*** НА ВАШЕМ АВТОРИТЕТНОМ СЕРВЕРЕ ***

1. Перейдите в каталог, в котором хранится зона, и сделайте резервную копия,
   на всякий случай. Предполагая, что зона называется "mytld":

```
$ cd /etc/namedb/master
$ sudo cp mytld mytld.backup
```

  Еще, создайте каталог для хранения ключей:

```
$ sudo mkdir /etc/namedb/keys
$ sudo chown bind /etc/namedb/keys

$ cd /etc/namedb/keys
```

2. Создайте первую пару ключей (ключ, подписывающий зону - ZSK)

```
$ sudo dnssec-keygen -a RSASHA256 -b 1024 -n ZONE mytld
```

Вывод команды будет примерно таким:

```
Generating key pair.....................+++++
+ ..................................................................................
.........................++++++
Kmytld.+008+51333
```

4. Создайте вторую пару ключей (ключ, подписывающий ключ - KSK)

```
$ sudo dnssec-keygen -f KSK -a RSASHA256 -b 2048 -n ZONE mytld
```

Опять, вы увидите вывод похожий на:

```
Generating key pair.............................................++
+ ..........................................................................+++
Kmytld.+008+52159
```

Давайте посмотрим на ключи:

```
# ls -l Kmytld.+008+5*
-rw-r--r--  1 root  wheel   203 Nov 29 00:07 Kmytld.+008+51333.key
-rw-------  1 root  wheel   937 Nov 29 00:07 Kmytld.+008+51333.private
-rw-r--r--  1 root  wheel   247 Nov 29 00:07 Kmytld.+008+52159.key
-rw-------  1 root  wheel  1125 Nov 29 00:07 Kmytld.+008+52159.private
```

5. Добавьте открытые ключи в конец файла зоны:

Отредактируйте файл зоны для "mytld", и добавьте ключи в конце:
Для того, чтобы узнать, какие файлы включить:

```
$ cd /etc/namedb/master
$ ls -lC1 /etc/namedb/keys/K*key
```

(скопируйте имена файлов, чтобы ва не пришлось набирать их вручную)

В файле "mytld", добавьте строки, соответствующие вашим ключам

```
  $ sudo ee mytld
```

```
; Ключи, публикуемые в наборе записей DNSKEY
```

```
    $include "/etc/namedb/keys/Kmytld.+008+51333.key"     ; ZSK
    $include "/etc/namedb/keys/Kmytld.+008+52159.key"     ; KSK
```

    Увеличьте серийный номер.
    Сохраните файл и выйдите из редактора.

6. Подпишите зону ключами

```
    $ cd /etc/namedb/keys
    $ sudo dnssec-signzone -x -o mytld -k Kmytld.+008+52159 ../master/mytld Kmytld.
+008+51333
```

    Вы должны увидеть:

```
Verifying the zone using the following algorithms: RSASHA256.
Zone signing complete:
Algorithm: RSASHA256: KSKs: 1 active, 0 stand-by, 0 revoked
                      ZSKs: 1 active, 0 stand-by, 0 revoked
../master/mytld.signed
```

    Замечание: хотя нам на самом деле и не надо указывать, какие ключи мы
    будем использовать - по умолчанию dnssec-signzone использует ключи,
    которые программа найде в самой зоне (те самые, добавленные на шаге 5
    при помощи $include) - это все равно хорошая идея.

    Таким образом мы делаем абсолютно ясным, какие именно ключи мы
    используем, особенно когда у вас есть несколько ключей.

    Подписанная зона была сохранена в каталоге master/, давайте ее
    проверим:

```
    $ cd /etc/namedb/master/
    $ ls -l mytld*

    -rw-r--r--  1 root  wheel   292 Nov 29 00:08 mytld
    -rw-r--r--  1 root  wheel  4294 Nov 29 00:20 mytld.signed
```

    Проверьте содержимое зоны в "mytld.signed", и посмотрите на новые
    записи и на подписи.

7. Заметьте, что был создан набор записей DS, готовый для передачи в
   родительскую зону:

```
    $ cd /etc/namedb/keys/
    $ ls -l dsset-*

    -rw-r--r--  1 root  wheel  155 Nov 29 00:22 dsset-mytld.
```

   Прогляните содержимое набора DS:

```
    $ cat dsset-mytld.
```

    Вы должны увидеть две строки, одну для каждого алгоритма используемого KSK.

8. Поменяйте раздел для зоны в /etc/namedb/named.conf, указывая на подписанную
зону:

```
    $ sudo ee /etc/namedb/named.conf
```

```
    zone "mytld" {
            type master;
            file "/etc/namedb/master/mytld.signed"; // загрузить подписанную зону
    };
```

9. Опять-таки в named.conf, включите dnssec (для авторитетных серверов):

    ... в разделе options { .. }; , добавьте

    ```
    dnssec-enable yes;
    ```

10. Переконфигурируйте или перезапустите ваш DNS сервер

    ```
    $ sudo rndc reconfig
    ```

    Вы можете также (хотя скорее всего, это не является необходимым) сделать:

    ```
    $ sudo rndc reload mytld
    ```

    ... для того чтобы "заставить" named перегрузить зону. Переконфигурирация обычно
    делает это, но в любом случае, перезагрузка не повредит :)

11. Проверьте, отвечает ли DNS сервер на запросы о записях DNSSEC:

    ```
    $ dig @127.0.0.1 mytld SOA +dnssec
    ```

12. Теперь вам нужно убедиться, что ваш слейв ТАКЖЕ сконфигурирован с поддержкой
    dnssec в своей конфигурации (шаг 8). Это уже должно быть сделано, потому
    что группа, отвечающая за ваш слейв тоже выполняет эту лабораторку, но
    проверьте в любом случае!

    Для проверки:

    ```
    $ dig @10.20.Y.1 mytld SOA +dnssec
    ```

    ... где Y - IP партнера вы выбрали как слейва для вашего домена - это может
    быть преподаватель, в таком случае спросите его.

13. Теперь вам нужно передать DS в родительскую зону

   Свяжитесь с администратором корневой зоны для того чтобы
   определить метод передачи. Это может быть scp или web интерфейс.

    a) при использовании RZM:

    Посетите https://rzm.dnssek.org/

    Залогиньтесь (вы должны были получить логин раньше)

    В Trust Anchor Details убедитесь, что ваш DS появился автоматически
    и что он совпадает с настоящим. Он НЕ БУДЕТ активирован автоматически -
    единственное, что RZM сделал, это "увидел" запись DNSKEY которую
    вы предполагаемо опубликовали, и теперь ждет вашего подтверждения
    для включения DS в родительскую зону.

    Сравните DS записи в файле dsset-mytld с тем, что показывает RZM,
    и потому нажмите на один или оба "глаза" (только один нужен на

самом деле), подождите появления "галочки" и нажмите "Update".

b) если RZM не используется:

Если администратор корневой зоны говорит использовать scp,
сделайте следующее:

```
$ cd /etc/namedb/keys
$ scp dsset-mytld. sysadm@a.root-servers.net:
```

... это скопирует файл "dsset-mytld." в каталог "sysadm" на сервере a.root-server,
и тогда администратор корневой зоны сможет включить этот файл в корневую зону
для подписи.

Сообщите ему, когда вы закачали этот файл.

14. Подождите несколько минут до появления DS в корневой зоне.

Распространение DS-записей на все корневые сервера займет какое-то
время (обновить файл корневой зоны, подписать его, опубликовать на
корневых серверах, подгрузить в кэширующий сервер и т.д.)

Для проверки того, что DS включен в родительскую (корневую) зону:

```
dig @a.root-servers.net DS mytld.
```

Когда вы убедились в том, что DS включен в родительскую зону,
используя dig:

... только тогда вы можете начать тестирование валидации!

15. Проверьте что бит AD установлен:

```
# dig @10.20.0.230 +dnssec www.MYTLD.
```

Установлен?

Если нет, заметьте, что администратор корневой зоны не обязательно успел
подписать корневую зону с вашим DS внутри, ИЛИ, из-за отрицательного
кэширования, запись DS может пока еще не быть в кэше. Вам возможно
придется подождать еще, но спросите администратора корневой зоны;
вы также всегда можете спросить корневой сервер напрямую:

```
# dig @a.root-servers.net DS mytld.
```

... чтобы убедиться что DS опубликован. Тогда осталось всего только
подождать, пока время кэширования истечет в системе разрешения имен,
прежде чем вы сможете проверить ваши подписи.

Или просто не ждите и разрешите валидацию на вашем собственном кэширующем
сервере (resolv.grpX.dns.nsrc.org) - смотрите соответствующую лабораторную
работу!