ДЕПАРТАМЕНТ КУЛЬТУРЫ ГОРОДА МОСКВЫ

ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ УЧРЕЖДЕНИЕ КУЛЬТУРЫ ГОРОДА МОСКВЫ «МОСКОВСКАЯ ГОСУДАРСТВЕННАЯ КАРТИННАЯ ГАЛЕРЕЯ НАРОДНОГО ХУДОЖНИКА СССР А.ШИЛОВА»

П Р И К А З

16 июня 2026 г. № 75

Об утверждении Инструкции по обращению со средствами криптографической защиты информации

В соответствии с требованиями Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных», Федерального закона от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации», а также нормативных актов в области криптографической защиты информации,

ПРИКАЗЫВАЮ:

1. Утвердить Инструкцию по обращению со средствами криптографической защиты информации согласно приложению № 1 к настоящему приказу.
2. Ведущему юрисконсульту довести настоящий приказ до сведения лиц в части, их касающейся.
3. Ведущему инженеру-электронику обеспечить размещение настоящего приказа на официальном сайте ГБУК г. Москвы «Галерея А. Шилова».
4. Контроль за исполнением настоящего приказа оставляю за собой.

Директор Ю.Г. Вохминцева

Приложение № 1
к приказу ГБУК г. Москвы «Галерея А. Шилова»
№ 75 от 16.06 2026 г.

ИНСТРУКЦИЯ
по обращению со средствами криптографической защиты информации

1. Общие положения

1.1. Инструкция в своем составе, терминах и определениях основывается на положениях Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи», Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну, утвержденной приказом ФАПСИ от 13.06.2001 № 152 (далее - Приказ № 152), Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (далее – Положение ПКЗ-2005), утвержденного приказом ФСБ РФ от 09.02.2005 № 66 (далее - Приказ №66), а также Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности, утвержденных приказом ФСБ от 10.07.2014 № 378.

1.2. Настоящая Инструкция разработана в целях регламентации действий лиц, допущенных к работе со средствами криптографической защиты информации (СКЗИ), которые осуществляют работы с применением СКЗИ.

1.3. Под работами с применением СКЗИ в настоящей Инструкции понимаются защищенное подключение к информационным системам, подписание электронных документов электронной подписью и проверка подписи, шифрование файлов другие действия согласно технической документации на СКЗИ.

1.4. Под обращением с СКЗИ в настоящей Инструкции понимается проведение мероприятий по обеспечению безопасности хранения, обработки и передачи по каналам связи с использованием СКЗИ информации ограниченного доступа.

1.5. Данная инструкция регламентирует работу с применением СКЗИ для защиты информации ограниченного доступа (включая персональные данные), не содержащей сведений, составляющих государственную тайну.

1.5. Термины и определения:

Информация ограниченного доступа – информация, доступ к которой ограничен федеральными законами;

Криптографический ключ (криптоключ) - совокупность данных, обеспечивающая выбор одного конкретного криптографического преобразования из числа всех возможных в данной криптографической системе.

Пользователи СКЗИ – работники Учреждения, непосредственно допущенные к работе с СКЗИ.

Средство криптографической защиты информации (СКЗИ) – совокупность аппаратных и(или) программных компонентов, предназначенных для подписания электронных документов и сообщений электронной подписью, шифрования этих документов при передаче по открытым каналам, защиты информации при передаче по каналам связи, защиты информации от несанкционированного доступа при ее обработке и хранении.

Компрометация – хищение, утрата, разглашение, несанкционированное копирование и другие происшествия, связанные с криптоключами и ключевыми носителями, в результате которых криптоключи могут стать доступными несанкционированным лицам и (или) процессам.

Ключевой документ - физический носитель определенной структуры, содержащий ключевую информацию (исходную ключевую информацию), а при необходимости - контрольную, служебную и технологическую информацию

Орган криптографической защиты (ОКЗ) – организация, разрабатывающая и осуществляющая мероприятия по организации и обеспечению безопасности хранения, обработки и передачи с использованием СКЗИ информации ограниченного доступа.

2. Порядок обращения со средствами криптографической защиты информации

2.1. Для получения допуска к работе с СКЗИ, работнику необходимо пройти обучение правилам работы с СКЗИ и проверку знаний в форме ознакомления с настоящей инструкцией, в том числе с Приказом № 152, Приказом № 66 и внесением их в Лист ознакомления по форме согласно Приложению №1 к настоящей Инструкции. Контроль над реализацией данных мероприятий возлагается на ответственное лицо - ведущего инженера–электроника (ответственное лицо за организацию работ по криптографической защите информации).

2.2. Пользователи СКЗИ обязаны:

2.2.1. не разглашать конфиденциальную информацию, к которой они допущены, рубежи ее защиты, в том числе сведения о криптоключах;

2.2.2. соблюдать требования к обеспечению безопасности конфиденциальной информации с использованием СКЗИ;

2.2.3. сообщать директору и ответственному лицу – ведущему инженеру–электронику о ставших им известными попытках посторонних лиц получить сведения об используемых СКЗИ или ключевых документах к ним;

2.2.4. сдать СКЗИ, эксплуатационную и техническую документацию к ним, ключевые документы, при увольнении или отстранении от исполнения обязанностей, связанных с использованием СКЗИ;

2.2.5. немедленно уведомлять директора и ответственное лицо - ведущего инженера–электроника о фактах утраты или недостачи СКЗИ, ключевых документов к ним, ключей от помещений, хранилищ, личных печатей и о других фактах, которые могут привести к разглашению защищаемых сведений конфиденциального характера, а также о причинах и условиях возможной утечки таких сведений.

2.3. Размещение и монтаж СКЗИ, а также другого оборудования, функционирующего с СКЗИ, должны свести к минимуму возможность неконтролируемого доступа посторонних лиц к указанным средствам. Техническое обслуживание такого оборудования и смена криптоключей осуществляются в отсутствие лиц, не допущенных к работе с данными СКЗИ. В обязательном порядке должны быть обеспечены условия хранения ключевых носителей, исключающие возможность доступа к ним посторонних лиц, несанкционированного использования или копирования ключевой информации.

2.4. Используемые или хранимые СКЗИ, эксплуатационная и техническая документация к ним, ключевые документы подлежат поэкземплярному учету в соответствии с журналом поэкземплярного учета средств криптографической защиты, эксплуатационной и технической документации к ним, ключевых документов (для обладателя конфиденциальной информации) по форме согласно приказу от 08.06.2026 № 69 «Об утверждении формы Журнала поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов поэкземплярного учета средств криптографической защиты, эксплуатационной и технической документации к ним, ключевых документов (для обладателя конфиденциальной информации)».

2.5. Для исключения утраты ключевой информации вследствие дефектов носителей рекомендуется, после получения ключевых носителей, создать рабочие копии. Копии должны быть промаркированы и должны использоваться, учитываться и храниться в общем порядке. Все копии учитываются за отдельным номером.

2.6. Намеченные к уничтожению (утилизации) СКЗИ подлежат изъятию из аппаратных средств, с которыми они функционировали. При этом СКЗИ считаются изъятыми из аппаратных средств, если исполнена предусмотренная эксплуатационной и технической документацией к СКЗИ процедура удаления программного обеспечения СКЗИ и они полностью отсоединены от аппаратных средств.

2.7. Пригодные для дальнейшего использования узлы и детали аппаратных средств общего назначения, не предназначенные специально для аппаратной реализации криптографических алгоритмов или иных функций СКЗИ, а также совместно работающее с СКЗИ оборудование (мониторы, принтеры, сканеры, клавиатура и т.п.) разрешается использовать после уничтожения СКЗИ без ограничений. При этом информация, которая может оставаться в устройствах памяти оборудования (например, в принтерах, сканерах), должна быть надежно удалена (стерта).

2.8. Ключевые документы должны быть уничтожены в сроки, указанные в эксплуатационной и технической документации к соответствующим СКЗИ. Если срок уничтожения эксплуатационной и технической документацией не установлен, то ключевые документы должны быть уничтожены не позднее 10 суток после вывода их из действия (окончания срока действия). Факт уничтожения оформляется в журнале поэкземплярного учета средств криптографической защиты, эксплуатационной и технической документации к ним, ключевых документов (для обладателя конфиденциальной информации).

2.11. Ключевые документы уничтожаются с оформлением акта по форме согласно приказу от 01.06.2026 № 65 «Об утверждении формы акта об уничтожении криптографических ключей, содержащихся на ключевых носителях и ключевых документов».

2.12. При обнаружении на рабочей станции с установленным СКЗИ программного обеспечения, не соответствующего объему и сложности решаемых задач на данном рабочем месте, а также вирусных программ, незамедлительно должны быть организованы работы по расследованию инцидента информационной безопасности.

3. Мероприятия при компрометации криптоключей

3.1. Под компрометацией криптоключей понимается:

3.1.1. хищение;

3.1.2. утрата носителей ключа;

3.1.3. утрата иных носителей ключа с последующим обнаружением;

3.1.4. возникновение подозрений на утечку ключевой информации или ее искажение;

3.1.5. нарушение целостности печатей на сейфах с носителями ключевой информации, если используется процедура, опечатывания сейфов;

3.1.6. утрата ключей от сейфов в момент нахождения в них носителей ключевой информации;

3.1.7. утрата ключей от сейфов в момент нахождения в них носителей ключевой информации с последующим обнаружением;

3.1.8. доступ посторонних лиц к ключевой информации;

3.1.9. другие события утери доверия к ключевой информации, согласно технической документации на СКЗИ.

3.2. В случае компрометации криптоключа пользователя незамедлительно должны быть приняты меры по отзыву криптоключа (отзыв ключа электронной подписи в удостоверяющем центре, обновление списков отозванных сертификатов, замена криптоключа пользователя и т.п.), а также проведено расследование по факту компрометации.

3.3. Криптоключи, в отношении которых возникло подозрение в компрометации, а также действующие совместно с ними другие криптоключи необходимо немедленно вывести из действия, если иной порядок не оговорен в эксплуатационной и технической документации к СКЗИ. О выводе криптоключей из действия необходимо сообщить директору и ответственному лицу - ведущему инженеру–электронику.

3.4. О нарушениях, которые могут привести к компрометации криптоключей, их составных частей или передававшейся (хранящейся) с их использованием конфиденциальной информации, пользователи СКЗИ обязаны сообщать ответственному лицу - ведущему инженеру–электронику.

3.5. Визуальный осмотр ключевых носителей многократного использования посторонними лицами не следует рассматривать как подозрение в компрометации криптоключей, если при этом исключалась возможность их копирования (чтения, размножения).

3.6. В случае компрометации криптоключей проводятся мероприятия по розыску и локализации последствий компрометации конфиденциальной информации, передававшейся (хранящейся) с использованием СКЗИ, а также осуществляется оповещение пользователей СКЗИ о предполагаемой компрометации криптоключей и необходимости их замены.

4. Права и обязанности ответственного лица за организацию работ по криптографической защите информации

4.1. При реализации мероприятий, связанных с обращением СКЗИ, ответственное лицо за организацию работ по криптографической защите информации должно руководствоваться действующим законодательством Российской Федерации, Приказом № 152, Приказом № 66, а также настоящей инструкцией.

4.2. Ведущий инженер–электроник (ответственное лицо за организацию работ по криптографической защите информации) обязан:

4.2.1. вести журнал поэкземплярного учета средств криптографической защиты, эксплуатационной и технической документации к ним, ключевых документов (для обладателя конфиденциальной информации);

4.2.2. вести лист ознакомления с настоящей инструкцией, Приказом № 152 и Приказом № 66;

4.2.3. обеспечить хранение установочных комплектов СКЗИ, эксплуатационной и технической документации к ним;

4.2.4. принимать ключевые документы СКЗИ от пользователя при его увольнении или отстранении от исполнения обязанностей, связанных с использованием СКЗИ;

4.2.5. проводить ежегодную проверку наличия СКЗИ, эксплуатационной и технической документации к ним, согласно журналу поэкземплярного учета средств криптографической защиты, эксплуатационной и технической документации к ним, ключевых документов (для обладателя конфиденциальной информации);

4.2.6. участвовать в мероприятиях по розыску и локализации последствий компрометации конфиденциальной информации;

4.2.7. не разглашать информацию ограниченного доступа, к которой он допущен, в том числе сведения о криптоключах;

4.2.8. обеспечить сохранность носителей ключевой информации и других документов о ключах, выдаваемых с ключевыми носителями;

4.2.9. контролировать целостность печатей (пломб) на технических средствах с установленными СКЗИ;

4.2.10. немедленно уведомлять непосредственного руководителя и директора о фактах компрометации криптоключей;

4.2.11. не допускать ввод одного номера лицензии на право использования СКЗИ более чем на одно рабочее место;

4.2.12. проводить (обеспечивать) плановую замену криптографических ключей не менее, чем за две недели до истечения срока действия ключевых документов;

4.2.13. принимать решение о дальнейших действиях с неиспользованными или выведенными из строя ключевыми документами, ключевыми носителями;

4.2.14. выявлять и устранять причины нештатного функционирования СКЗИ.

5. Ответственность лиц, допущенных к работе с СКЗИ

5.1. За нарушение установленных требований по эксплуатации криптосредств предусмотрена ответственность в соответствии с действующим законодательством Российской Федерации.

Приложение № 1
к Инструкции
по обращению со средствами
криптографической защиты информации, утв.
приказом от «___»_____ 20___ г. № _____

Лист ознакомления
с Инструкцией по обращению со средствами
криптографической защиты информации
(утверждена приказом от «___»_____ 20___ г. № _____)

№ п/п	ФИО	Должность	Подпись, дата