# Правила работы со средствами криптографической защиты информации для работников ГКУЗ «ККПБ им. В. Х. Кандинского»

## 1. Общие положения

Настоящая Инструкция разработана в целях регламентации действий лиц, допущенных к работе со средствами криптографической защиты информации (СКЗИ).

Функции органа криптографической защиты информации для проведения мероприятий по обеспечению безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации ограниченного доступа возложены на отдел АСУ ГКУЗ «ККПБ им. В. Х. Кандинского».

Инструкция в своем составе, терминах и определениях основывается на положениях «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 июня 2001 г. №152 (далее – Инструкция ФАПСИ от 13 июня 2001 г. №152) и «Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)», утвержденного приказом ФСБ РФ от 9 февраля 2005 г. N 66.

## 2. Термины и определения

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

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.

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

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

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.

Электронная подпись - информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию.

## 3. Работа с СКЗИ

Обладатели конфиденциальной информации, если они приняли решение о необходимости криптографической защиты такой информации или если решение о необходимости ее криптографической защиты принято государственными органами или государственными организациями, обязаны выполнять указания соответствующих органов криптографической защиты по всем вопросам организации и обеспечения

безопасности хранения, обработки и передачи по каналам связи с использованием СКЗИ конфиденциальной информации.

Размещение и монтаж СКЗИ, а также другого оборудования, функционирующего с СКЗИ, в помещениях пользователей 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. На время отсутствия пользователей СКЗИ указанное оборудование, при наличии технической возможности, должно быть выключено, отключено от линии связи и убрано в опечатываемые хранилища.

Используемые или хранимые СКЗИ, эксплуатационная и техническая документация к ним, ключевые документы подлежат поэкземплярному учету по установленным формам в соответствии с требованиями Положения ПКЗ-2005.

Непосредственно к работе с СКЗИ пользователи допускаются только после соответствующего обучения.

Обучение пользователей правилам работы с СКЗИ осуществляют сотрудники соответствующего органа криптографической защиты. Документом, подтверждающим должную специальную подготовку пользователей и возможность их допуска к самостоятельной работе с СКЗИ, является заключение, составленное комиссией соответствующего органа криптографической защиты на основании принятых от этих лиц зачетов по программе обучения.

Пользователи СКЗИ обязаны:

1. не разглашать конфиденциальную информацию, к которой они допущены, рубежи ее защиты, в том числе сведения о криптоключах;
2. соблюдать требования к обеспечению безопасности конфиденциальной информации с использованием СКЗИ;
3. сообщать в орган криптографической защиты о ставших им известными попытках посторонних лиц получить сведения об используемых СКЗИ или ключевых документах к ним;
4. сдать СКЗИ, эксплуатационную и техническую документацию к ним, ключевые документы в соответствии с порядком, установленным настоящей Инструкцией, при увольнении или отстранении от исполнения обязанностей, связанных с использованием СКЗИ;
5. немедленно уведомлять орган криптографической защиты 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.

Неиспользованные или выведенные из действия ключевые документы подлежат возвращению в орган криптографической защиты или по его указанию должны быть уничтожены на месте.

Уничтожение криптоключей (исходной ключевой информации) может производиться путем физического уничтожения ключевого носителя, на котором они расположены, или путем стирания (разрушения) криптоключей (исходной ключевой информации) без повреждения ключевого носителя (для обеспечения возможности его многократного использования).

Контроль за соблюдением правил пользования СКЗИ и условий их использования, указанных в правилах пользования на них, осуществляется:

1. обладателем, пользователем (потребителем) защищаемой информации, установившим режим защиты информации с применением СКЗИ;
2. собственником (владельцем) информационных ресурсов (информационных систем), в составе которых применяются СКЗИ;

3. ФСБ России в рамках контроля за организацией и функционированием криптографической и инженерно-технической безопасности информационно-телекоммуникационных систем, систем шифрованной, засекреченной и иных видов специальной связи.

**Перечень нормативных правовых документов, связанных с работой со средствами криптографической защиты информации (СКЗИ):**

1. Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 г. № 149-ФЗ
2. Федеральный закон «О персональных данных» от 27 июля 2006 г. № 152-ФЗ
3. Федеральный закон «Об электронной подписи» от 06.04.2011 № 63-ФЗ
4. «Инструкция 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» (утверждена Приказом ФАПСИ от 13.06.2001 № 152)
5. «Положение о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации» (Положение «ПКЗ-2005») (утверждено Приказом ФСБ от 9 февраля 2005г. № 66)
6. «Типовые требования по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных» (утверждены руководством 8 Центра ФСБ России 21 февраля 2008 г. № 149/6/6-622)
7. «Кодекс РФ об административных правонарушениях (КоАП РФ)» от 30.12.2001 № 195-ФЗ (Глава 13. Административные правонарушения в области связи и информации)
8. «Уголовный кодекс Российской Федерации» от 13.06.1996 № 63-ФЗ (Глава 28. Преступления в сфере компьютерной информации)
9. «Трудовой кодекс Российской Федерации» от 30.12.2001 № 197-ФЗ (Глава 14. Защита персональных данных работника)
10. Эксплуатационная и техническая документация к СКЗИ "КриптоПро CSP"