DNSSEC в домене .RU

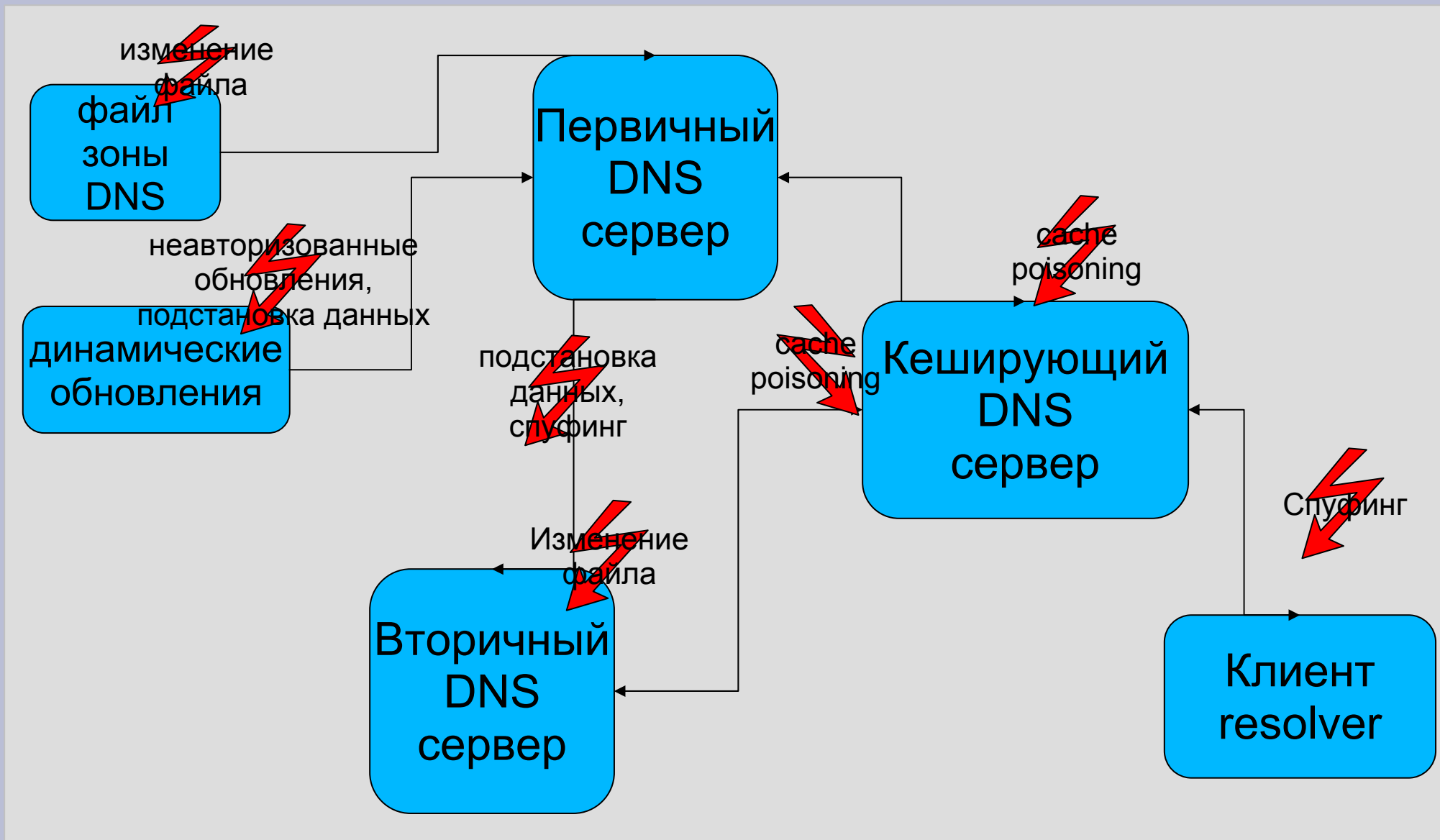
Garant-Park-Telecom

Внедрение защищенного протокола DNS в домене .RU

Зачем нужен DNSSEC?

- **DNS определяет, с каким именно сервером будет установлено соединение**
- **Протокол DNS не является надежным с точки зрения безопасности**

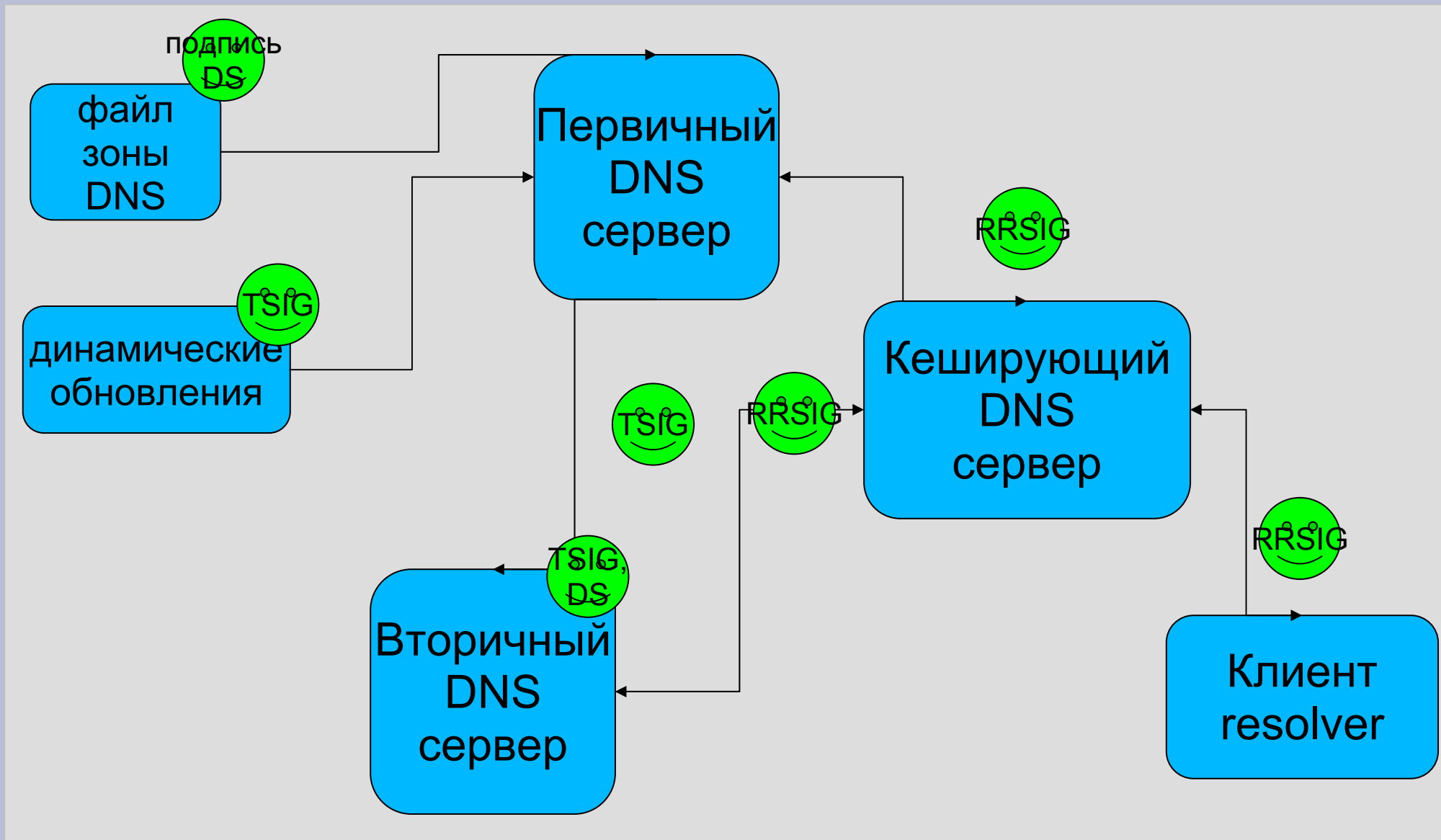
Источники угрозы



Так ли реальна угроза?

- Перехват пользовательской информации путем создания сайта-прослойки
- Перехват электронной почты, сообщений icq, паролей и т.д.
- Перехват передаваемых файлов
- Перехват телефонных звонков, использующих интернет-телефонию
- Выдача искаженной информации
- Искажения при обратном DNS-преобразовании

Решение DNSSEC



Поддерживающее ПО

- **BIND 9**
- **Drill Firefox extension (http://www.nlnetlabs.nl/ldns/)**
- **RIPE tools**
- **Интеграция с LDAP, IPSEC**
- **Портал http://www.dnssec.net/**

Настройка кеширующего DNS

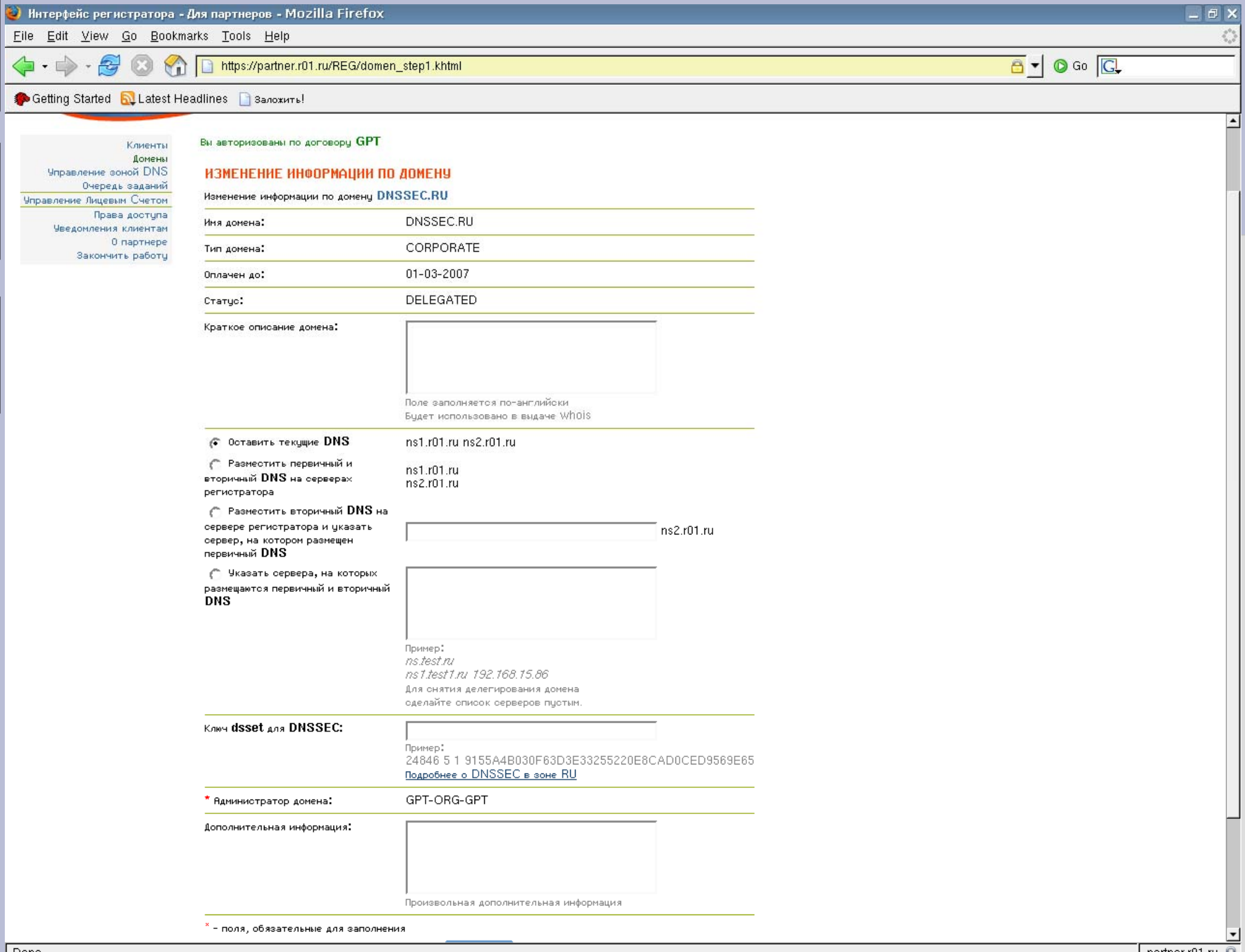
- Включение поддержки DNSSEC
  - **DNSSEC в корневом домене**
  - **“Острова безопасности”**
- **Уже подписаны: .NL, .SE, .MX, .*.UK, .COM, .NET, .ORG, RIPE backresolve**
  - **Look-aside DLV**
  - **Теперь и .RU**
  - **http://www.dnssec.ru/**

Делегирование домена с использованием DNSSEC

- Перевод домена к регистратору R01
- Генерирование ключей
- Подпись домена
- Делегирование с использованием DNSSEC: DS

Генерирование ключей

- dns# dnssec-keygen -r/dev/random -a RSASHA1 -b 1024 -n dnssec.ru
- -> Kdnssec.ru.+005+25721
- dns# dnssec-keygen -r/dev/random -f KSK -a RSASHA1 -b 1024 -n ZONE dnssec.ru
- -> Kdnssec.ru.+005.32463
- Добавляем ключи в файл домена
- $INCLUDE Kdnssec.ru.+005+25721
- $INCLUDE Kdnssec.ru.+005.32463
- dnssec-signzone -r /dev/random -o dnssec.ru -k Kdnssec.ru.+005+32463 dnsec.ru Kdnssec.ru.+005+25721.key


Интерфейс регистратора - Для партнеров - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
https://partner.r01.ru/REG/domen_step1.khtml
Go
Getting Started
Latest Headlines
Заложить!
Клиенты
Домены
Управление зоной DNS
Очередь заданий
Управление Лицевым Счетом
Права доступа
Уведомления клиентам
О партнере
Закончить работу
Вы авторизованы по договору GPT
ИЗМЕНЕНИЕ ИНФОРМАЦИИ ПО ДОМЕНУ
Изменение информации по домену DNSSEC.RU
Имя домена: DNSSEC.RU
Тип домена: CORPORATE
Оплачен до: 01-03-2007
Статус: DELEGATED
Краткое описание домена:
Поле заполняется по-английски
Будет использовано в выдаче Whois
Оставить текущие DNS
ns1.r01.ru ns2.r01.ru
Разместить первичный и вторичный DNS на серверах регистратора
ns1.r01.ru
ns2.r01.ru
Разместить вторичный DNS на сервере регистратора и указать сервер, на котором размещен первичный DNS
ns2.r01.ru
Указать сервера, на которых размещаются первичный и вторичный DNS
Пример:
ns.test.ru
ns1.test1.ru 192.168.15.86
Для снятия делегирования домена
сделайте список серверов пустым.
Ключ dsset для DNSSEC:
Пример:
24846 5 1 9155A4B030F63D3E33255220E8CAD0CED9569E65
Подробнее о DNSSEC в зоне RU
* Администратор домена: GPT-ORG-GPT
Дополнительная информация:
Произвольная дополнительная информация
* - поля, обязательные для заполнения

Настройка клиентского Bind

- options { dnssec-enable yes; };
- trusted-keys { "ru." 257 3 5 "AQPFTcrI419hTu06QuPs95t9e8rirIvmpNtqLRDKTu28iPv4xbNxKLbEuVlsjhfaSPqmqKnNmb7WeexloTCVbJe1jYf8g0c1Crec8TvglLq/PB/JCxD3aD2pmlBx6sOCiSXR3VpjvqMUzENI/PajSFpKnPs3dLAwrDrkqwSI M/ORZw=="; };
- zone “.ru” { type forward; forwarders { 195.24.65.7; 72.36.251.21; }; };

Проверка

```
$dig @127.0.0.1 ns.dnssec.ru +retry=1 +dnssec +multiline

; <<>> DiG 9.3.0beta3 <<>> @127.0.0.1 +retry=1 +dnssec +multiline
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 50414
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 5
```

Наличие флага ad и означает, что был получен защищенный DNS-ответ