**Создание запроса на тестовый сертификат открытого ключа**

Действия при создании запроса на сертификат:

1. Выбрать из основного меню Windows: «Пуск» - «Программы» - «Авест» - «Персональный менеджер сертификатов Авест для ГосСУОК» - «Создать запрос» - «Подготовить запрос на сертификат»;
2. В появившемся окне мастера создания запроса на сертификат выбрать шаблон для создания сертификата (см. [Рисунок 1. Выбор шаблона для создания сертификата](#page35)) и нажать кнопку «Далее»;



Рисунок 1. Выбор шаблона для создания сертификата

1. В следующем диалоговом окне необходимо задать атрибуты (заполнить пустые поля) будущего владельца сертификата, включаемые в запрос на сертификат (см. [Рисунок 2.](#page36) [Заполнение атрибутов владельца сертификата](#page36));



Рисунок 2. Заполнение атрибутов владельца сертификата

1. Затем появится диалоговое окно, в котором будет указано применение личного ключа пользователя (см. [Рисунок 3. Применени](#page44)е личного ключа). Необходимые параметры применения личного ключа уже заданы по умолчанию (являются константой) и не требуют корректировки.



Рисунок 3. Применение личного ключа

1. В следующем диалоговом окне следует определить срок действия сертификата пользователя (см. [Рисунок 4. Ввод сроков действия сертификата](#page30));

По умолчанию включен флажок «Срок действия сертификата задается удостоверяющим центром» и поля «действителен с» и «действителен по» заполнены значениями «0». Для того, чтобы указать другой срок действия сертификата, необходимо убрать флажок «Срок действия сертификата задается удостоверяющим центром» и ввести нужный срок действия (при этом максимальный срок действия тестовых сертификатов – 6 месяцев).



 [Рисунок 4. Срок](#page30) действия сертификата

1. После указания сроков действия сертификата в окне «Создание открытого и секретного ключа» следует задать имя контейнера (см. [Рисунок 5. Атрибуты ключевой пары](#page38)).



 Рисунок 5. Атрибуты ключевой пары

1. Далее в открывшемся окне необходимо:
- выбрать подключенный к компьютеру носитель ключевой информации, на который необходимо записать контейнер (в поле «Носитель» должен отобразиться серийный номер носителя);
- ввести пароль от носителя ключевой информации или придумать новый (если пароль на носитель еще не установлен);
- нажать кнопку «ОК» (см. Рисунок 6. Генерация ключей)



 Рисунок 6. Генерация ключей

Далее (для сбора случайных последовательностей) необходимо водить курсором мыши в пределах появившегося окна, пока соответствующая полоса не будет полностью заполнена. После указанных действия откроется окно «Формирование карточки открытого ключа». Если оставить галочки по умолчанию и нажать кнопку «Далее», то на следующем шаге откроется карточка открытого ключа, в которой можно проверить введенные данные, а также распечатать саму карточку открытого ключа (при необходимости). После просмотра сведений необходимо закрыть окно.

1. В открывшемся окне «Экспорт запроса в файл» необходимо указать путь сохранения сформированного файла запроса (\*.req). Для этого нужно нажать кнопку «Обзор», выбрать путь сохранения и нажать кнопку «Далее».
2. В последнем окне мастера создания запроса на сертификат будет информация о том, что запрос на сертификат создан. Для окончания работы с мастером создания запроса на сертификат надо нажать кнопку «Закрыть».