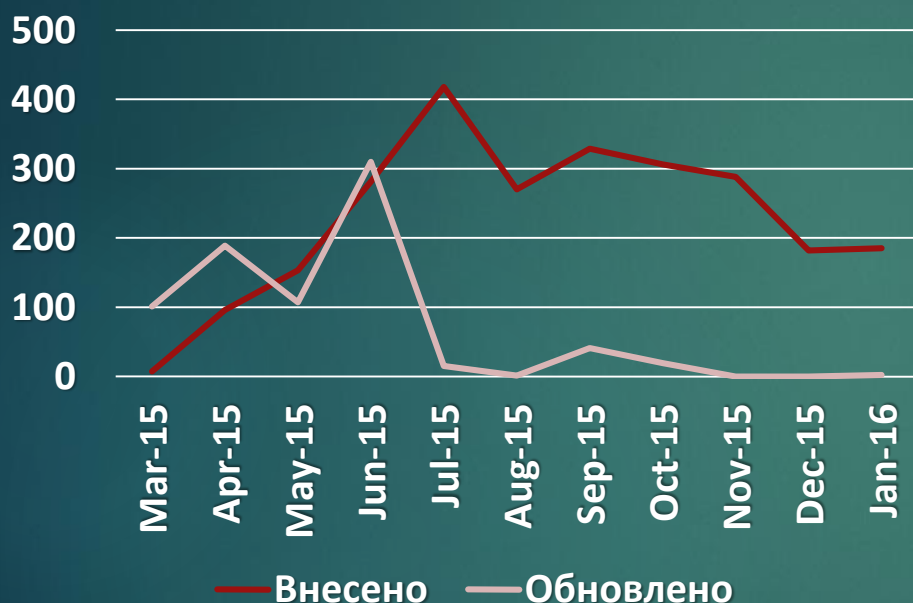
Статистические данные актуальны по состоянию на 25.01.2016 г.

# Динамика уязвимостей

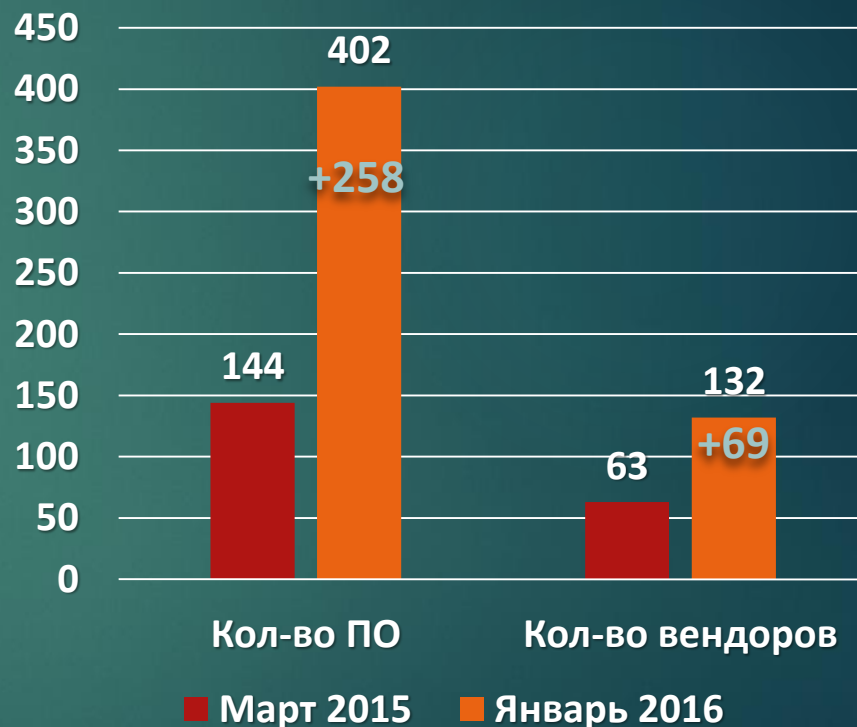
10

Изменения с 10 марта 2015 по настоящее время

Кол-во уязвимостей



Наполнение базы уязвимостей

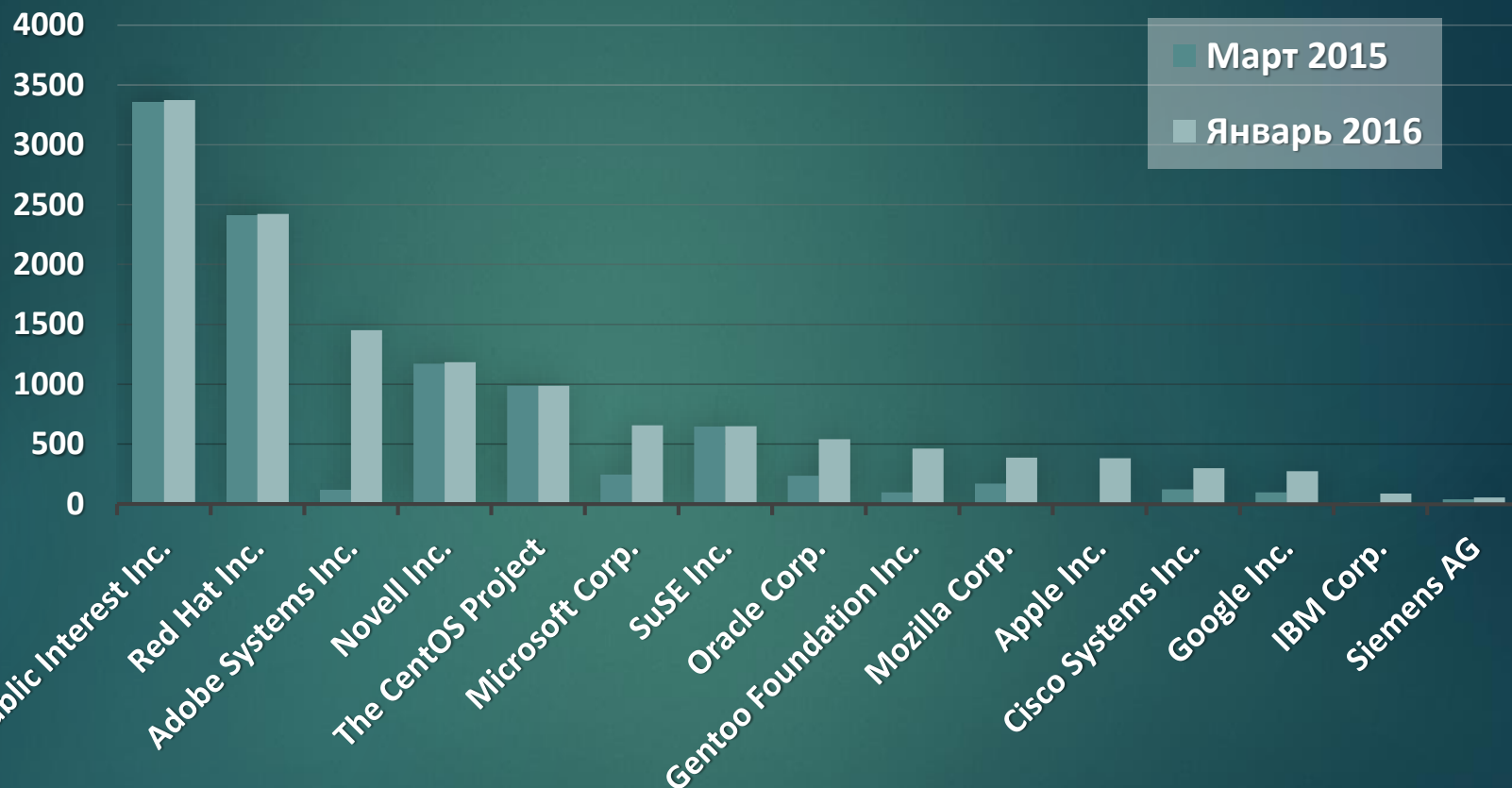


Статистические данные актуальны по состоянию на 25.01.2016 г.

# Динамика уязвимостей

11

## TOP-15 вендоров\*



\*По данным аналитиков [bdu.fstec.ru](http://bdu.fstec.ru) (январь 2016 г.)

# Динамика уязвимостей

12

## Распределение по уровню опасности



Статистические данные актуальны по состоянию на 25.01.2016 г.

## Распределение по типу программного обеспечения



Статистические данные актуальны по состоянию на 25.01.2016 г.

# Потребители информации

14

Изменения с 10 марта 2015 по настоящее время

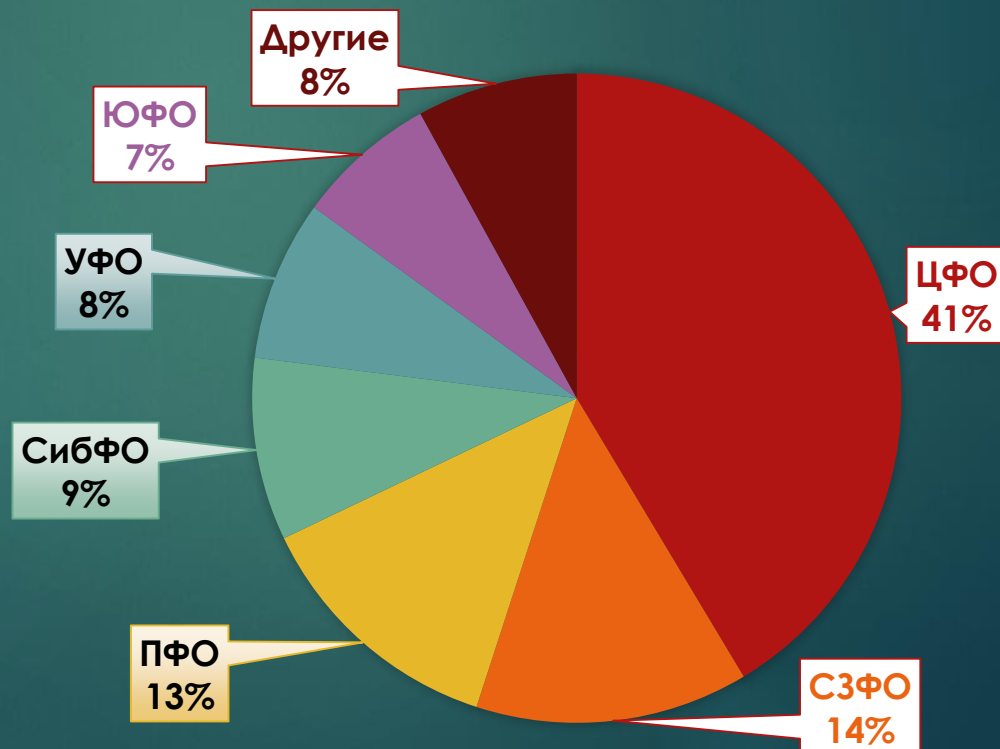


Банк данных угроз  
безопасности  
информации

- 56008 посещений
- 26430 уникальных пользователей
- 295460 страниц просмотрено

Потребители  
банка данных угроз

## ПО ФЕДЕРАЛЬНЫМ ОКРУГАМ



Банк данных  
угроз безопасности информации  
в сравнении с мировыми  
аналогами

# Сравнение баз данных угроз

16

База данных	Возраст (лет)	Кол-во описаний угроз	Кол-во страниц	Наличие описания действий по нейтрализации угрозы	Последнее обновление
BSI IT-Grundschutz-Kataloge	12	682	4883	да	Ноябрь 2014
bdu.fstec.ru	1	182	182	нет	Август 2015



# Сравнение баз данных уязвимостей

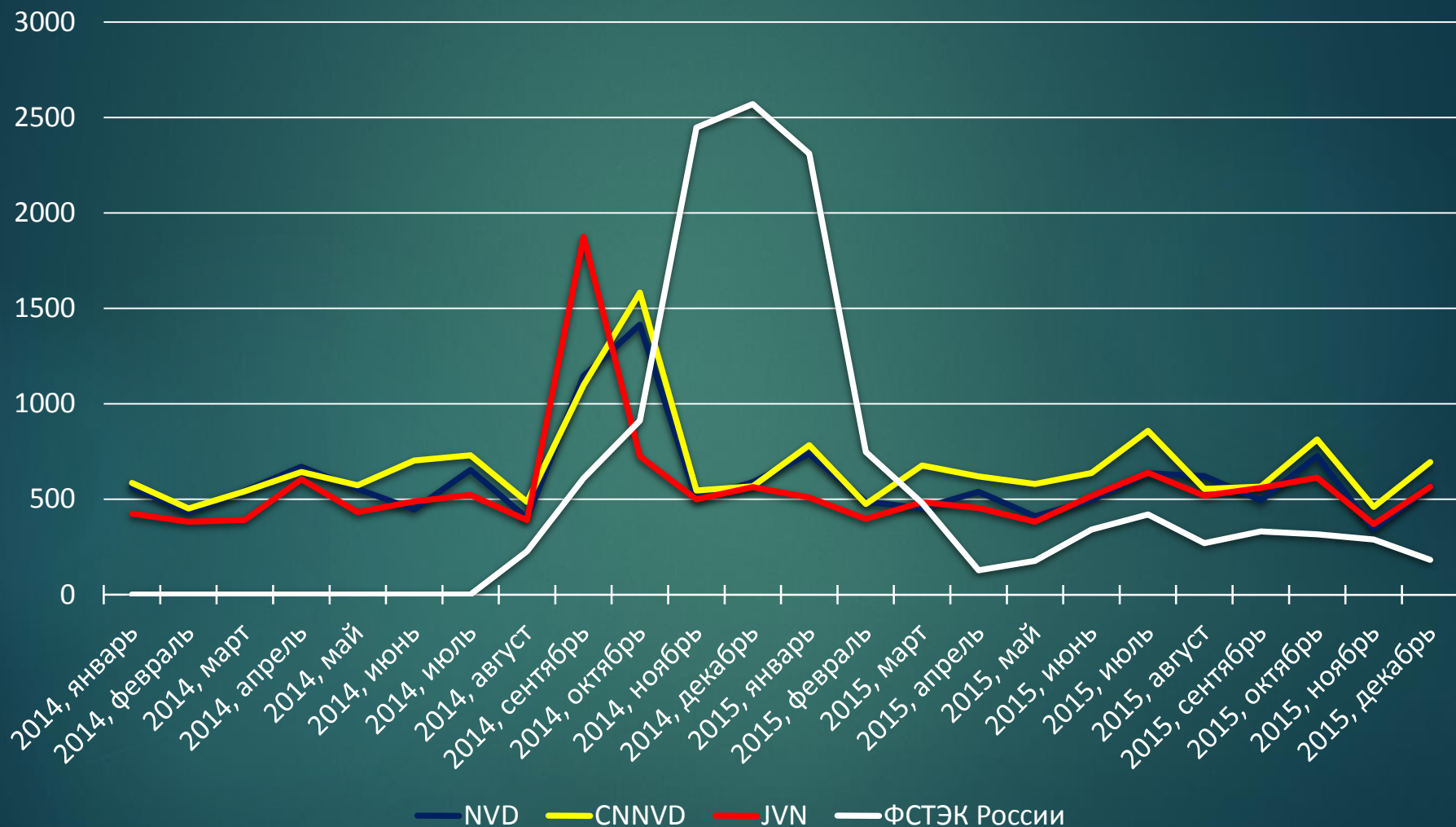
17

База данных	Возраст (лет)	Кол-во описаний	Кол-во полей	Кол-во программ	Кол-во вендоров	Примечание
OSVDB	14	>120000	16	-	>13000	«Открытая» БД
X-Force	19	>110000	12	-	-	БД IBM
CNNVD	17	>80000	9	>18000	>11000	БД Китая
SecurityFocus	17	>80000	11	-	>15000	БД Symantec
<b>CVE/NVD</b>	<b>17</b>	<b>&gt;75000</b>	<b>16</b>	<b>&gt;29000</b>	<b>&gt;15000</b>	<b>БД США</b>
JVN iPedia	14	>58000	14	-	>11000	БД Японии
ExploitDB	13	>35000*	7	-	-	БД эксплойтов
SecurityLab.ru	16	>34000	19	-	-	БД Positive Tech.
SecurityTracker	15	>22000	16	>6500	>3900	БД SecurityGlobal
CiscoSecurity	15	>19000	25	-	-	БД Cisco
bdu.fstec.ru	1	>13000	21	402	138	БД России
OVAL	14	>12000	9	-	-	БД OVAL-описаний
АЛТЭК-СОФТ	8	-	11	-	-	БД OVAL-описаний
...	Известно <b>более 60</b> баз данных уязвимостей					

# Уязвимости в цифрах

18

Наполняемость баз данных уязвимостей

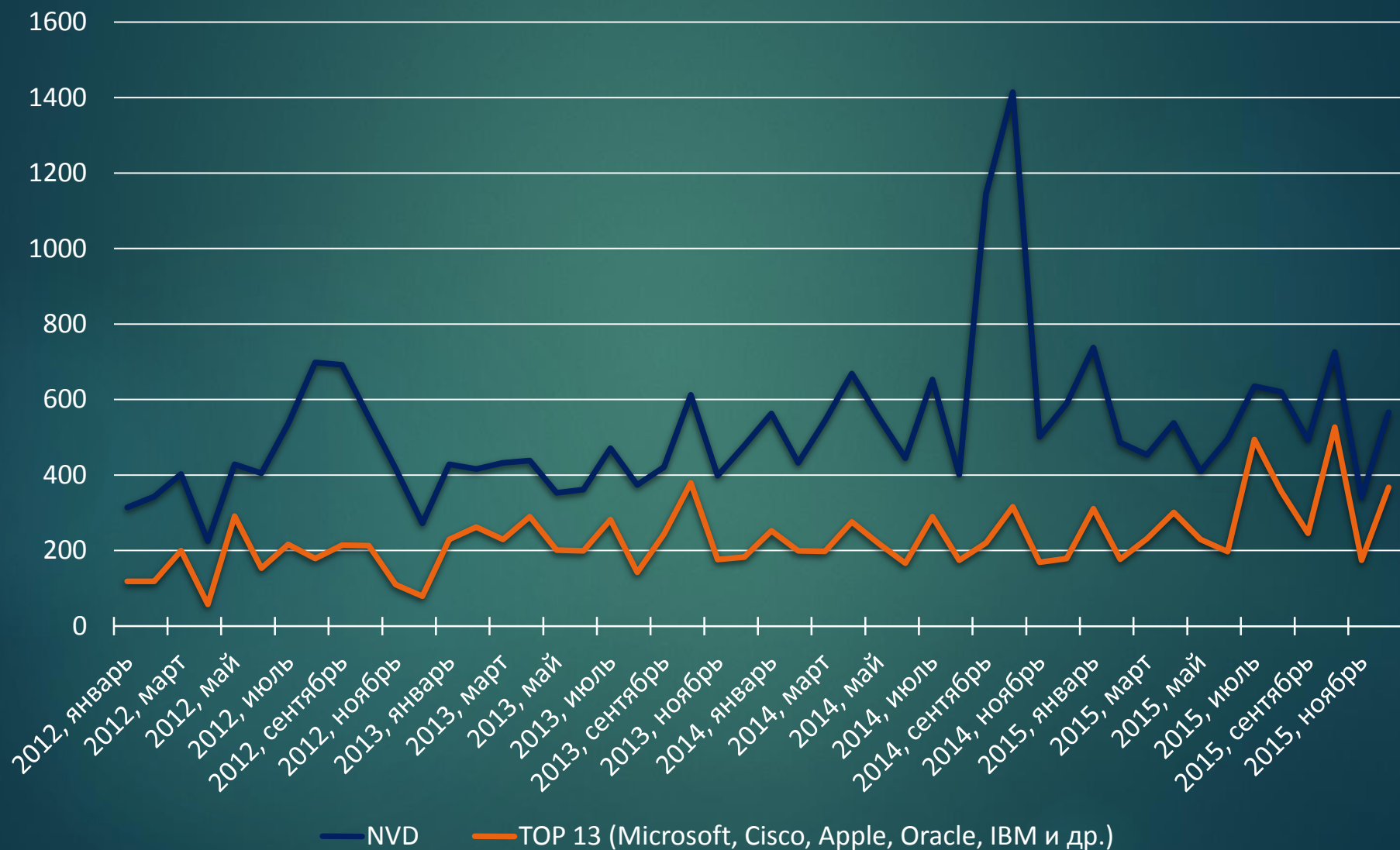


Статистические данные актуальны по состоянию на 25.01.2016 г.

# Уязвимости в цифрах

19

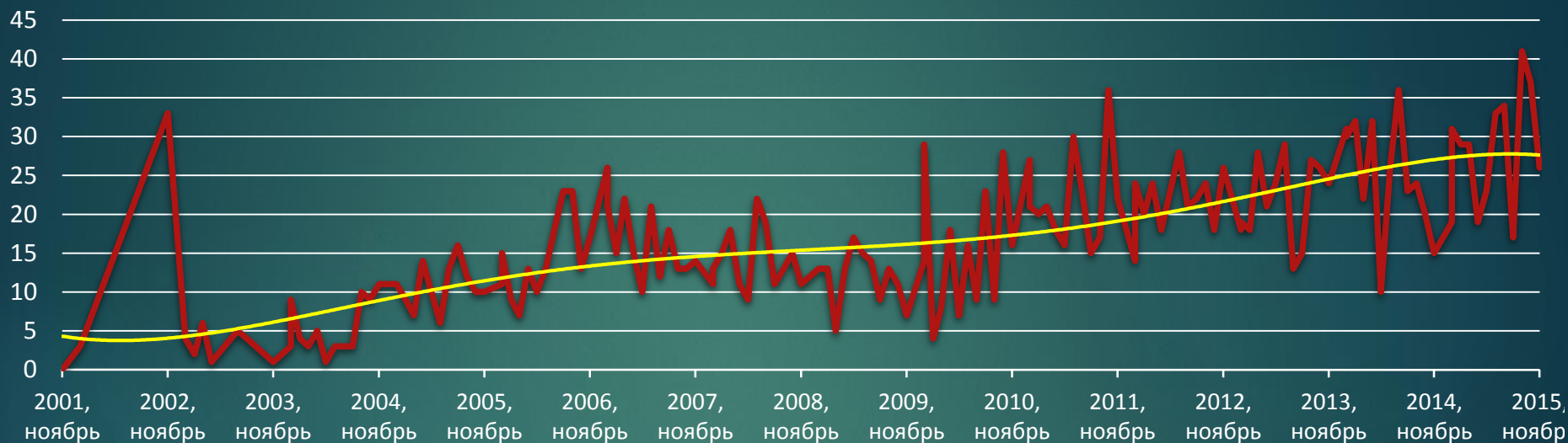
Использование сведений основных вендоров в базе данных NVD



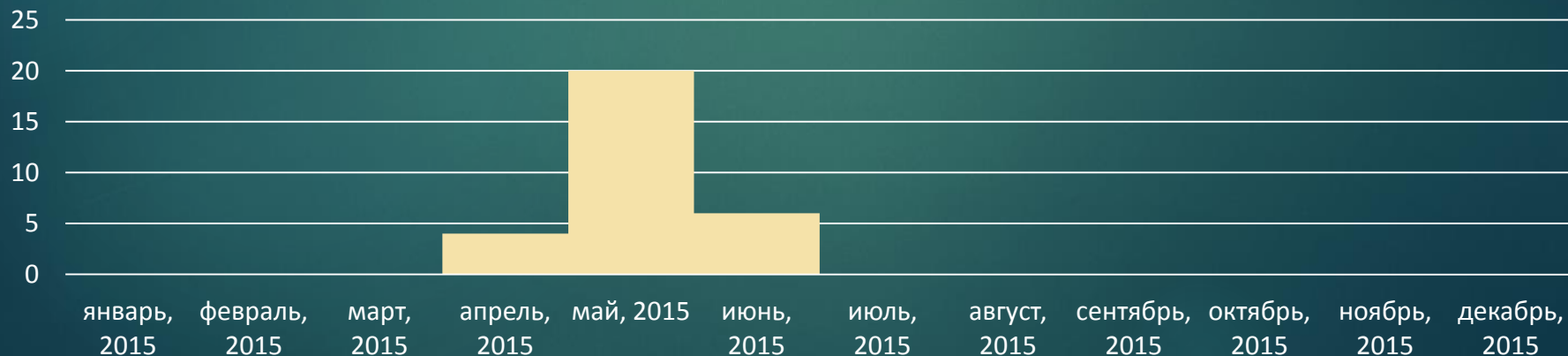
# Уязвимости в цифрах

20

Динамика публикации сведений об уязвимостях, появившихся впервые в базе данных JVN iPedia



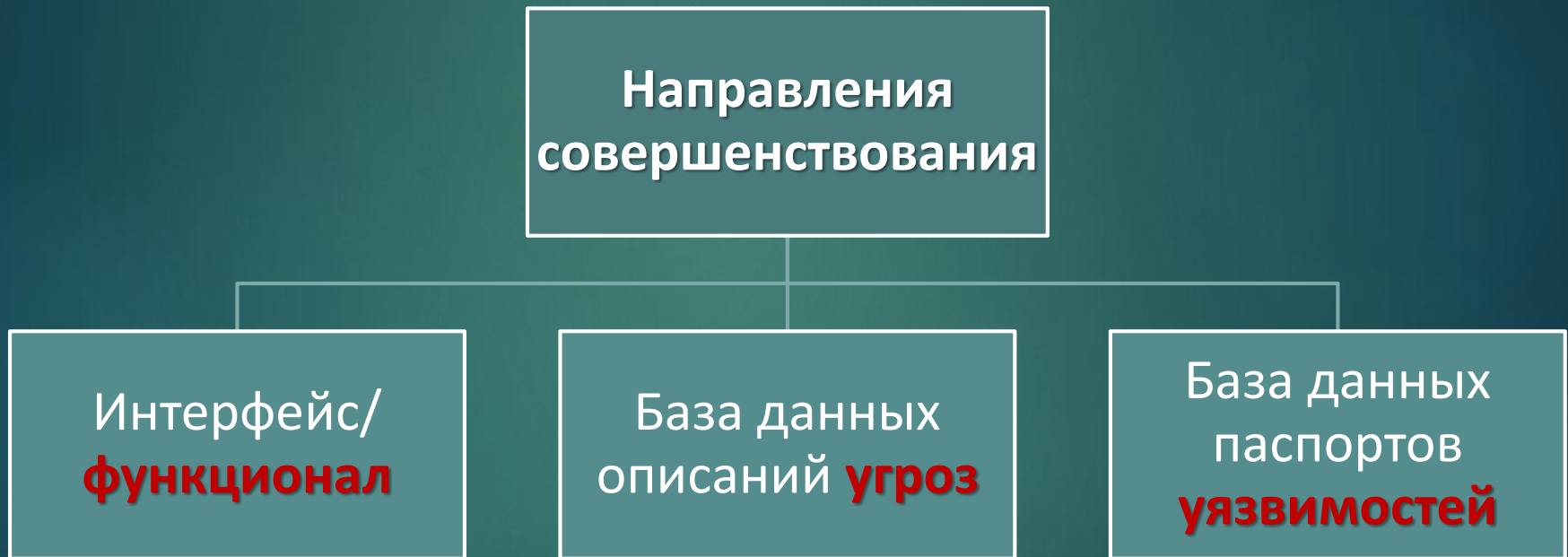
Динамика публикации сведений об уязвимостях, появившихся впервые в базе данных ФСТЭК России



# Перспективы развития банка данных угроз безопасности информации

# В перспективе: банк данных

Перспективы развития и совершенствования банка данных



# В перспективе: функционал

23

Перспективы **совершенствования** функционала/интерфейса сайта

**Совершенствование системы фильтров уязвимостей**

**Совершенствование модуля «Инфографика»**

- Реализация новой диаграммы «Критические уязвимости программного обеспечения различных вендоров»;
- Реализация новой диаграммы «Время, затраченное вендорами на устранение выявленных уязвимостей»

**Добавление новых полей в описания уязвимостей и угроз**

**Модернизация элементов пользовательского интерфейса**

# В перспективе: функционал

24

Перспективы **разработки** функционала/интерфейса сайта

Реализация функционала выгрузки записей об уязвимостях и угрозах в соответствии с пользовательской выборкой

Реализация функционала подписки на обновления Банка данных

- Реализация подписки на обновления Банка данных;
- Реализация личного кабинета для выбора критериев подписки (пользовательские шаблоны подписки)

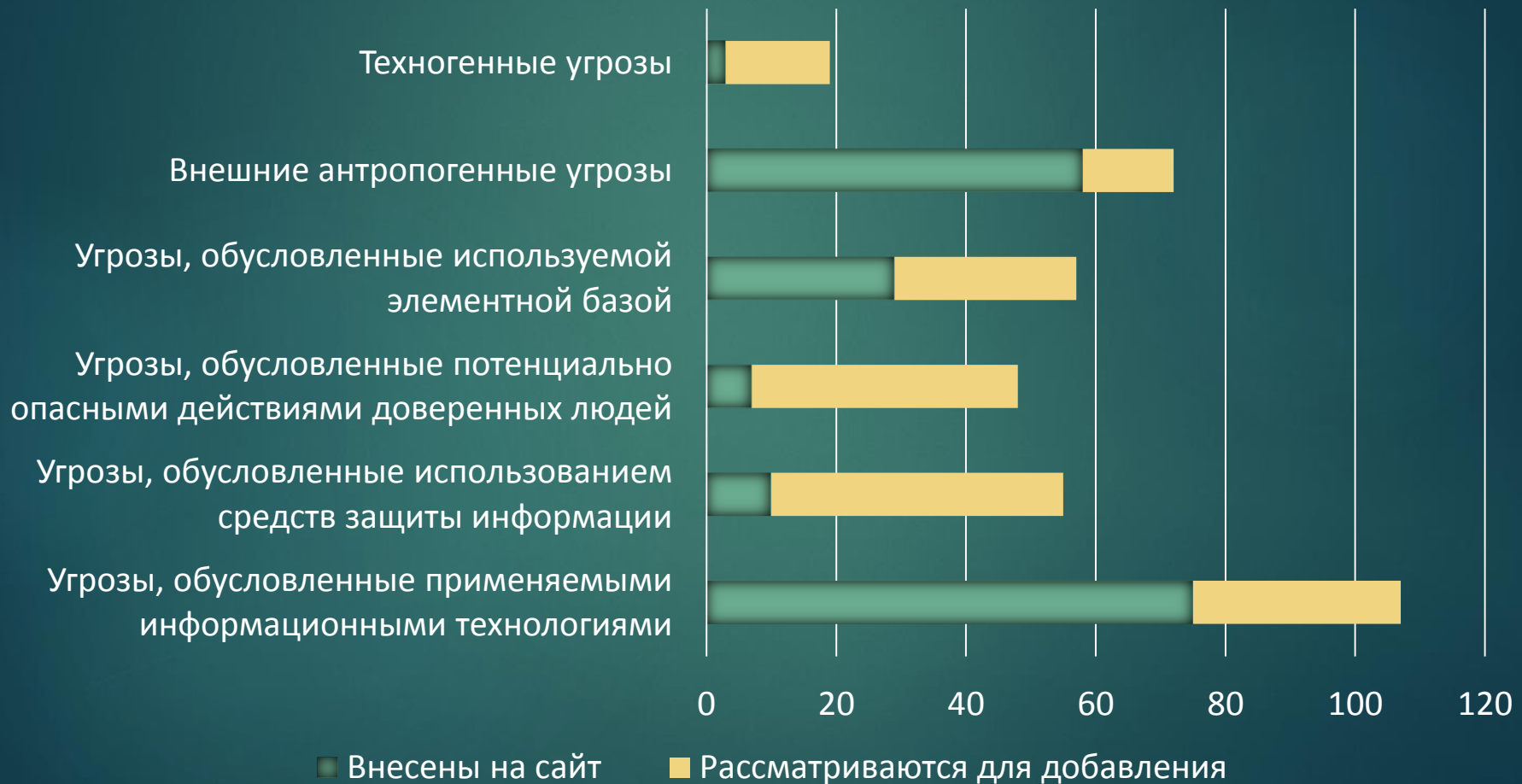
Реализация статистического модуля для сбора информации об обращениях к ресурсам сайта

Реализация нового раздела, включающего небезопасные конструкции кода



# В перспективе: угрозы

## Перспективы пополнения перечня угроз



# В перспективе: угрозы

26

Разработка различных классификаций

Классификация  
«по результату (по инцидентам)»

Классификационный  
признак

Категория инцидента

Угрозы

Различные ошибки

Физические потери и кражи

Использование  
вредоносного ПО

Атаки на web-приложения

Отказ в обслуживании

Некорректные действия пользователей

«Взлом» POS-терминалов

«Нелегальное чтение» платёжных карт

Кибершпионаж

Иные угрозы

# В перспективе: угрозы

27

Разработка различных классификаций

Классификация  
«по источнику»

Классификационный  
признак

Расположение  
источника

Природа источника

Угрозы

Внутренние

Внешние

Обусловленные  
наличием в ИС...

...информационных  
технологий

...средств ЗИ

...доверенных людей

...элементной базы

Антропогенные

Техногенные

# В перспективе: угрозы

28

## Разработка различных классификаций

### Классификация «по результату»

Классификационный  
признак

Последствие  
реализации

Результат реализации

Приводящие к...

...нарушению  
конфиденциальности

...нарушению  
целостности

...нарушению  
доступности

Копирование  
защищаемых данных

Ознакомление со  
служебной информацией

Выход из строя

Неверные сведения

Отключение части  
функций безопасности

Ошибки в работе системы

Прерывание сеанса связи

Отказ в доступе

Отказ чтения

Потеря привилегий на  
доступ

Ознакомление с  
защищаемыми данными

Получение учётных  
данных нарушителем

Отказ в доступе

Ошибки в документации

Добавление вредоносных  
функций

Повреждение данных

Удаление данных

Отказ записи

Потеря документации

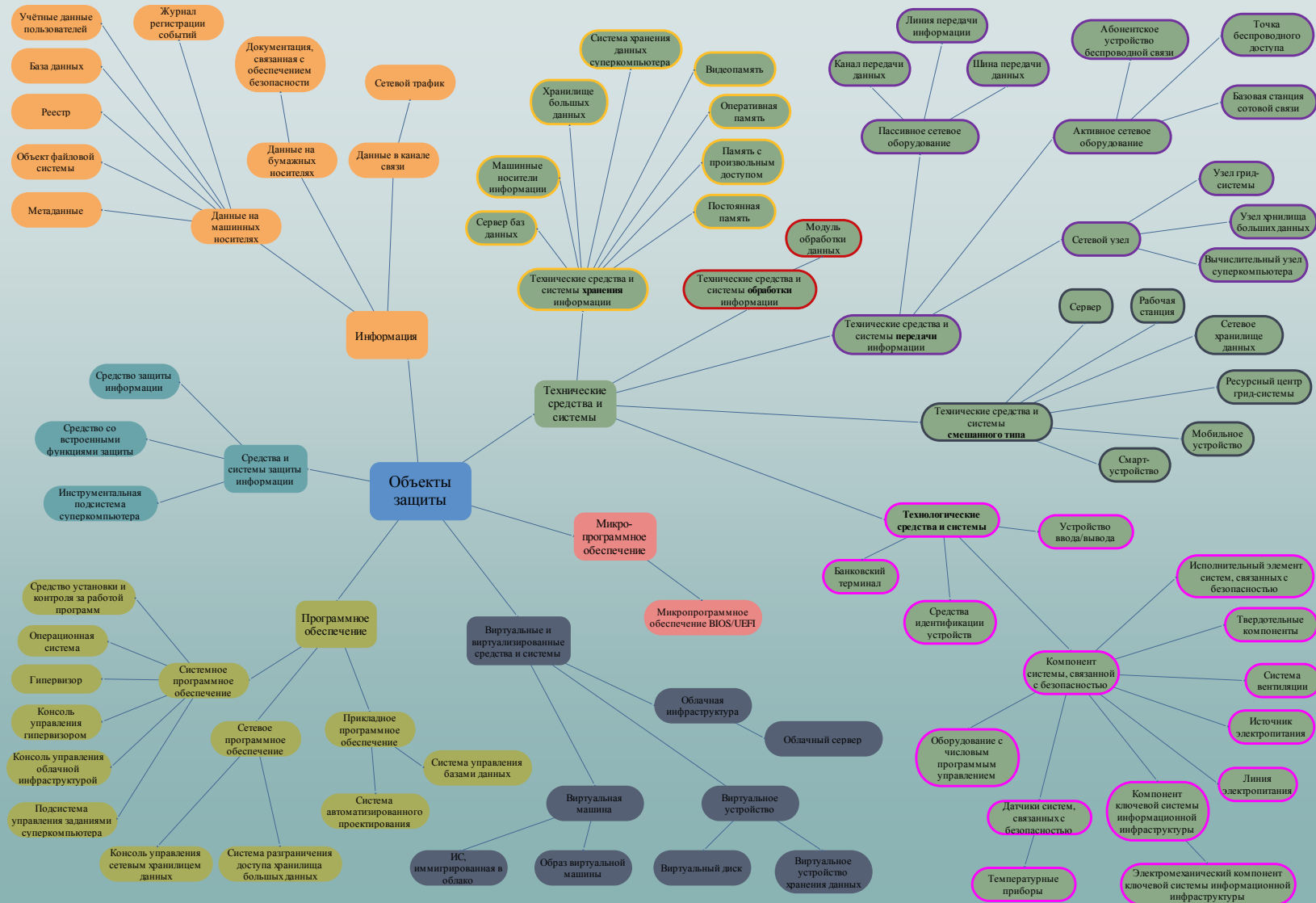
Потеря части  
функционала системы

Угрозы

# В перспективе: угрозы

29

## Классификация «по объекту»



# В перспективе: уязвимости

30

Перспективы пополнения базы данных уязвимостей в 2016 году

## Добавление полей в паспорт уязвимости

- «Дата устранения уязвимости»
- CVSS 3.0
- описание на языке OVAL
- «Способ нейтрализации уязвимости»

## Основное направление дальнейших исследований

- Отечественное ПО

Спасибо за внимание