Устройство криптографической защиты данных «Криптон»


Ключевые элементы ГОСТ 28147-89
Набор узлов замены (8*16*4=512 бит)
256 битный ключ
Системообразующий элемент
Хранится в файле uz.db3 на ключевом носителе
Первый ключевой элемент, вводимый в криптоплату при инициализации
Создается криптоадминистратором
Все ПК криптосети должны иметь одинаковые УЗ

Ключевая система «Криптон»

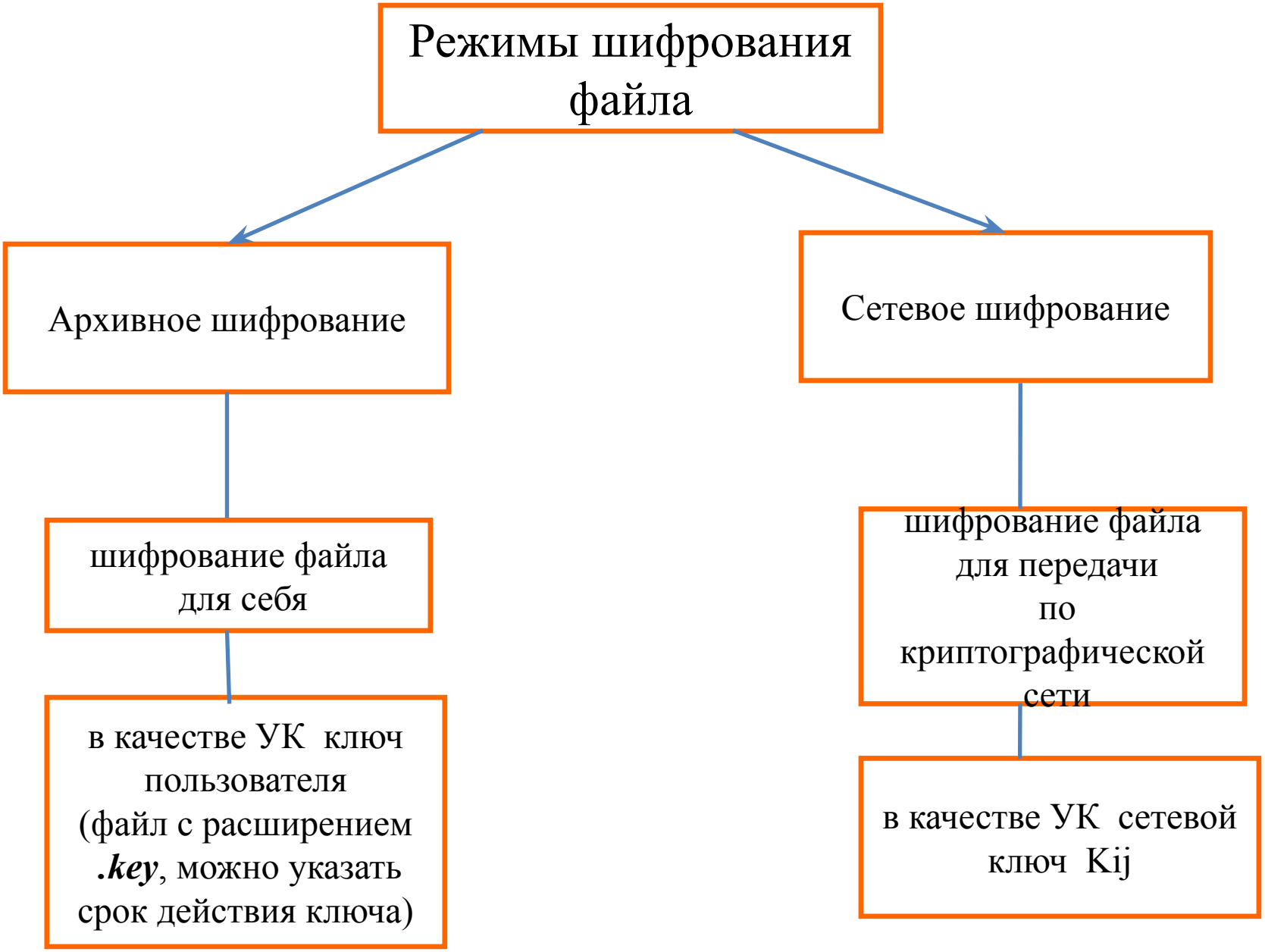
Датчик случайных чисел генерирует файловый ключ

Каждый файл шифруется на своем файловом ключе

Файловый ключ при передаче шифруется на условном ключе

Условный ключ шифруется на главном ключе, который хранится в файле qk.db3

Главный ключ шифруется на пароле, который вводится администратором

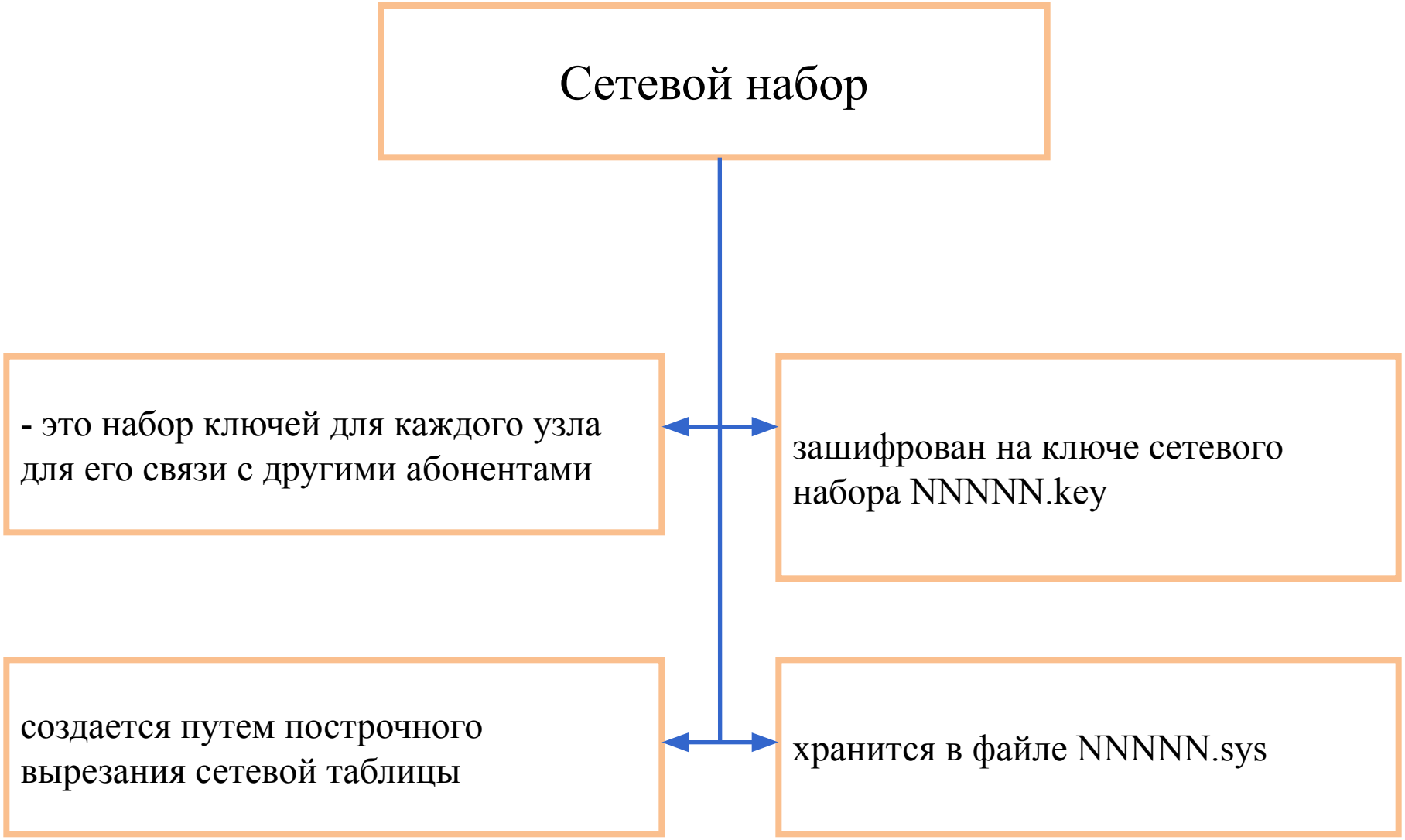

Режимы шифрования файла
Архивное шифрование
Сетевое шифрование
шифрование файла для себя
в качестве УК ключ пользователя (файл с расширением ***.key***, можно указать срок действия ключа)
шифрование файла для передачи по криптографической сети
в качестве УК сетевой ключ Kij

Матрица сетевой таблицы симметрична: $k_{ij} = k_{ji}$.

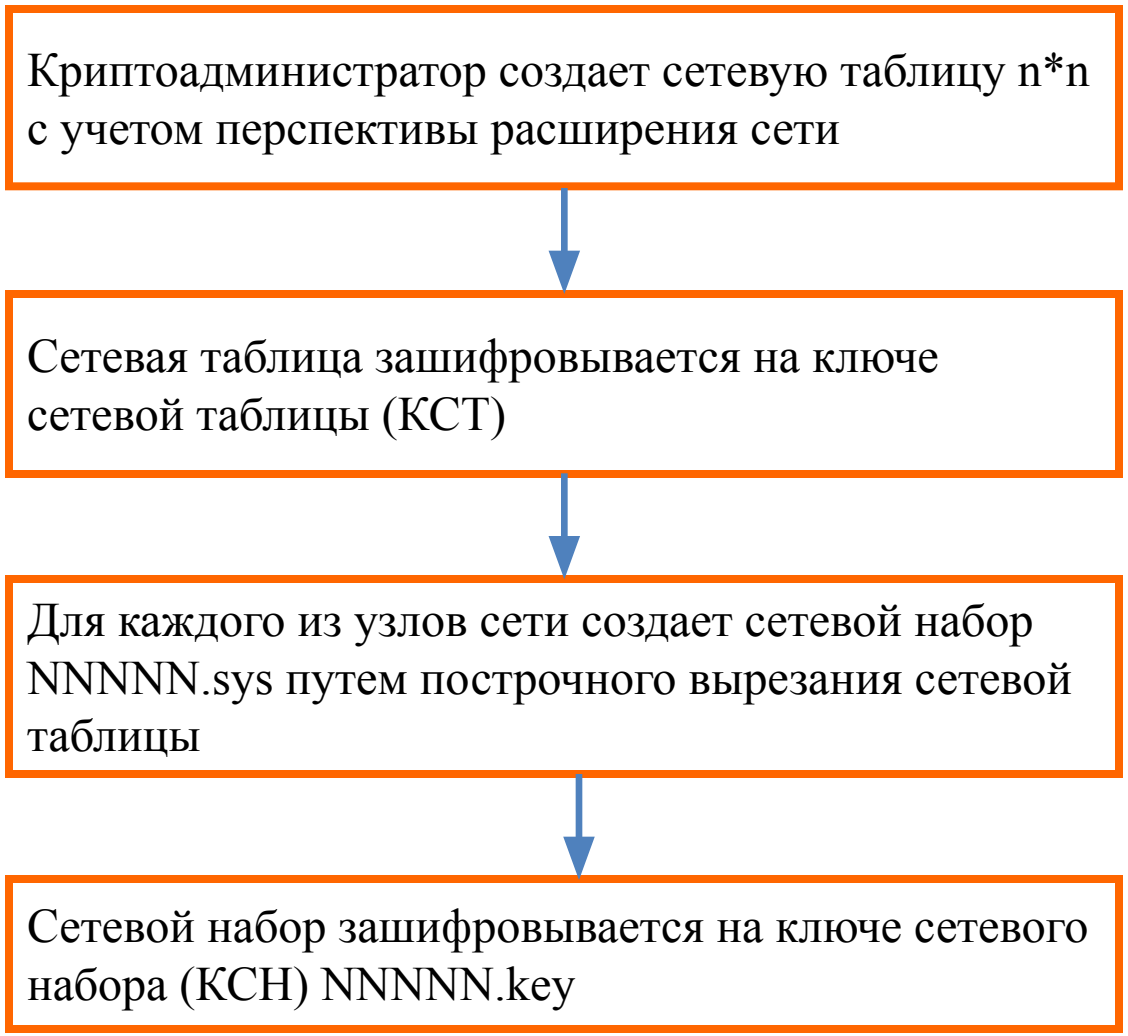
	k_{12}	k_{13}	k_{14}	k_{14}	k_{16}	k_{17}	k_{18}	k_{19}
k_{21}		k_{23}	k_{24}	k_{25}	k_{26}	k_{27}	k_{28}	k_{29}
k_{31}	k_{32}		k_{34}	k_{35}	k_{36}	k_{37}	k_{38}	k_{39}
k_{41}	k_{42}	k_{43}		k_{45}	k_{46}	k_{47}	k_{48}	k_{49}
k_{51}	k_{52}	k_{53}	k_{54}		k_{56}	k_{57}	k_{58}	k_{59}
k_{61}	k_{62}	k_{63}	k_{64}	k_{65}		k_{67}	k_{68}	k_{69}
k_{71}	k_{72}	k_{73}	k_{74}	k_{75}	k_{76}		k_{78}	k_{79}
k_{81}	k_{82}	k_{83}	k_{84}	k_{85}	k_{86}	k_{87}		k_{89}
k_{91}	k_{92}	k_{93}	k_{94}	k_{95}	k_{96}	k_{97}	k_{98}	

Создание сетевого набора

	k_{12}	k_{13}	k_{14}	k_{14}	k_{16}	k_{17}	k_{18}	k_{19}
k_{21}		k_{23}	k_{24}	k_{25}	k_{26}	k_{27}	k_{28}	k_{29}
k_{31}	k_{32}		k_{34}	k_{35}	k_{36}	k_{37}	k_{38}	k_{39}
k_{41}	k_{42}	k_{43}		k_{45}	k_{46}	k_{47}	k_{48}	k_{49}
k_{51}	k_{52}	k_{53}	k_{54}		k_{56}	k_{57}	k_{58}	k_{59}
k_{61}	k_{62}	k_{63}	k_{64}	k_{65}		k_{67}	k_{68}	k_{69}
k_{71}	k_{72}	k_{73}	k_{74}	k_{75}	k_{76}		k_{78}	k_{79}
k_{81}	k_{82}	k_{83}	k_{84}	k_{85}	k_{86}	k_{87}		k_{89}
k_{91}	k_{92}	k_{93}	k_{94}	k_{95}	k_{96}	k_{97}	k_{98}	


Сетевой набор
- это набор ключей для каждого узла для его связи с другими абонентами
зашифрован на ключе сетевого набора NNNNN.key
создается путем построчного вырезания сетевой таблицы
хранится в файле NNNNN.sys

Создание сетевых ключей



Сетевое шифрование

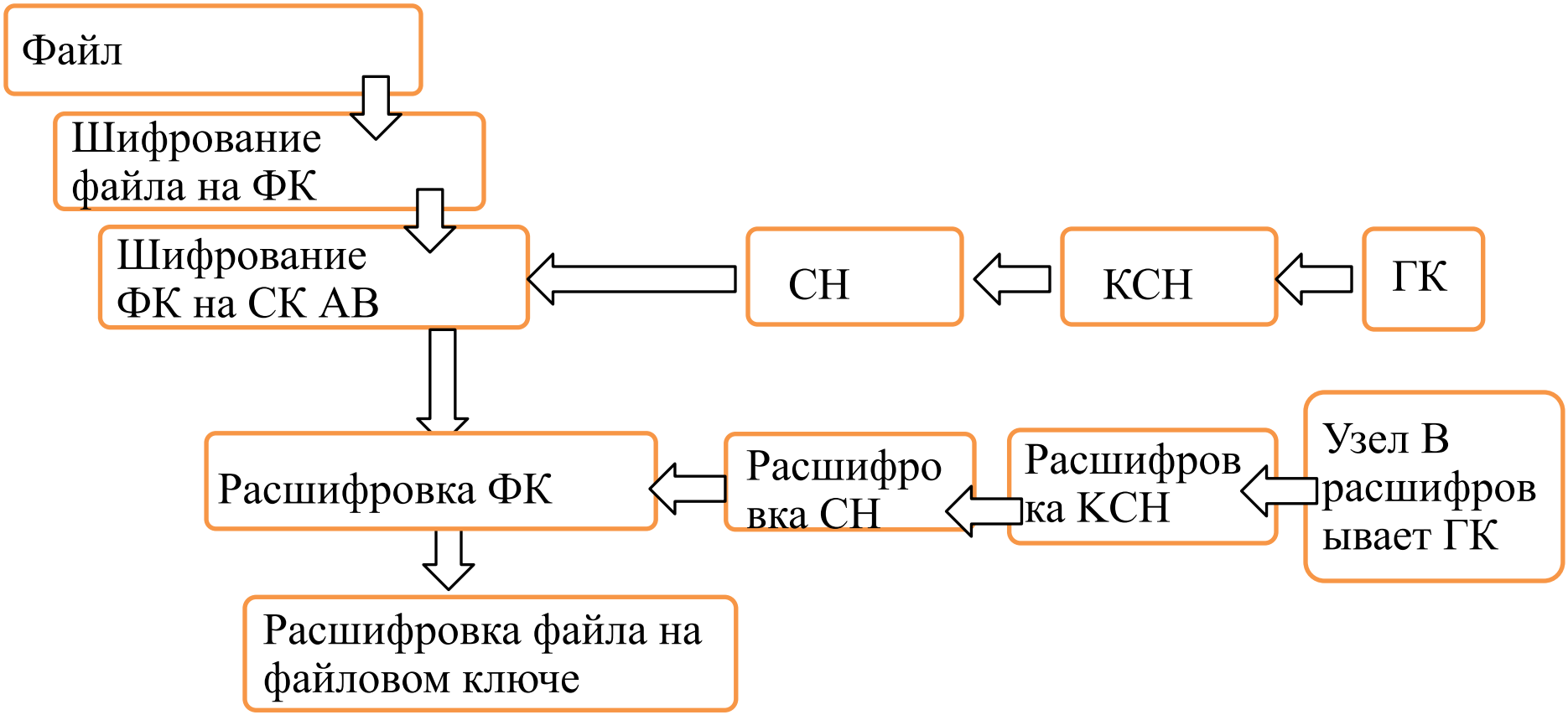
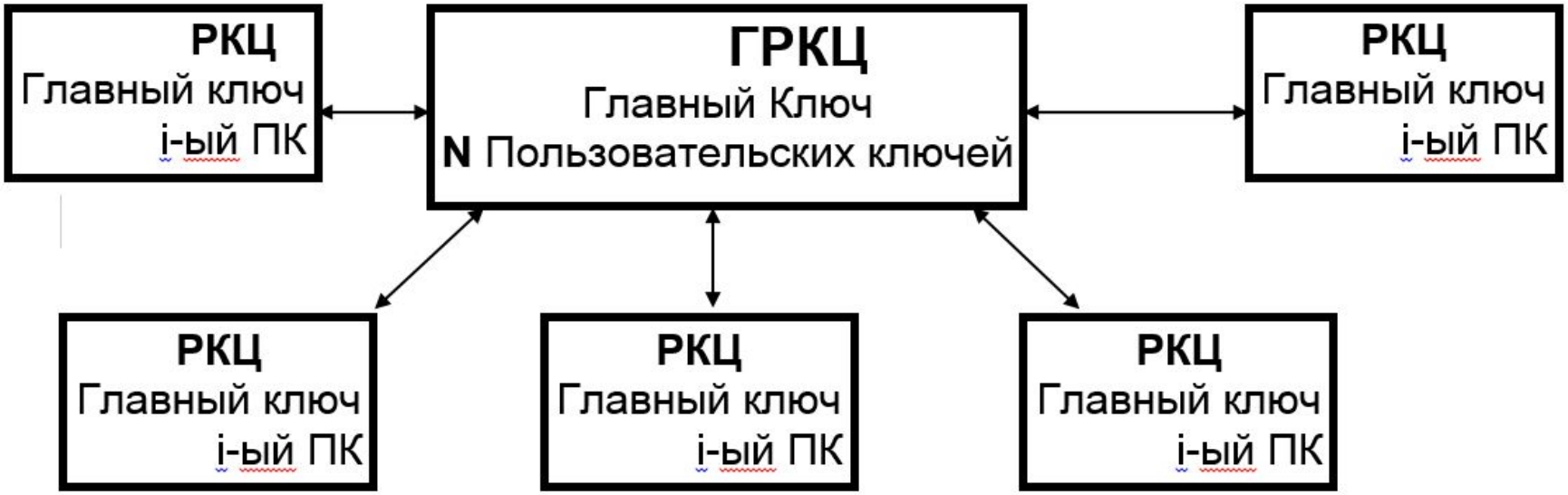


Схема «звезда»



Создание ключей при организации взаимодействия центрального офиса с филиалами при помощи криптоплат «Криптон»

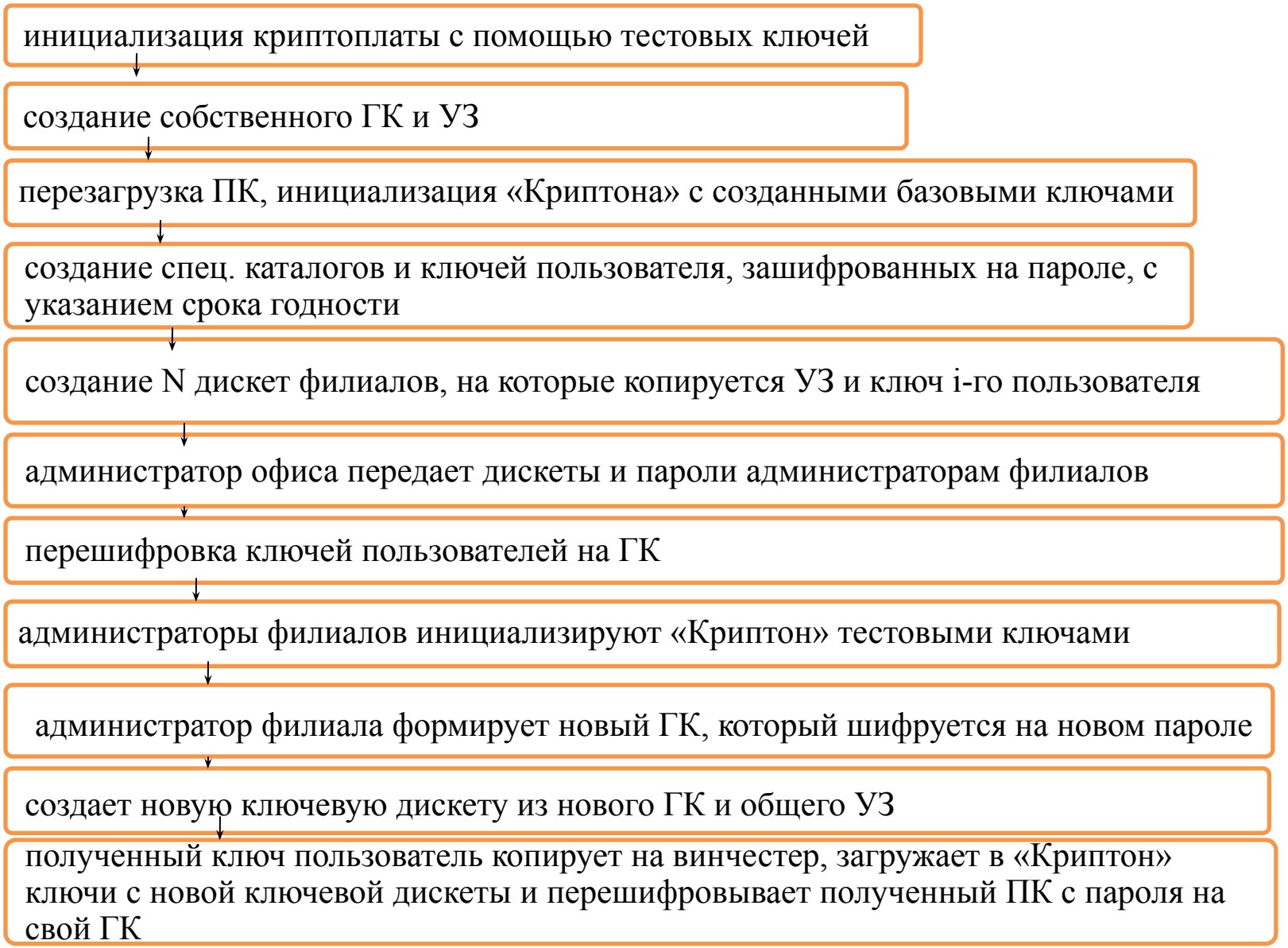
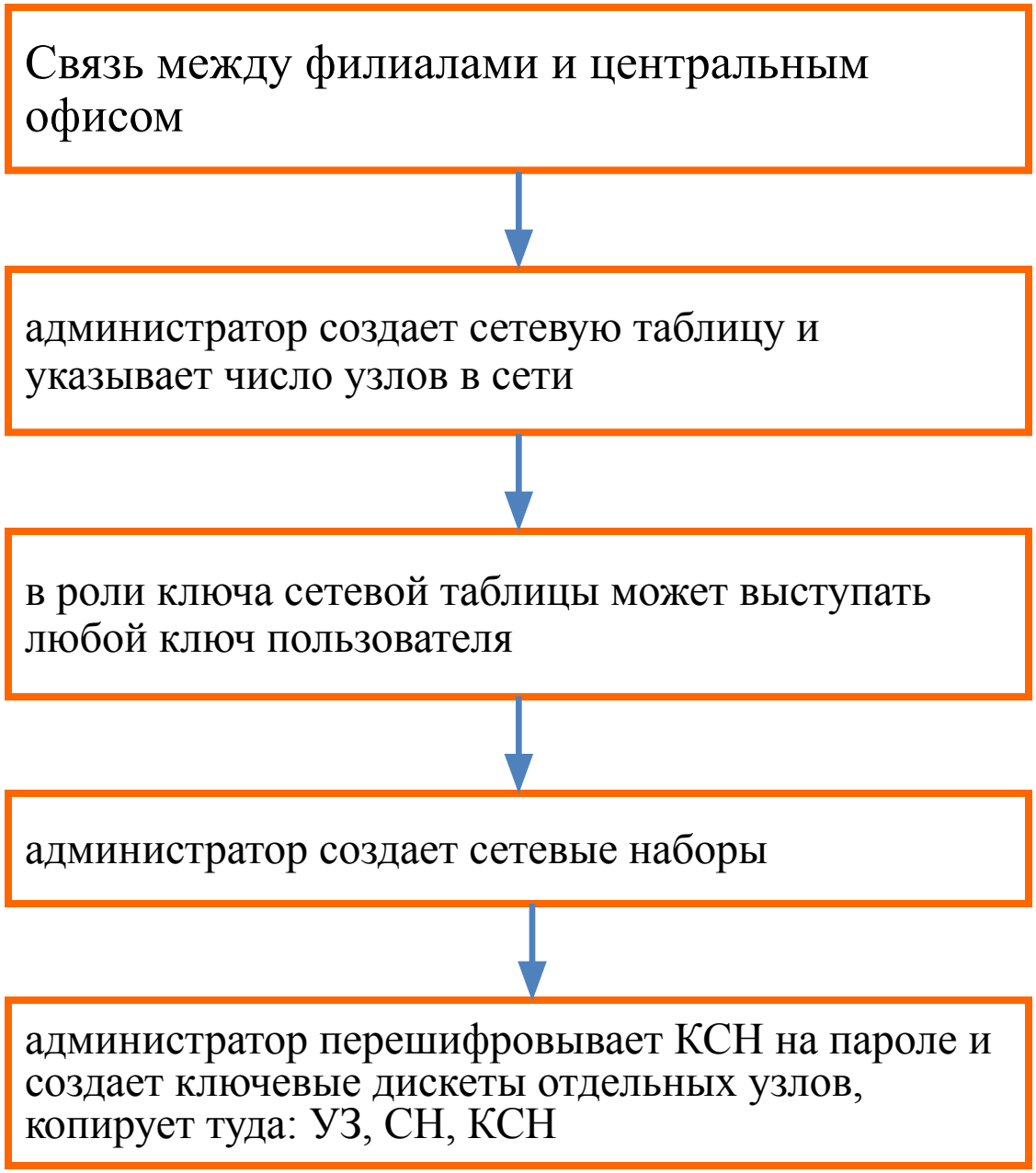


Схема «сеть»

№ РКЦ	ГРКЦ (1)	РКЦ1 (2)	РКЦ2 (3)	РКЦ3 (4)
ГРКЦ (1)	$К_{11}$	$К_{12}$	$К_{13}$	$К_{14}$
РКЦ1 (2)	$К_{21}$	$К_{22}$	$К_{23}$	$К_{24}$
РКЦ2 (3)	$К_{31}$	$К_{32}$	$К_{33}$	$К_{34}$
РКЦ3 (4)	$К_{41}$	$К_{42}$	$К_{43}$	$К_{44}$


Связь между филиалами и центральным офисом
администратор создает сетевую таблицу и указывает число узлов в сети
в роли ключа сетевой таблицы может выступать любой ключ пользователя
администратор создает сетевые наборы
администратор перешифровывает КСН на пароле и создает ключевые дискеты отдельных узлов, копирует туда: УЗ, СН, КСН

Особенности организации взаимодействия центрального офиса с филиалами при помощи криптоплат «Криптон»

- при большом числе компьютеров целесообразно использовать ключи пользователя
- при большом числе пользователей, взаимодействующих друг с другом, целесообразно использовать сетевые таблицы
- хранить УЗ и ГК на внешнем носителе
- остальные ключи хранить на винчестере, используя длинные пароли и не реже 1 раза в год , меняя сетевую систему.