УТВЕРЖДЕНО

приказом ГБУ Республики Коми «ЦБИ»

от «04» апреля 2014 года №25/ОД

**ИНСТРУКЦИЯ**

**пользователей средств криптографической защиты информации**

1. **Общие положения**

Настоящая Инструкция разработана в целях регламентации действий пользователей, допущенных к работе со средствами криптографической защиты информации (СКЗИ) в организациях, которые осуществляют работы с применением СКЗИ (далее – Организация).

Под Организацией в настоящей Инструкции понимаются органы государственной власти Республики Коми, подведомственные им организации, органы местного самоуправления Республики Коми, подведомственные им организации.

Под работами с применением СКЗИ в настоящей Инструкции понимаются защищенное подключение к информационным системам, подписание электронных документов электронной подписью и проверка подписи, шифрование файлов и т.д.

СКЗИ должны использоваться для защиты информации ограниченного доступа (включая персональные данные), не содержащей сведений, составляющих государственную тайну.

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 Государственное бюджетное учреждение Республики Коми "Центр безопасности информации". Данные мероприятия выполняются в соответствии с Постановлением Правительства Республики Коми от 31 декабря 2010 г. N 506 «О региональном операторе безопасности инфраструктуры электронного правительства в Республике Коми» и на основании Лицензии ФСБ России на осуществление деятельности по предоставлению услуг в области шифрования информации.

Настоящая 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.

1. **Термины и определения**

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

Исходная ключевая информация - совокупность данных, предназначенных для выработки по определенным правилам криптоключей;

Ключевая информация - специальным образом организованная совокупность криптоключей, предназначенная для осуществления криптографической защиты информации в течение определенного срока;

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

Ключевой носитель - физический носитель определенной структуры, предназначенный для размещения на нем ключевой информации (исходной ключевой информации).

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.

Персональный компьютер (ПК) - вычислительная машина, предназначенная для эксплуатации пользователем Организации в рамках исполнения должностных обязанностей.

Пользователи СКЗИ – работники Организации, 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.

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.

1. **Порядок получения допуска пользователей к работе с СКЗИ**

Для работы с СКЗИ привлекаются физические лица, назначенные соответствующим приказом руководителя организации (включенные в перечень пользователей СКЗИ). Основанием для включения в перечень является Заключение о допуске к самостоятельной работе с СКЗИ.

Решение о готовности пользователя к самостоятельной работе с СКЗИ принимает комиссия органа криптографической защиты ГБУ Республики Коми «ЦБИ» на основании результатов принятого у пользователя зачета.

Для того чтобы получить Заключение о допуске к самостоятельной работе с СКЗИ, пользователю необходимо выполнить следующее:

1. Самостоятельно ознакомиться с положениями
   * 1. Федерального закона «Об электронной подписи» № 63-ФЗ от 06.04.2011;
     2. Приказа «об утверждении 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» N 152 от 13.06.2001;
     3. Данной инструкции.
2. Зарегистрироваться на официальном сайте ГБУ Республики Коми «ЦБИ» <http://www.cbikomi.ru/>
3. Пройти тестирование на знание правил работы с СКЗИ. Модуль тестирования находится на вкладке «Удостоверяющий центр» на сайте ГБУ Республики Коми «ЦБИ» или доступен по следующей ссылке: <http://www.cbikomi.ru/test/test_na_znaniya_pravil_raboty_so_skzi_kriptopro_csp_vipnet>
4. При успешном прохождении тестирования пользователь получит по электронной почте бланк Заключения о допуске пользователя к самостоятельной работе с СКЗИ. Необходимо распечатать бланк в двух экземплярах, подписать, скрепить оттиском печати Организации и направить оба экземпляра в ГБУ Республики Коми "ЦБИ" по адресу 167000, г. Сыктывкар, ул. Интернациональная, д. 108, оф. 227. Если в организации тестирование проходят сразу несколько пользователей, то отправку Заключений рекомендуется проводить централизованно через Ответственного за организацию работ по криптографической защите информации.
5. **Обязанности пользователей СКЗИ**

Пользователи СКЗИ обязаны

1. не разглашать информацию ограниченного доступа, к которой они допущены, в том числе сведения о криптоключах;
2. сохранять носители ключевой информации и другие документы о ключах, выдаваемых с ключевыми носителями;
3. соблюдать требования к обеспечению с использованием СКЗИ безопасности информации ограниченного доступа;
4. сообщать в ОКЗ о ставших им известными попытках посторонних лиц получить сведения об используемых СКЗИ или ключевых документах к ним;
5. сдать СКЗИ, эксплуатационную и техническую документацию к ним, ключевые документы при увольнении или отстранении от исполнения обязанностей, связанных с использованием СКЗИ;
6. немедленно уведомлять ОКЗ 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.

Пользователь несет ответственность за то, чтобы на ПК, на котором установлены СКЗИ, не были установлены и не эксплуатировались программы (в том числе, программы-вирусы), которые могут нарушить функционирование СКЗИ. На ПК, оборудованном СКЗИ, программное обеспечение должно быть лицензионным.

При обнаружении на ПК, оборудованном СКЗИ, посторонних программ или вирусов, работа с СКЗИ на данном рабочем месте должна быть прекращена. Незамедлительно организуются мероприятия по анализу и ликвидации негативных последствий данного нарушения.

Все полученные обладателем информации ограниченного доступа экземпляры СКЗИ, эксплуатационной и технической документации к ним, ключевых документов должны быть выданы под расписку в соответствующем журнале поэкземплярного учета пользователям СКЗИ, несущим персональную ответственность за их сохранность.

**Не допускается**

1. разглашать информацию ограниченного доступа, к которой был допущен Пользователь СКЗИ;
2. разглашать содержимое ключевых носителей или передавать сами носители лицам, к ним не допущенным;
3. выводить ключевую информацию на дисплей и(или) принтер;
4. вставлять ключевой носитель в порт ПК при проведении работ, не являющихся штатными процедурами использования ключей (шифрование/расшифровывание информации, проверка электронной цифровой подписи и т.д.), а также в порты других ПК;
5. записывать на ключевом носителе постороннюю информацию;
6. вносить какие-либо изменения в программное обеспечение СКЗИ;
7. использовать бывшие в работе ключевые носители для записи новой информации без предварительного уничтожения на них ключевой информации путем переформатирования (рекомендуется физическое уничтожение носителей).

О нарушениях, которые могут привести к компрометации криптоключей, их составных частей или передававшейся (хранящейся) с их использованием информации ограниченного доступа, пользователи СКЗИ обязаны сообщать Ответственному за организацию работ по криптографической защите информации.

1. **Ответственность пользователей СКЗИ**

Пользователи СКЗИ отвечают за исполнение своих функциональных обязанностей и сохранность информации ограниченного доступа, которая стала ему известной вследствие исполнения им своих служебных обязанностей.

Ответственность лиц, допущенных к работе с СКЗИ, за неисполнение и/или ненадлежащее исполнение своих обязанностей, предусмотренных соответствующими инструкциями (Инструкция по обращению с СКЗИ, Инструкция пользователя СКЗИ), а также за разглашение информации ограниченного доступа, ставшей ему известной вследствие исполнения им своих служебных обязанностей, определяется действующим законодательством Российской Федерации и условиями трудового договора.

1. **Заключительные положения**

Контактная информация Государственного бюджетного учреждения Республики Коми "Центр безопасности информации":

**Адрес**: 167000, г. Сыктывкар, ул. Интернациональная, д. 108, оф. 227.

**Телефон:** (8212) 301-211

**Сайт**: [http://www.cbikomi.ru](http://www.cbikomi.ru/test/test_na_znaniya_pravil_raboty_so_skzi_kriptopro_csp_vipnet)