Организация корпоративного защищенного почтового обмена при помощи почтового клиента DioPost-M (КС1, КС2, КС3)

Программное обеспечение DioPost-M является почтовым клиентом, предназначенным для обмена как конфиденциальной почтовой корреспонденцией (с использованием криптографических средств защиты информации), так и открытой почтовой корреспонденцией (не защищенной криптографическими методами) между пользователями почтовых систем. Для организации обмена защищенной корреспонденцией используется несимметричная ключевая схема (PKI). Услуги по предоставлению клиентам открытых и закрытых ключей выполняет удостоверяющий центр (УЦ) «Крипто-ПРО» или иной УЦ. Для генерации закрытых ключей и запросов к УЦ на выдачу сертификатов на стороне удаленных пользователей используется программное обеспечение «МГК-3» производства ООО «Фактор-ТС». Для хранения ключевой информации используется криптографический USB-токен (Rutoken, eToken), съемный USB-носитель и т. п. Для обеспечения классов защиты КС2, КС3 необходимо дополнительно использовать сертифицированные ФСБ средства защиты на рабочих станциях с установленным ПО DioPost-M. На рис. 3 изображена типовая схема реализации защищенного обмена с использованием ПО DioPost-M.

Необходимое оборудование и ПО	Назначение	Производитель
Почтовый клиент DioPost-M	Защищенный почтовый обмен	«Фактор-ТС»
Почтовый сервер	Пересылка сообщений	Любой
ПО МГК-4 (модуль генерации ключей)	Генерация запросов на сертификат	«Фактор-ТС»
Удостоверяющий центр (УЦ)	Управление инфраструктурой PKI	«Крипто-ПРО»
ПО оператора УЦ	Выписка сертификатов по запросу	«Крипто-ПРО»
Электронный токен («Рутокен»)	Хранение ключей и сертификатов	«Актив»
Планшет, ноутбук (Windows)	Установка ПО DioPost-M	Lenovo, Asus
Межсетевой экран (ФСБ МЭЗ)	Защита УЦ от внешних угроз	Любой
АПМДЗ (ФСБ) (для рабочих мест)	Для класса защищенности КС2, КС3	Setec, «Анкад»

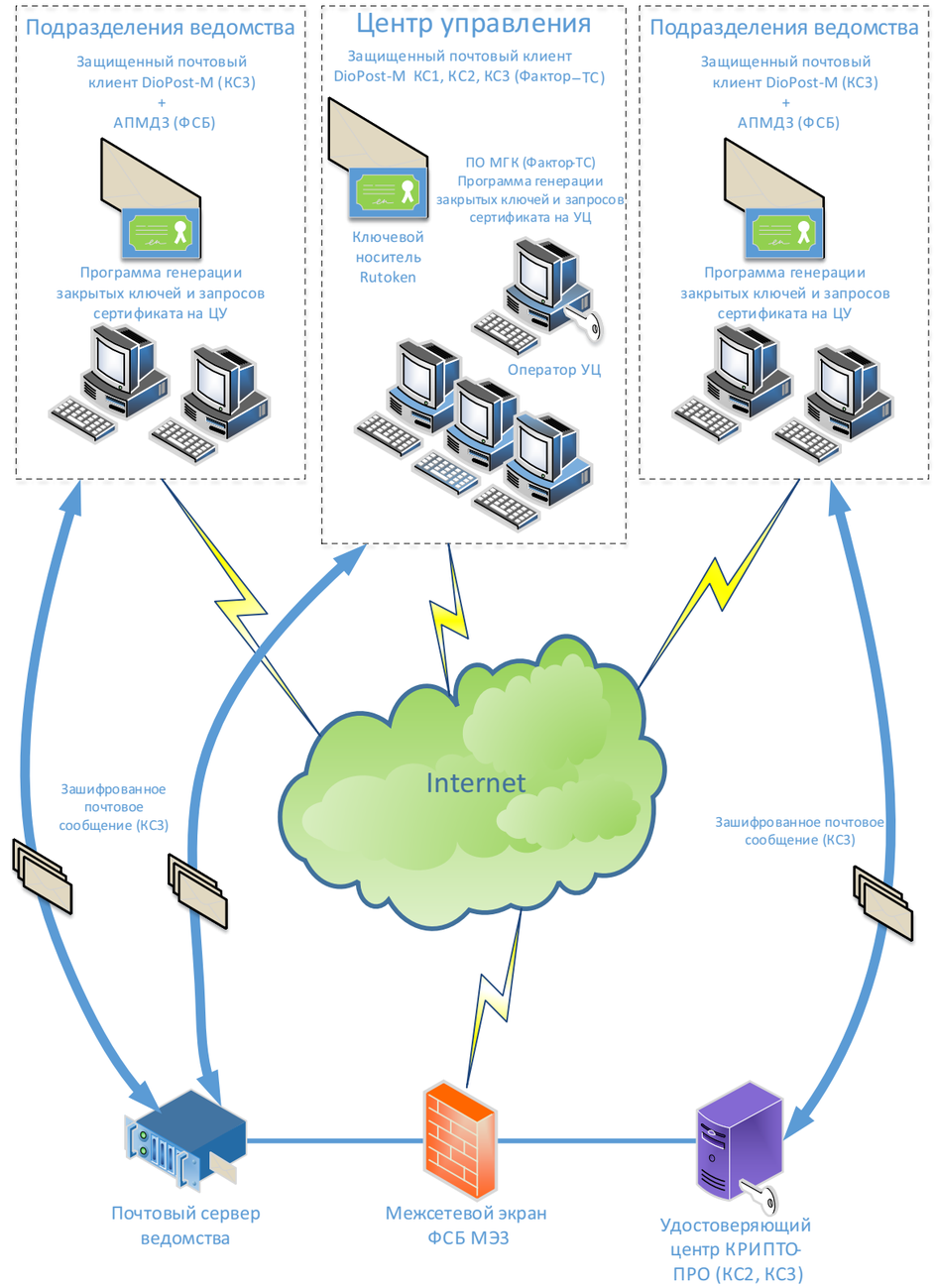

Рис. 7. Организация корпоративного защищенного почтового обмена при помощи почтового клиента DioPost-M (КС1, КС2, КС3)