DNSSEC включаем в BIND-е

Создаем каталог для хранения ключей и переходим в него:

```
# cd /var/name && mkdir keys && cd keys
```

Генерируем мастер ключ (KSK):

```
#  dnssec-keygen -f KSK -a RSASHA256 -b 2048 -n ZONE -r /dev/urandom tst-amo.net.ua
```

- -f KSK – флаг о формировании мастер ключа;
- -a RSASHA256 – используемый алгоритм шифрования;
- -b 2048 – размер ключа в битах;
- -n ZONE – для DNS-зоны;
- -r /dev/urandom – путь к файлу со случайными данными;
- tst-amo.net.ua – домен, для которого предназначен ключ

Генерируем ключ для зоны (ZSK):

```
# dnssec-keygen -a RSASHA1 -b 2048 -n ZONE -r /dev/urandom tst-amo.net.ua
```

Меняем владельца:

```
# chown -R named:named /var/named/keys
```

Так как DNSSEC основан на обеспечении цепочки доверия, чтобы процесс верификации заработал, требуется чтобы регистратор заверил созданный KSK-ключ, подтвердив своё доверие. Для этого создадим на основе KSK-ключа DSKEY-ключ (Delegation Signature Key)

```
# dnssec-dsfromkey Ktst-amo.net.ua.+008+22218
tst-amo.net.ua.      IN      DS      22218      8      1
CDB052AE305815F96068F4FCEB57FD9BD47D7470
tst-amo.net.ua.      IN      DS      22218      8      2
578D09B53ADE8A9AE6410DEA8631BFAF2AE570F6E4E0CED88703D76BD9D7BE
AE
```

Далее необходимо добавить DS-записи в панели регистратора домена. Они были сгенерированы при выполнении dnssec-signzone

и находятся в файле dsset-my-domain в таком виде:

Значения полей в DS-записи:

86400 – TTL данной записи
22218 – Key Tag
8 – Algorithm
1 и 2 – Digest Type

В приведенном выше примере при генерации ключей был использован алгоритм RSA-SHA1, поэтому запись имеет номер 8.

Таблица номеров алгоритмов:

Number	**Algorithm**
1	RSAMD5
2	DH
3	DSA/SHA1
4	ECC
5	RSA/SHA-1
6	DSA-NSEC3-SHA1
7	RSASHA1-NSEC3-SHA1
8	RSA/SHA-256
9	–
10	RSA/SHA-512
11	–
12	ГОСТ Р 34.10-2001

Digest Type в приведенном примере у первой записи равен 1, во второй 2.

Таблица номеров Digest Type:

Number	**Digest Type**
1	SHA-1
2	SHA-256

3	SHA-512