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

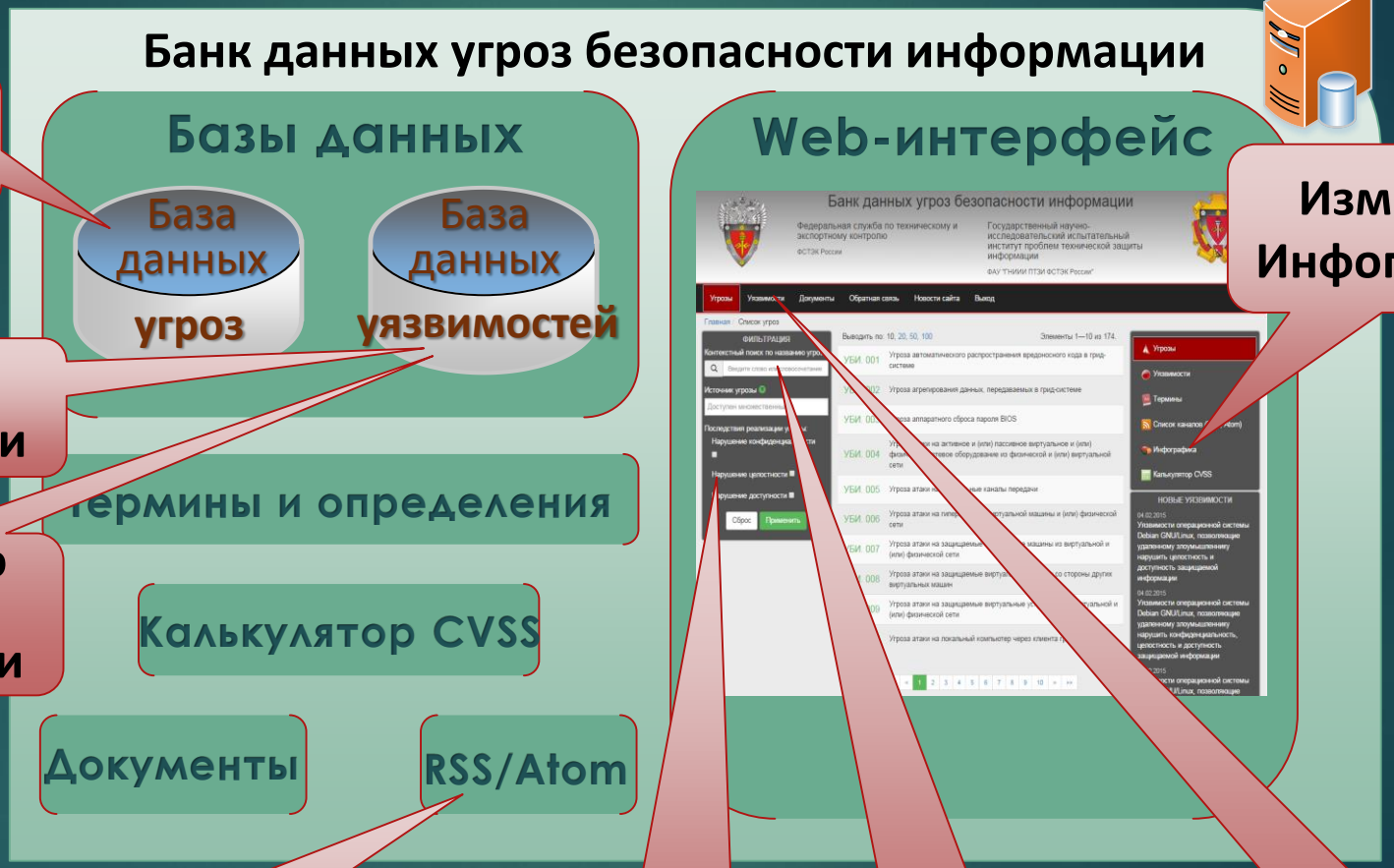
2. Банк данных угроз безопасности информации в сравнении с мировыми аналогами

3. Перспективы развития банка данных угроз безопасности информации

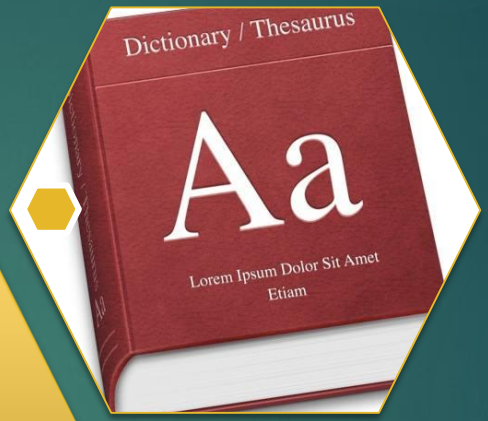
Текущее состояние информационных ресурсов банка данных угроз безопасности информации

Годовой отчёт

Изменения с 10 марта 2015 по настоящее время



Банк данных в цифрах



64 термина

182 описания угроз

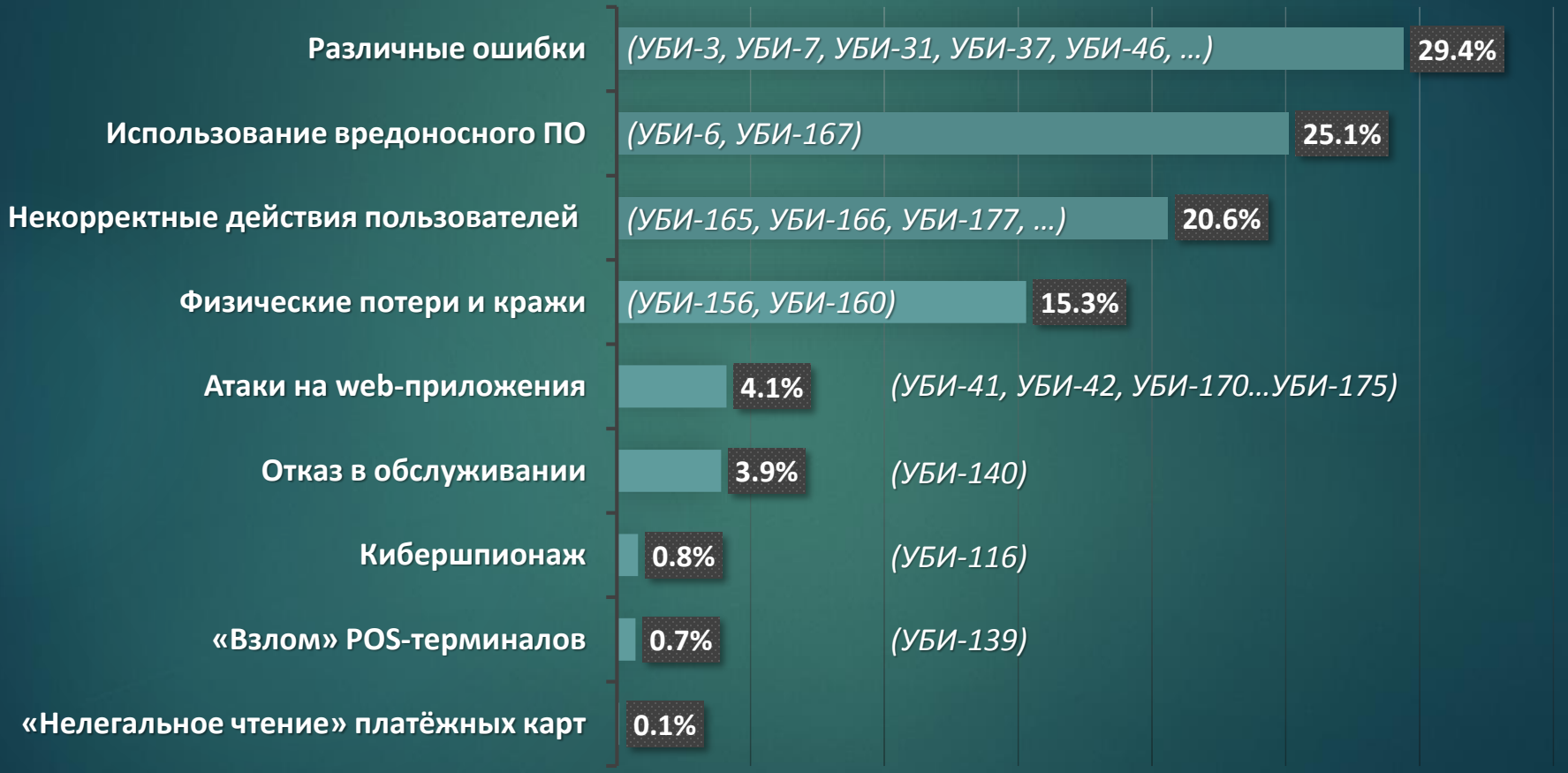
13052 паспорта уязвимостей

Данные актуальны по состоянию на 25.01.2016 г.

Динамика угроз

Распределение инцидентов по шаблонам атак

Нарушение безопасности информации



По данным «2015 Data Breach Investigations Report» © 2015 Verizon

Динамика угроз

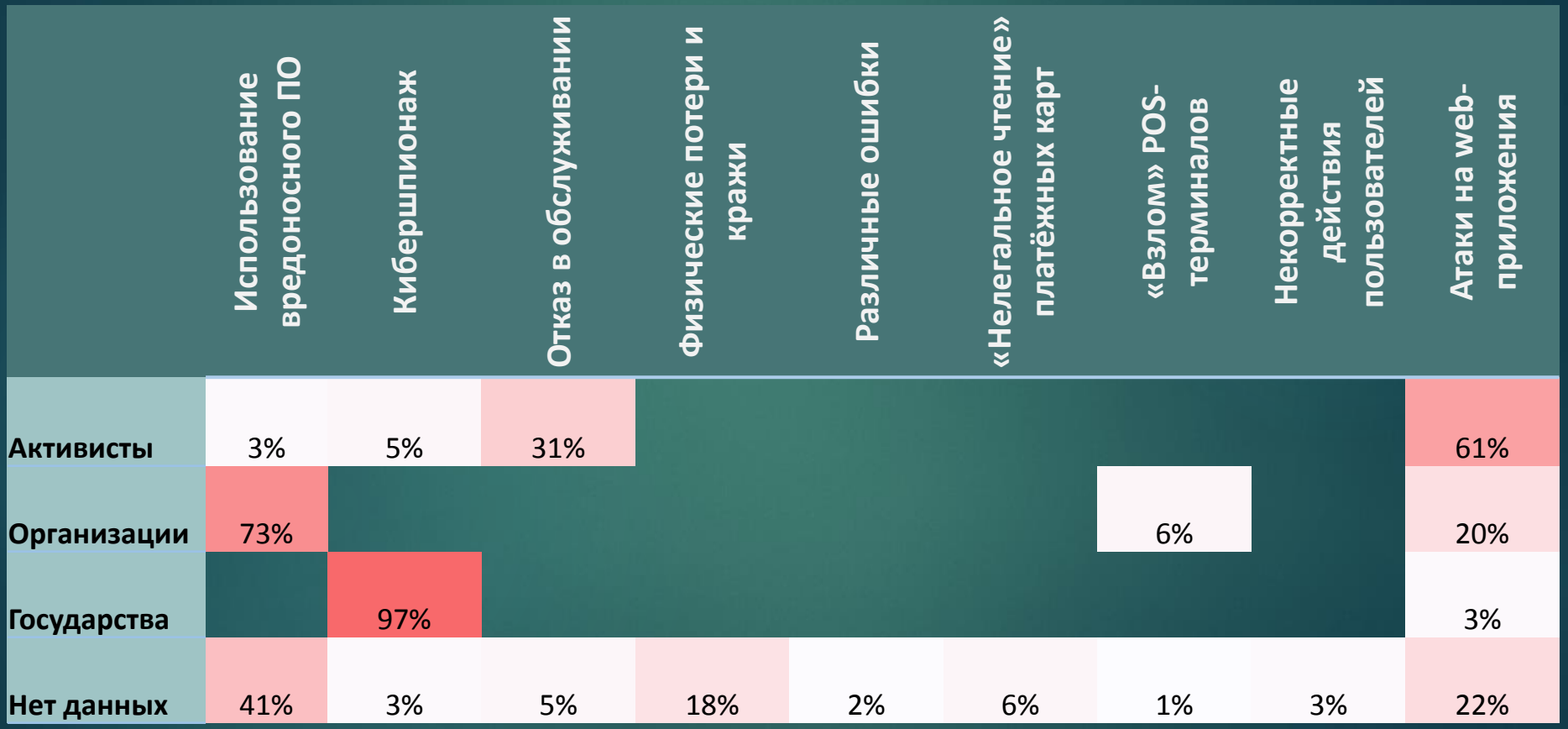
Распределение инцидентов по шаблонам атак

Нарушение только конфиденциальности информации

По данным «2015 Data Breach Investigations Report» © 2015 Verizon

Динамика угроз

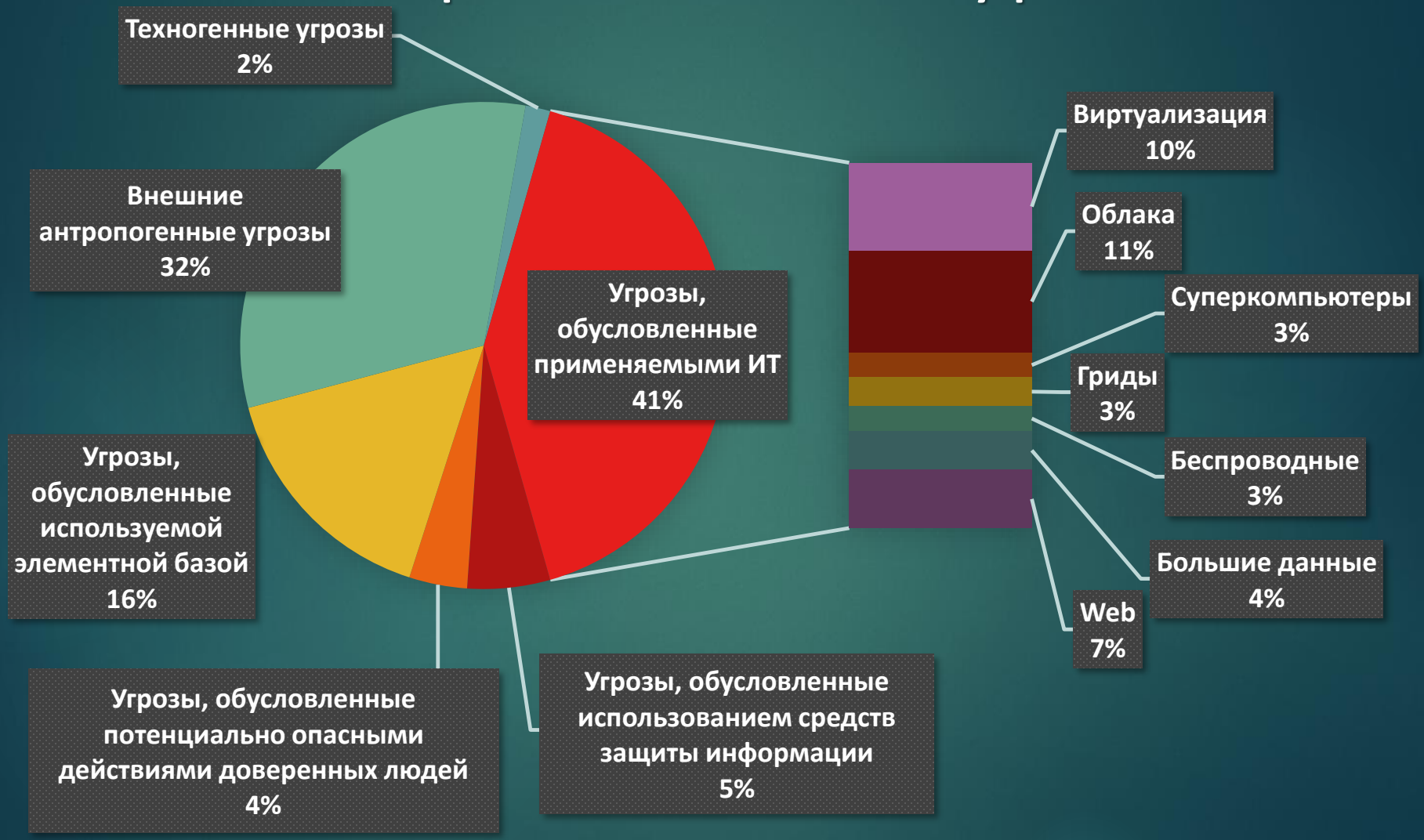
Распределение инцидентов по шаблонам атак и нарушителям



По данным «2015 Data Breach Investigations Report» © 2015 Verizon

Угрозы в цифрах

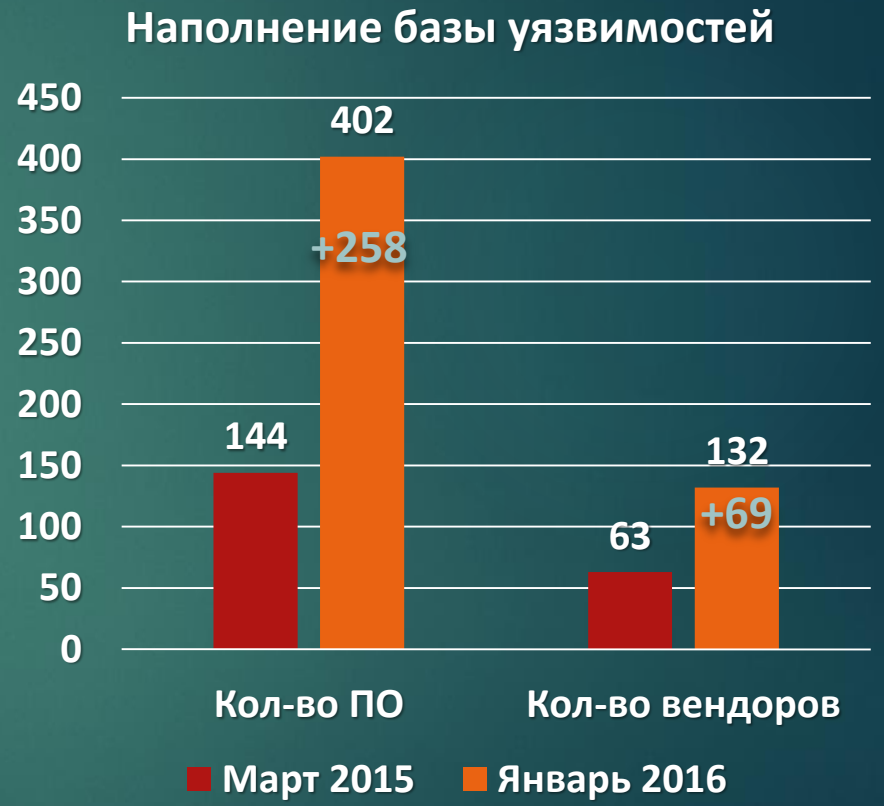
Причины возникновения угроз



Статистические данные актуальны по состоянию на 25.01.2016 г.

Динамика уязвимостей

Изменения с 10 марта 2015 по настоящее время

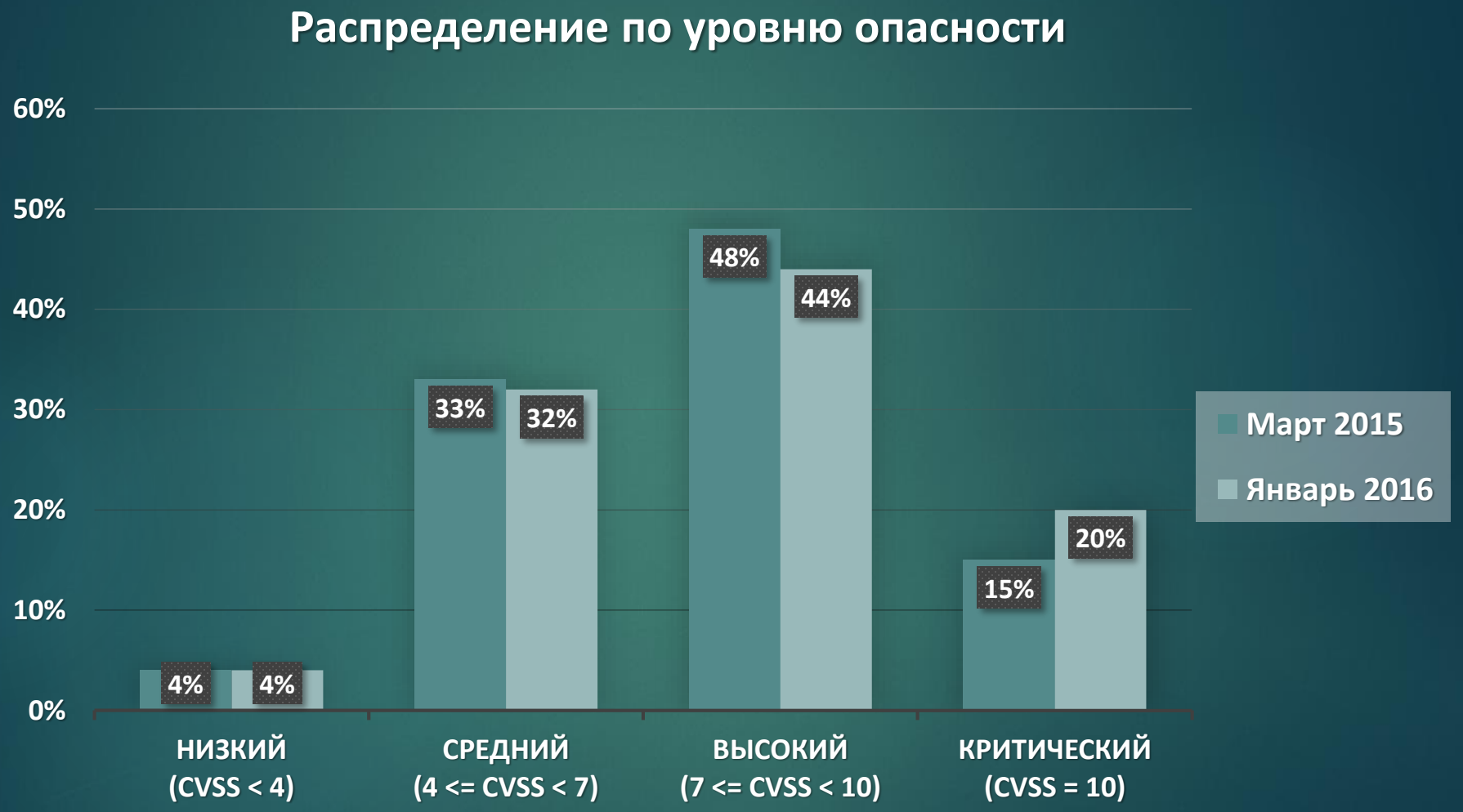


Статистические данные актуальны по состоянию на 25.01.2016 г.

Динамика уязвимостей

*По данным аналитиков bdu.fstec.ru (январь 2016 г.)

Динамика уязвимостей



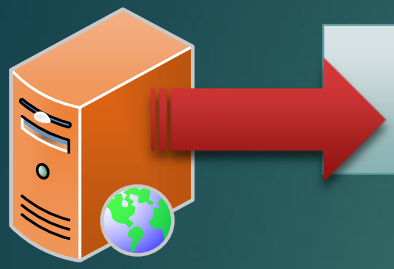
Статистические данные актуальны по состоянию на 25.01.2016 г.

Уязвимости в цифрах

Статистические данные актуальны по состоянию на 25.01.2016 г.

Потребители информации

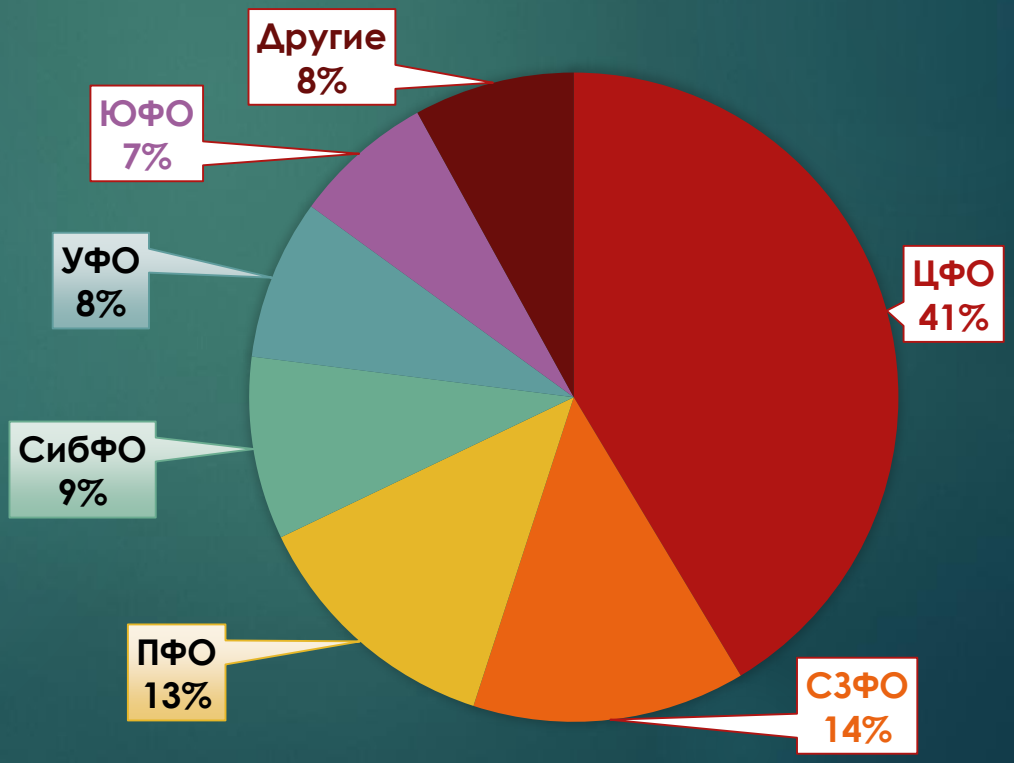
Изменения с 10 марта 2015 по настоящее время



Потребители банка данных угроз

Банк данных угроз безопасности информации

ПО ФЕДЕРАЛЬНЫМ ОКРУГАМ



- 56008 посещений
- 26430 уникальных пользователей
- 295460 страниц просмотрено

Банк данных угроз безопасности информации в сравнении с мировыми аналогами

Сравнение баз данных угроз

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

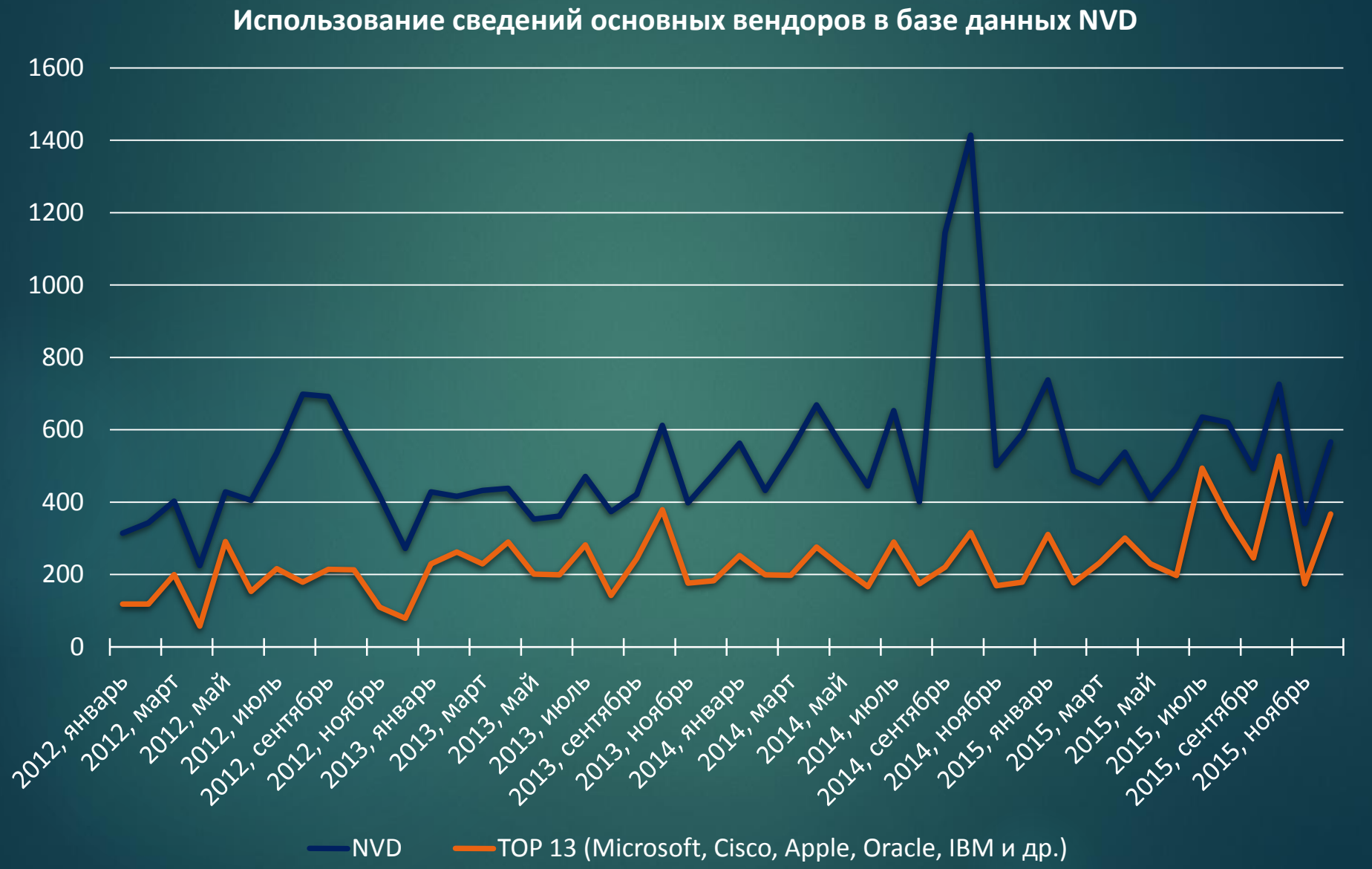
Сравнение баз данных уязвимостей

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
CVE/NVD	**17**	**>75000**	**16**	**>29000**	**>15000**	**БД США**
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
АЛТЭКС-СОФТ	8	-	11	-	-	БД OVAL-описаний
…	Известно **более 60** баз данных уязвимостей					

Уязвимости в цифрах

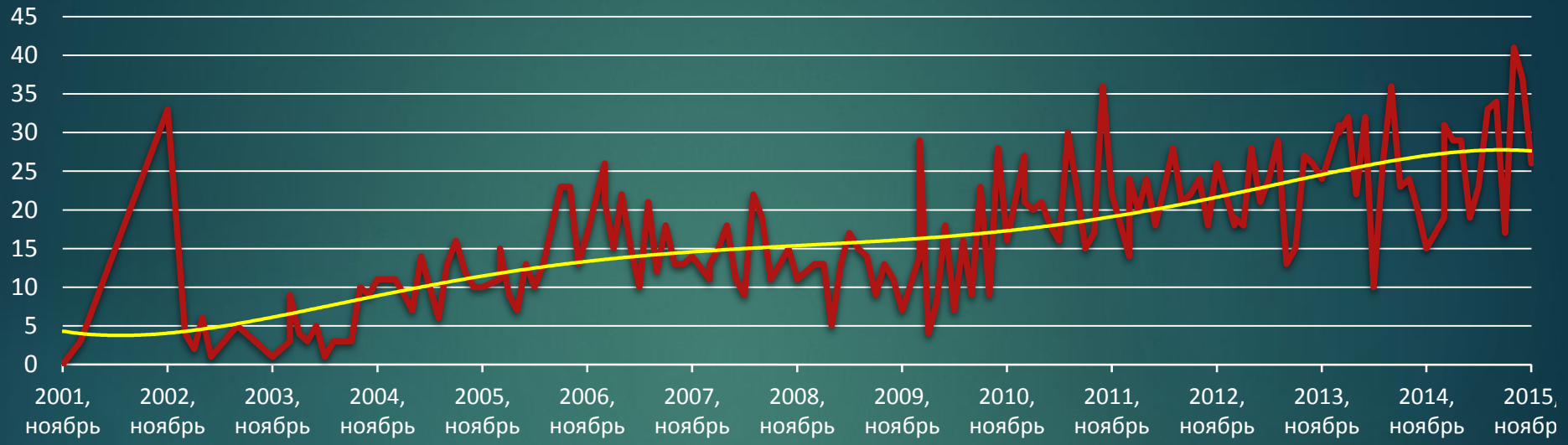
Статистические данные актуальны по состоянию на 25.01.2016 г.

Уязвимости в цифрах

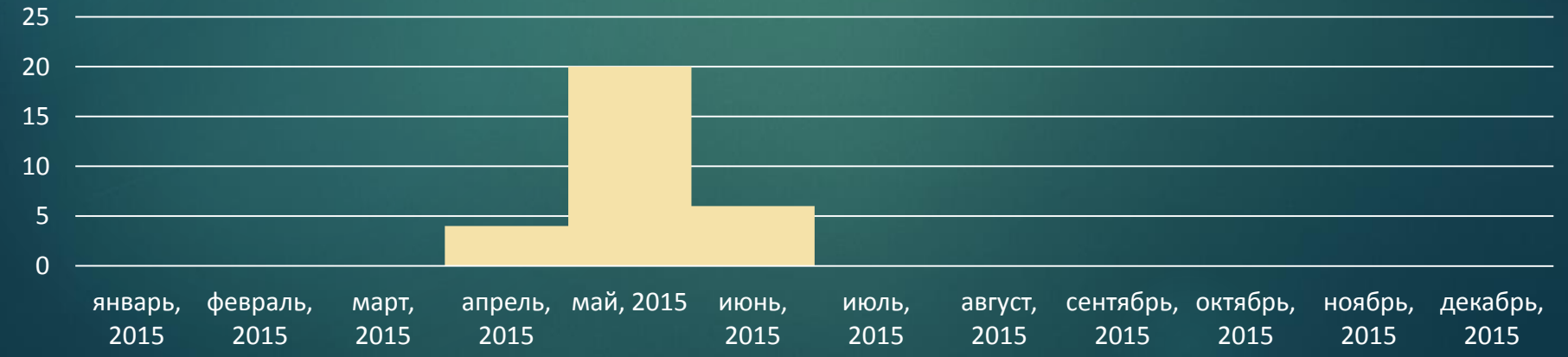


Уязвимости в цифрах

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



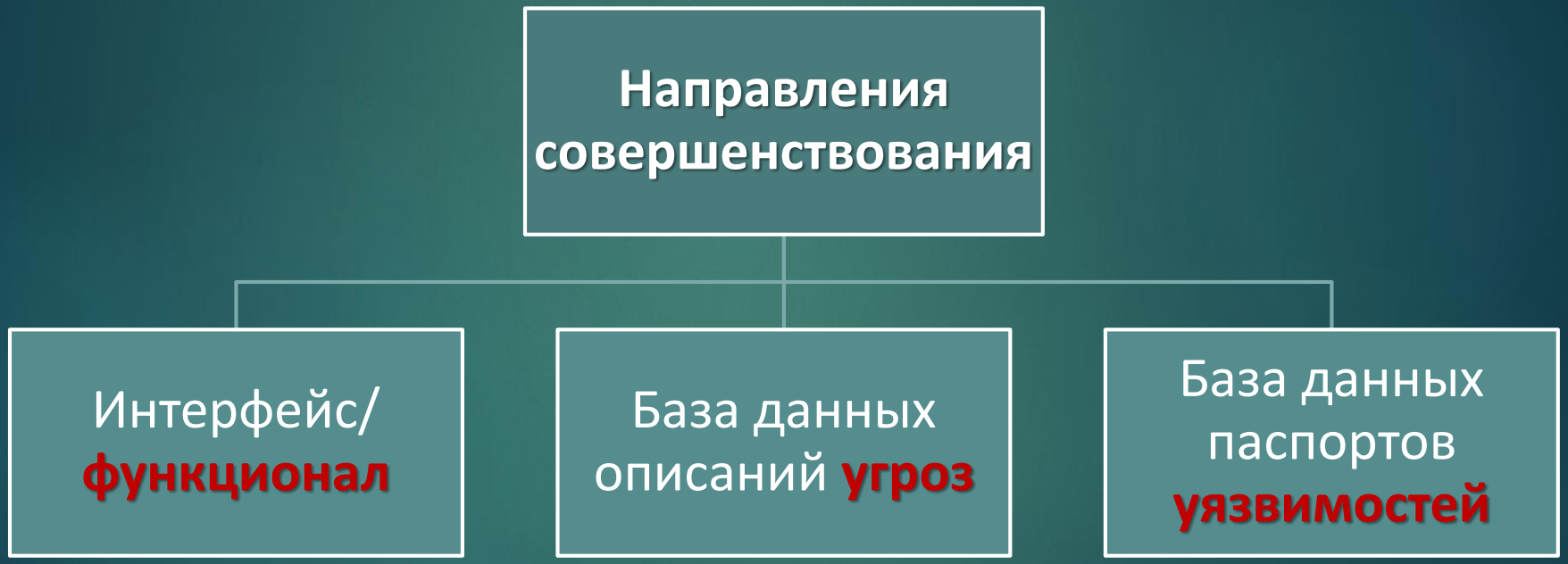
Динамика публикации сведений об уязвимостях, появившихся впервые в базе данных ФСТЭК России



Перспективы развития банка данных угроз безопасности информации

В перспективе: банк данных

Перспективы развития и совершенствования банка данных



В перспективе: функционал

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

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

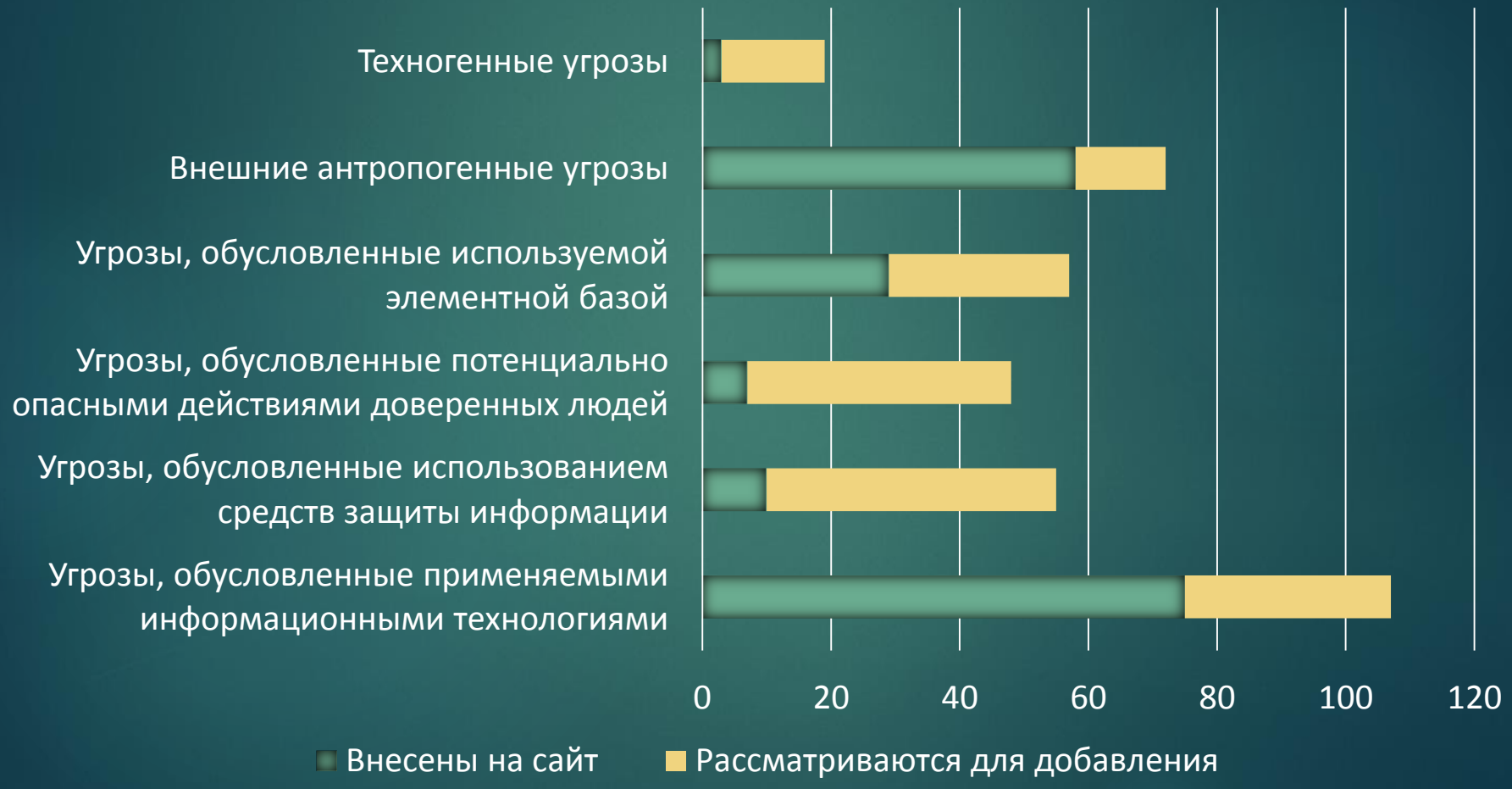
- Реализация подписки на обновления Банка данных;
- Реализация личного кабинета для выбора критериев подписки (пользовательские шаблоны подписки)

Реализация статистического модуля для сбора информации об обращениях к ресурсам сайта

Реализация нового раздела, включающего небезопасные конструкции кода

В перспективе: угрозы

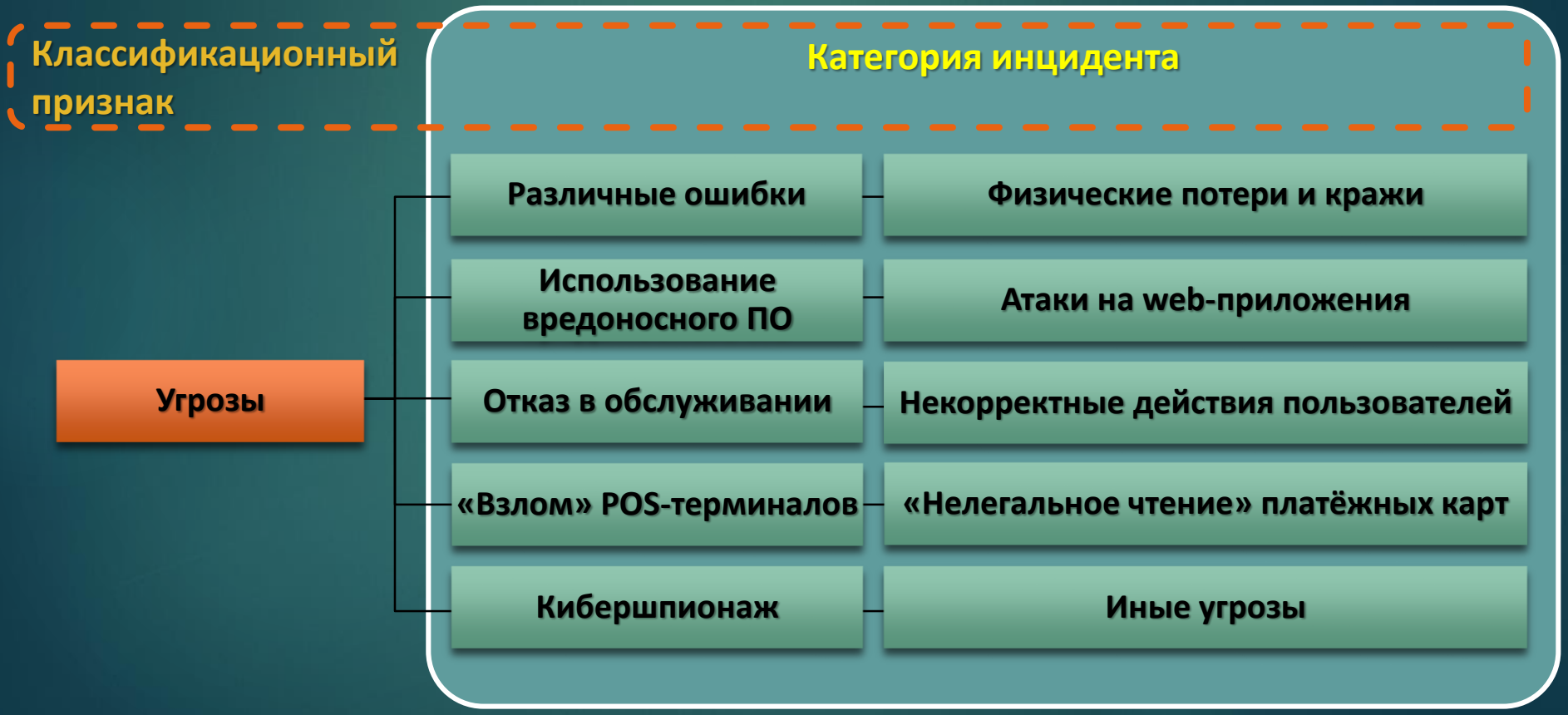
Перспективы пополнения перечня угроз



В перспективе: угрозы

Разработка различных классификаций

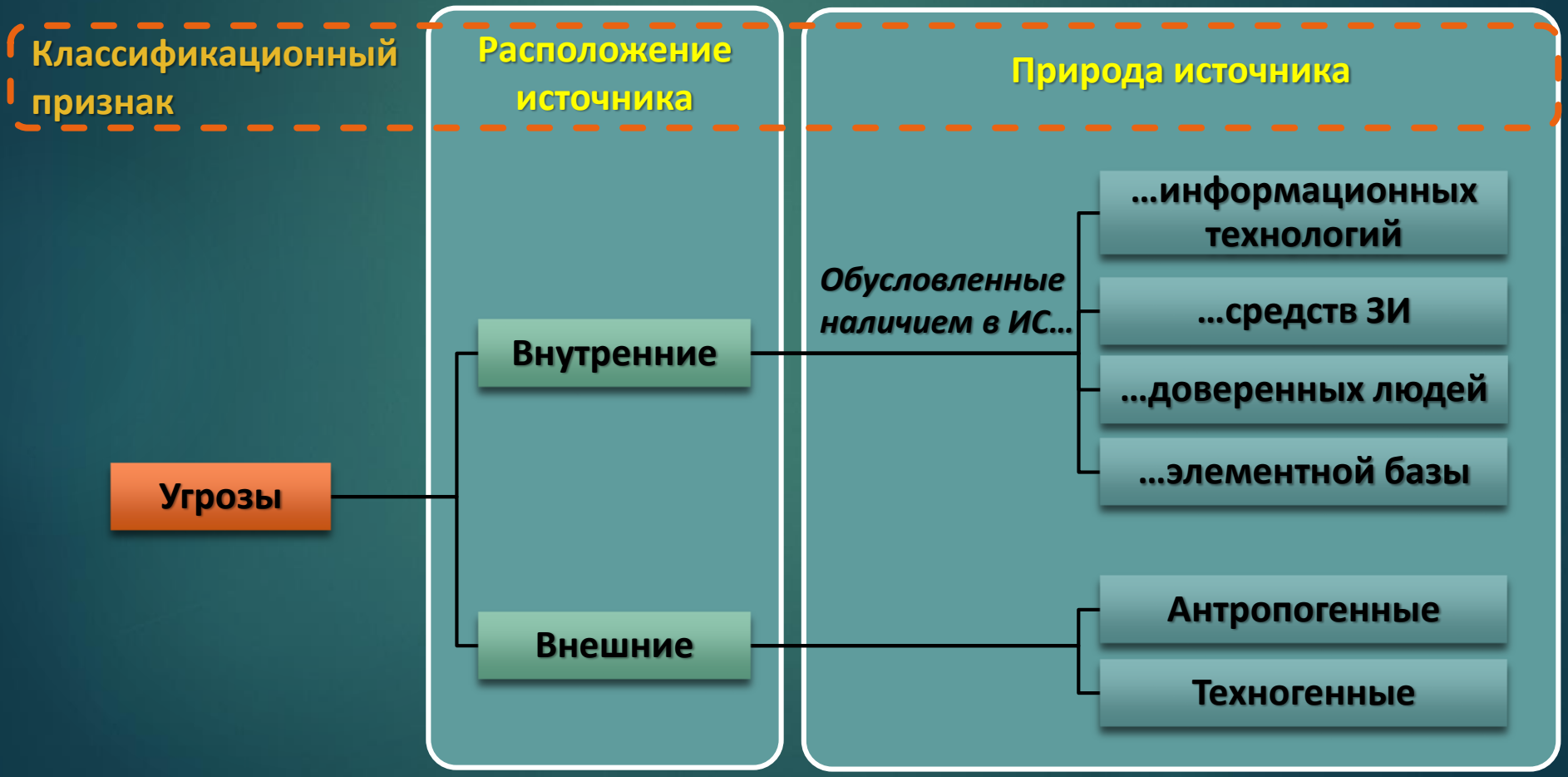
Классификация «по результату (по инцидентам)»



В перспективе: угрозы

Разработка различных классификаций

Классификация «по источнику»



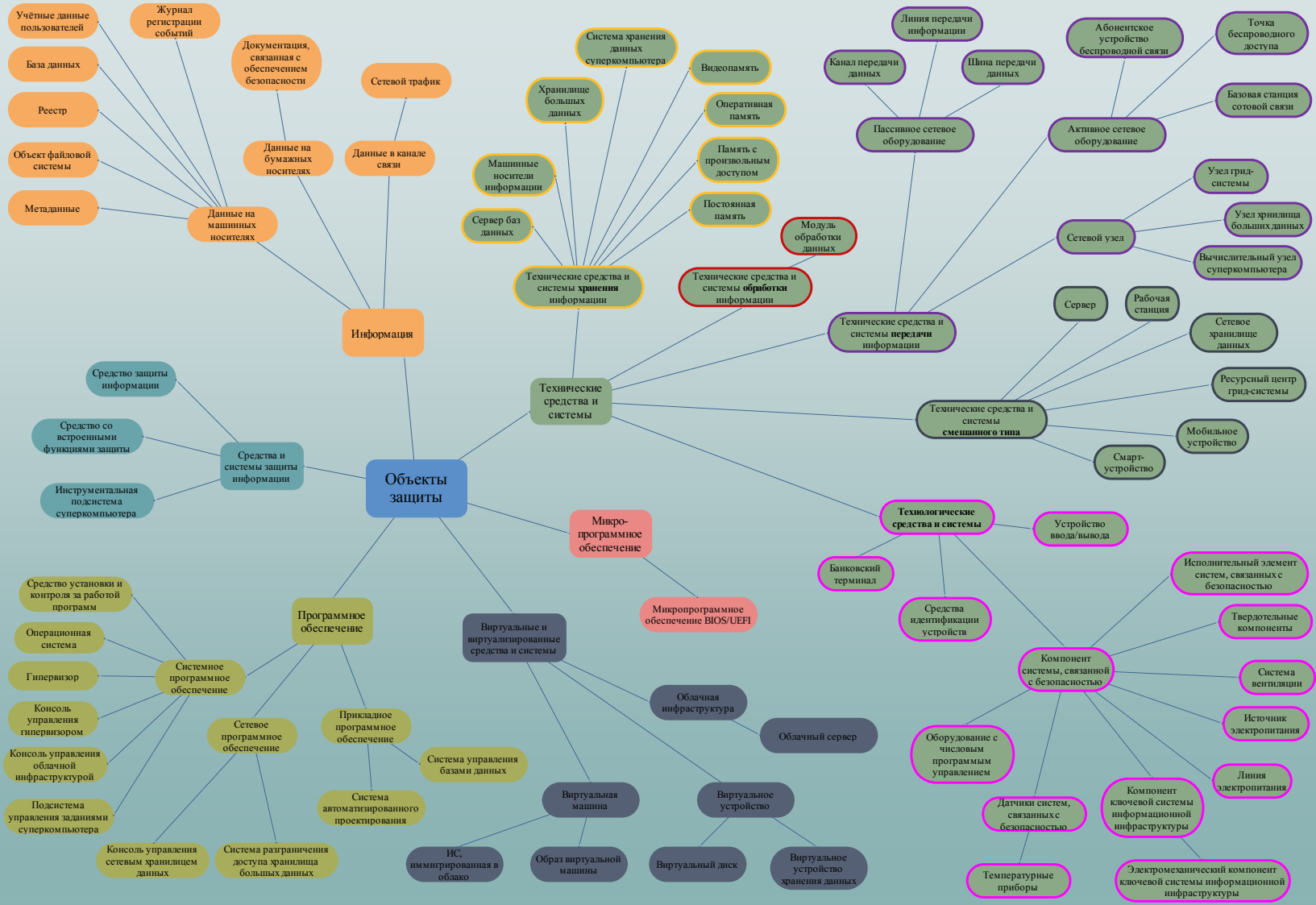
В перспективе: угрозы

Разработка различных классификаций

Классификация «по результату»

В перспективе: угрозы

Классификация «по объекту»



В перспективе: уязвимости

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