



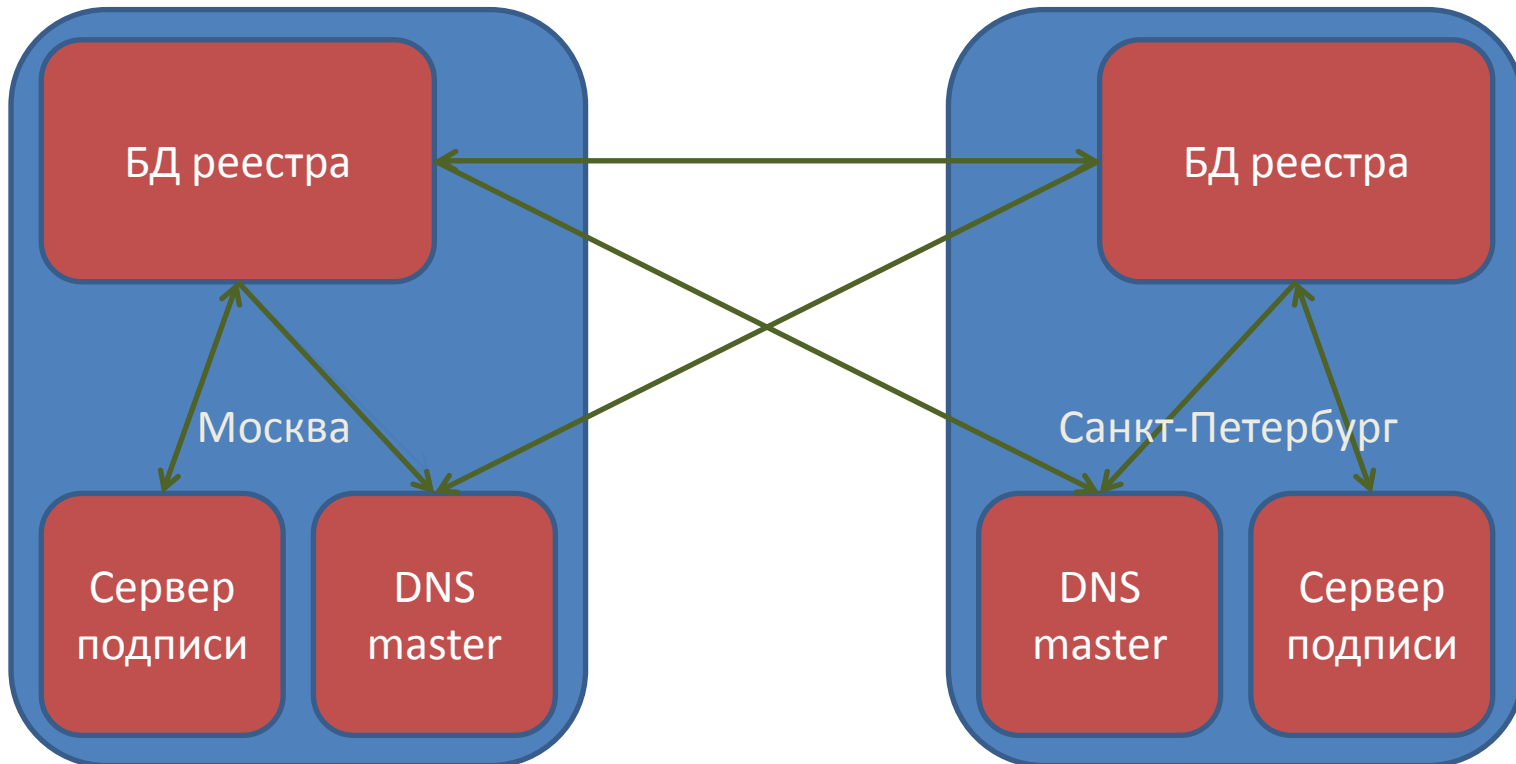
Technical  
Center  
of Internet

# DNSSec в России

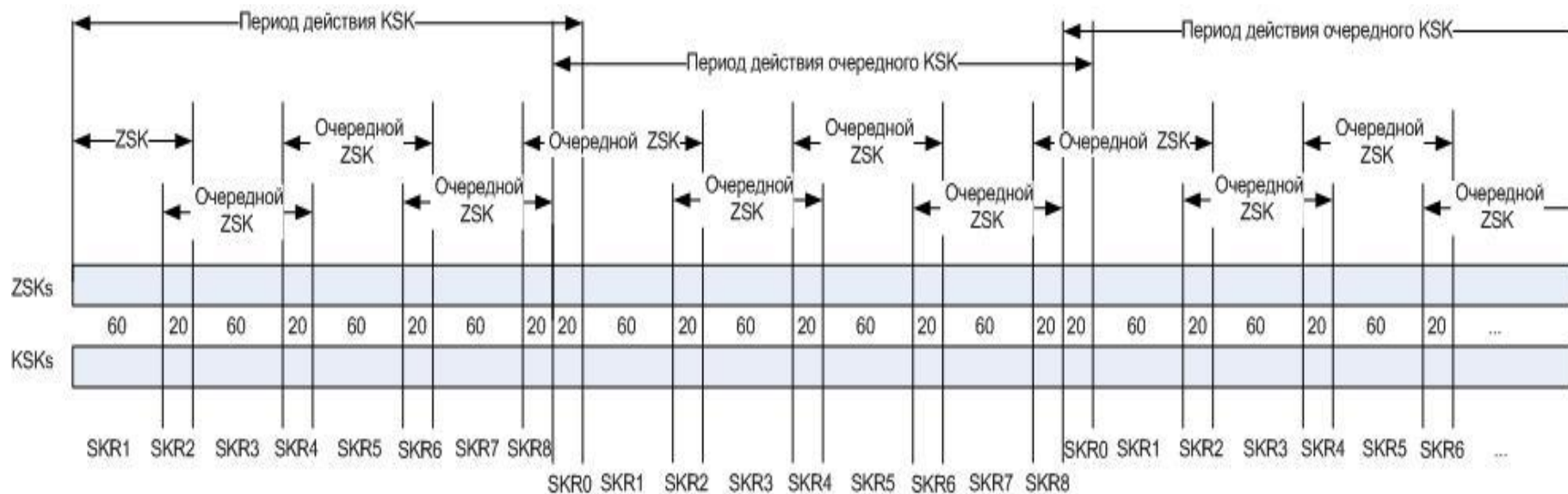
Андреев Петр  
[apn@ripn.net](mailto:apn@ripn.net)

Технический Центр Интернет









SKR2, SKR4, SKR6, SKR8 – ротация ZSK

SKR0 – ротация KSK



## Реализация



Technical  
Center  
of Internet

```
Создан новый ключ: 14072  
Дата создания: 04.12.2012  
Алгоритм: RSASHA256  
Длина ключа: 2048  
Открытый ключ:  
ru. IN DNSKEY 257 3 8  
AwEAAaPobiYPPlusu0ISLB4W+rrtpki/1d4pFxEdpQnWmMCeqznKXQC/  
AmIFopkUQHx1+v1AVy6e/dWaVxfSDMkH1Rdf8qJSTTgnp1QyUsvA2bvj  
KIGYVVrgcyoj/09rE02SLPko+fC6Ud5mS8f+GCuG+9T8uvj1Qk28WbAi  
PgL6dFIL4AaEt1HpHF6FXtkv3DRft+Z+xWSBEwEGJJzp2v14s0qUhVdo  
q2QqsnS6bUL9Z/GF5aroRuNYL2TD4w6pPm41eI6A83tavvBBvQQG16nb  
fkkZMm7Twiy+paZmfJJYyqueW4HSBMExMUv75Wj07nj1yRGMtCn9qIpe  
LR5bFQ83Hzc=
```

< OK >

Технический Центр Интернет

<ul style="list-style-type: none"> <li>Общая информация</li> <li>Новости</li> <li>+ Администрирование</li> <li>+ Журналы</li> <li>- Администрирование DNSSEC</li> <li><b>Параметры DNSSEC</b></li> <li>Управление ключами</li> <li>Ротация</li> <li>Публикации зоны</li> <li>Журналы и оповещения</li> <li>Наборы ключей</li> <li>Хранимые RRSIG</li> <li>Выгрузка KSR</li> <li>Выход</li> </ul>	<div style="background-color: #f0f0f0; padding: 5px; margin-bottom: 5px;"><b>РЕДАКТИРОВАТЬ ПАРАМЕТРЫ DNSSEC</b></div> <div style="margin-bottom: 5px;">             Зона <span style="border: 1px solid #ccc; padding: 2px;">RU</span> </div> <div style="margin-bottom: 5px; text-align: right;"> <span style="border: 1px solid #ccc; padding: 2px 5px;">Перейти</span> </div> <div style="margin-bottom: 5px;">             Подписывать зону <input checked="" type="checkbox"/> </div> <div style="margin-bottom: 5px;">             Использовать внешний KSK <input checked="" type="checkbox"/> </div> <div style="margin-bottom: 5px;">             Подтверждение шагов при ротации KSK <input checked="" type="checkbox"/> </div> <div style="margin-bottom: 5px;">             Подтверждение шагов при ротации ZSK <input checked="" type="checkbox"/> </div> <div style="margin-bottom: 5px;">             Алгоритм для ключей <span style="border: 1px solid #ccc; padding: 2px;">RSASHA256</span> </div> <div style="margin-bottom: 5px;">             Длина ключа KSK <span style="border: 1px solid #ccc; padding: 2px;">2048</span> </div> <div style="margin-bottom: 5px;">             Длина ключа ZSK <span style="border: 1px solid #ccc; padding: 2px;">1024</span> </div> <div style="margin-bottom: 5px;">             Период валидности KSK, дней <span style="border: 1px solid #ccc; padding: 2px;">365</span> </div> <div style="margin-bottom: 5px;">             Период валидности ZSK, дней <span style="border: 1px solid #ccc; padding: 2px;">90</span> </div> <div style="margin-bottom: 5px;">             Период валидности RRSIG, сек <span style="border: 1px solid #ccc; padding: 2px;">3888000</span> </div> <div style="margin-bottom: 5px;">             Разброс периода RRSIG, сек <span style="border: 1px solid #ccc; padding: 2px;">1296000</span> </div> <div style="margin-bottom: 5px;">             Смещение периода RRSIG, сек <span style="border: 1px solid #ccc; padding: 2px;">3600</span> </div> <div style="margin-bottom: 5px;">             Количество итераций NSEC3 (от 1 до 10) <span style="border: 1px solid #ccc; padding: 2px;">3</span> </div> <div style="margin-bottom: 5px;">             TTL зоны по умолчанию <span style="border: 1px solid #ccc; padding: 2px;">345600</span> </div> <div style="text-align: right; margin-top: 5px;"> <span style="border: 1px solid #ccc; padding: 2px 5px;">Сохранить</span> <span style="border: 1px solid #ccc; padding: 2px 5px; margin-left: 5px;">Отмена</span> <span style="border: 1px solid #ccc; padding: 2px 5px; margin-left: 5px;">Показать шаблоны и таймауты</span> </div>
--	---



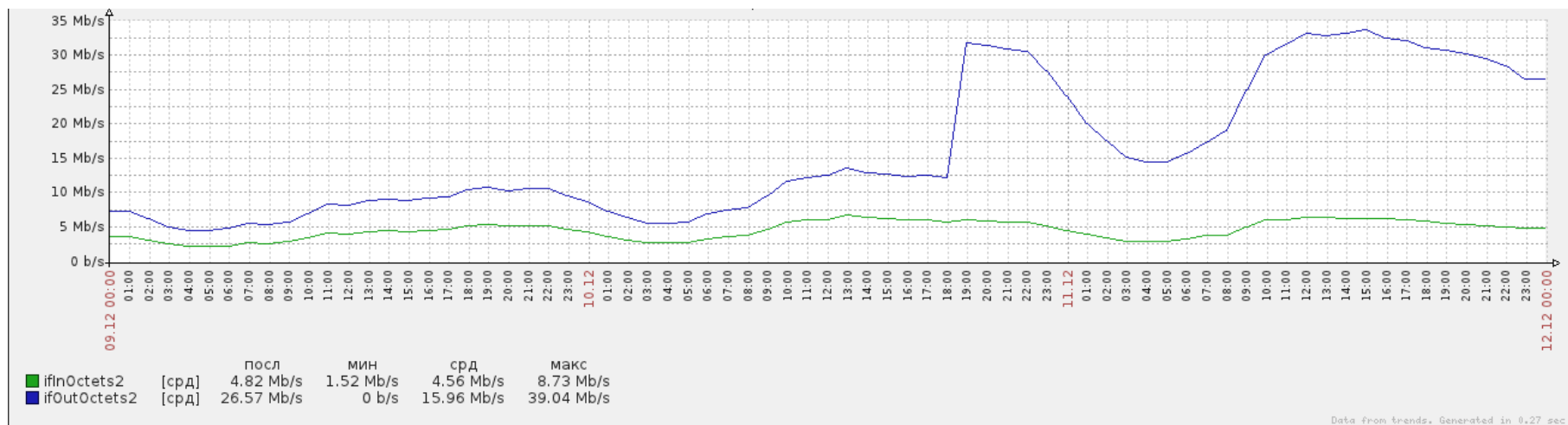
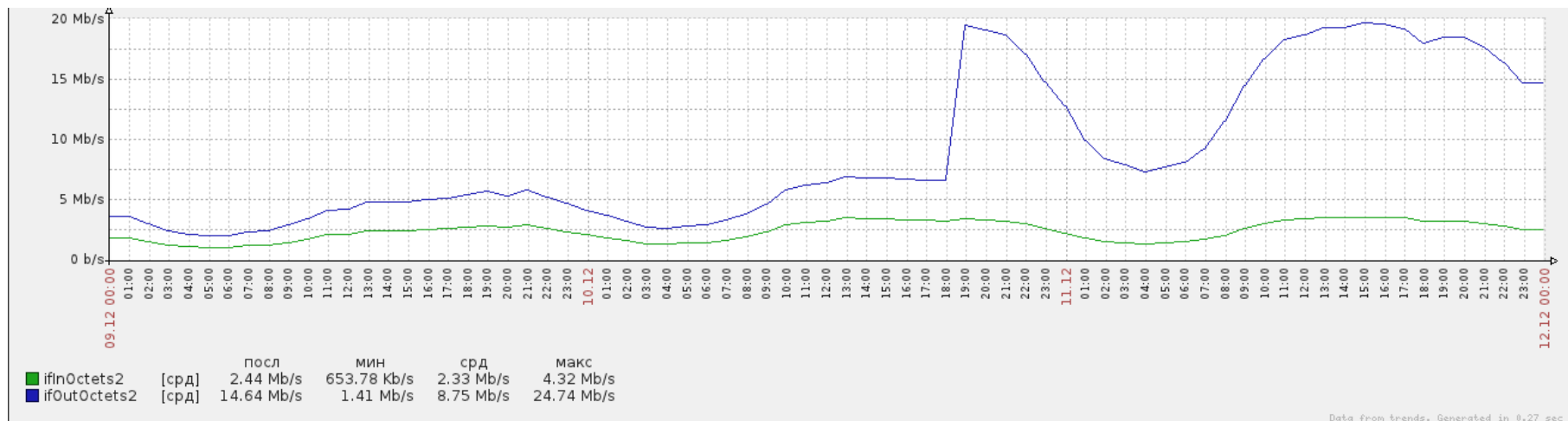
## Результат



Technical  
Center  
of Internet

	RU	SU	РФ
Всего	4166496	100287	600475
Подписанных	90	15	9
GOST	0	2	0
RSA/SHA-256	48	3	3
RSA/SHA-512	10	1	0
RSA/SHA-1	30	5	5
RSASHA1-NSEC3	2	2	1







## Результат



Technical  
Center  
of Internet

DNSSec-ready resolvers	
Запросов	4 000 000 000
DO бит	70%
Лидеры	
RND	92%
KZN	84%
NSK	83%
EKT	81%



## Результат



Technical  
Center  
of Internet

Статистика по доменам		
TLD	Кол-во доменов	Кол-во подписанных
RU	4166496	90
DE	15000000	1500
CZ	1049163	395559
BR	3203040	410414
NL	5243494	1446050



## Как дальше жить?



Technical  
Center  
of Internet

### -Техническому центру:

- Следовать описанному протоколу для имеющих и будущих TLD;

### - Регистраторам:

- Дать больше информации о DNSSec у себя на сайтах;

### - Пользователям:

- Взвесить «за» и «против» и решить – подписывать или нет.



**Technical  
Center  
of Internet**

Вопросы?