Рекомендации по хранению и обращению с СИСТЕМНЫМ ИДЕНТИФИКАТОРОМ

1) Только уполномоченные сотрудники должны иметь доступ до СИСТЕМНОГО ИДЕНТИФИКАТОРА;
2) Должны быть приняты меры защиты СИСТЕМНОГО ИДЕНТИФИКАТОРА от разглашения третьим лицам и сотрудникам, в чьи служебные обязанности не входит работа с СИСТЕМНЫМ ИДЕНТИФИКАТОРОМ, при хранении и передаче СИСТЕМНОГО ИДЕНТИФИКАТОРА;
3) В зависимости от имеющихся рисков компрометации СИСТЕМНОГО ИДЕНТИФИКАТОРА, на периодической основе рекомендуется обновлять используемый СИСТЕМНЫЙ ИДЕНТИФИКАТОР, но не реже установленного срока жизни СИСТЕМНОГО ИДЕНТИФИКАТОРА;
4) Необходимо использовать СИСТЕМНЫЙ ИДЕНТИФИКАТОР, удовлетворяющий требованиям, указанным в ПАК. Не рекомендуется использовать в качестве СИСТЕМНОГО ИДЕНТИФИКАТОРА слова, содержащиеся в словарях и списках утекших паролей. Для наибольшего уровня безопасности рекомендуется использовать случайную величину в качестве СИСТЕМНОГО ИДЕНТИФИКАТОРА;
5) Не используйте одно и то же значение СИСТЕМНОГО ИДЕНТИФИКАТОРА повторно;
6) Не сохраняйте СИСТЕМНЫЙ ИДЕНТИФИКАТОР в логах приложений и устройств, через которые проходят запросы, содержащие системный идентификатор. Если возможность не сохранять СИСТЕМНЫЙ ИДЕНТИФИКАТОР в логах отсутствует, то необходимо применить к этим логам меры защиты, аналогичные применяемым для СИСТЕМНОГО ИДЕНТИФИКАТОРА;
7) Аутентификационные данные АДМИНИСТРАТОРА КЛЮЧЕЙ или АДМИНИСТРАТОРА ДП ID должны быть защищены от разглашения третьим лицам, т.к. с использованием этих аутентификационных данных зарегистрированный СИСТЕМНЫЙ ИДЕНТИФИКАТОР может быть изменен.