ПАМЯТКА
по эксплуатации средств криптографической защиты информации

1. Термины и сокращения:

УЦ	Аккредитованный удостоверяющий центр ГБУЗ «ЧОМИАЦ»
СКЗИ	Средство криптографической защиты информации, сертифицированное ФСБ России
Пользователь СКЗИ	Лицо, допущенное работе с СКЗИ
Спецпомещение	Помещение, в котором используются или хранятся СКЗИ, установочные диски СКЗИ, эксплуатационная и техническая документация к ним, носители ключевой информации
Криптографический ключ (криптоключ)	Совокупность данных, обеспечивающая выбор одного конкретного криптографического преобразования из числа всех возможных в данной криптографической системе
Ключевая информация	Специальным образом организованная совокупность криптоключей, предназначенная для осуществления криптографической защиты информации в течение определенного срока
Ключевой носитель	Физический носитель определенной структуры, предназначенный для размещения на нем ключевой информации
ЭП	Электронная подпись
Сертификат ЭП	Электронный документ, выданный УЦ и подтверждающий принадлежность ключа проверки ЭП владельцу сертификата ключа проверки ЭП

2. Обязанности пользователей СКЗИ

2.1. Хранить выданные СКЗИ, установочные диски СКЗИ, эксплуатационную и техническую документация к ним, ключевые носители в шкафах индивидуального пользования, оборудованных опечатывающими устройствами.

2.2. Вести журнал учета доступа к шкафу индивидуального пользования.

2.3. Не допускать компрометации ключевой информации. Под компрометацией понимается хищение, утрата, разглашение, несанкционированное копирование и другие действия, в результате которых ключевая информация может стать доступной посторонним лицам и (или) процессам.

2.4. Не допускать копирования информации с ключевых носителей или установочных дисков СКЗИ или записи какой-либо информации на ключевые носители или установочные диски СКЗИ.

2.5. Носители ключевой информации использовать только на своем рабочем месте.

2.6. Сообщать о ставших им известными попытках посторонних лиц получить сведения об используемых СКЗИ или ключевых носителях лицу, ответственному за обеспечение безопасности в информационных системах.

2.7. Проверять целостность пломб-наклеек на системных блоках, а при наличии признаков их вскрытия – уведомлять лицо, ответственное за обеспечение безопасности в информационных системах.

2.8. Немедленно уведомлять лицо, ответственное за обеспечение безопасности в информационных системах, о фактах утраты установочных дисков СКЗИ или документации к ним, носителей ЭП, ключей от помещений, ключей от шкафов индивидуального

пользования, личных печатей-пломбиров и о других фактах, которые могут привести к негативным последствиям для информационной безопасности.
2.9. При увольнении или отстранении от исполнения обязанностей, связанных с использованием СКЗИ, сдать установочные диски СКЗИ, документацию к ним, носители ключевой информации, ключи от помещений и шкафов индивидуального пользования.

3. Требования к Спецпомещениям

3.1. Спецпомещения должны иметь прочные входные двери с замками, гарантирующими надежное закрытие Спецпомещений в нерабочее время.
3.2. Окна Спецпомещений, расположенных на первых или последних этажах зданий, а также окна, находящиеся около пожарных лестниц и других мест, откуда возможно проникновение в Спецпомещения посторонних лиц, должны быть оборудованы металлическими решетками, или ставнями, или охранной сигнализацией, или другими средствами, препятствующими неконтролируемому проникновению в Спецпомещения.
3.3. Должна быть исключена возможность неконтролируемого проникновения или пребывания в Спецпомещениях посторонних лиц, а также просмотра посторонними лицами ведущихся там работ.
3.4. Двери Спецпомещений должны быть постоянно закрыты на замок и могут открываться только для санкционированного прохода сотрудников и посетителей.
3.5. Для предотвращения просмотра извне Спецпомещений их окна должны быть защищены жалюзи, шторами.
3.6. По окончании рабочего дня двери Спецпомещения и установленные в них шкафы индивидуального пользования должны быть заперты и опечатаны, а в журналы учета доступа внесены записи о закрытии.

4. Мероприятия при компрометации ключа электронной подписи

4.1. Пользователь обязан незамедлительно уведомить УЦ о компрометации ключа ЭП или подозрения на компрометацию.
4.2. При компрометации или подозрении на компрометацию пользователь направляет в УЦ заявление об аннулировании сертификата ЭП (приложение 7 к Регламенту работы УЦ).
4.3. В случае подтверждения факта компрометации ключа ЭП УЦ аннулирует сертификат ключа проверки ЭП с уведомлением владельца аннулированного сертификата.

5. Ответственность

5.1. Допущенные в Спецпомещения несут персональную ответственность за сохранность ключей от помещений и личных печатей-пломбиров, а также за допущение бесконтрольного нахождения в Спецпомещениях посторонних лиц.
5.2. Пользователи СКЗИ кроме ответственности, предусмотренной п. 5.1 настоящей памятки, также несут персональную ответственность за сохранность установочных дисков СКЗИ, документации к ним, ключевых носителей, ключей от шкафов индивидуального пользования.
5.3. Пользователи СКЗИ несут ответственность за несоблюдение обязанностей, перечисленных в п. 2 настоящей памятки.
5.4. Нарушение требований нормативных правовых документов Российской Федерации в области информационной безопасности предусматривает гражданско-правовую, административную и уголовную ответственность.