Приложение 2 к приказу
от 18 марта 2019 года № 51

ИНСТРУКЦИЯ
по обращению со средствами криптографической защиты информации

1. Общие положения

Настоящая Инструкция разработана в целях регламентации действий лиц, допущенных к работе со средствами криптографической защиты информации (далее – СКЗИ) в ГУК ТО «ОЦРИНКиТ» (далее – Организация).

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.

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

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

Функции по проведению мероприятий по обеспечению безопасности хранения, обработки и передачи по каналам связи с использованием СКЗИ информации ограниченного доступа осуществляют пользователи СКЗИ.

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), «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, «Типовыми требованиями 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», утвержденными руководством 8 Центра ФСБ России 21 февраля 2008 г. №149/6/6–622.

2. 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;

Персональный компьютер (далее – 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 – 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

Размещение и монтаж СКЗИ, а также другого оборудования, функционирующего со СКЗИ, в помещениях пользователей СКЗИ сводит 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. В противном случае, в организации обеспечиваются условия хранения ключевых носителей, исключающие возможность доступа к ним посторонних лиц, несанкционированного использования и/или копирования ключевой информации.

Для исключения утраты ключевой информации вследствие дефектов носителей рекомендуется, после получения ключевых носителей, создать рабочие копии. Копии должны быть соответствующим образом маркированы и должны использоваться, учитываться и храниться так же, как оригиналы.

Единицей поэкземплярного учета ключевых документов считается ключевой носитель многократного использования. Если один и тот же ключевой носитель многократно используют для записи криптоключей, то его каждый раз следует регистрировать отдельно.

Передача СКЗИ, эксплуатационной и технической документации к ним, ключевых документов допускается только между пользователями СКЗИ под расписку в соответствующих журналах поэкземплярного учета.

При обнаружении на рабочем месте, оборудованном СКЗИ, посторонних программ или вирусов, нарушающих работу указанных средств, работа со СКЗИ на данном рабочем месте прекращается и организуется проведение мероприятий по анализу и ликвидации негативных последствий данного происшествия.

4. Действия в случае компрометации ключей

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.

К компрометации ключей относятся следующие события:

1) утрата носителей ключа;
2) утрата иных носителей ключа с последующим обнаружением;
3) увольнение сотрудников, имевших доступ к ключевой информации;
4) возникновение подозрений на утечку информации или ее искажение;
5) доступ посторонних лиц к ключевой информации;
6) другие события утери доверия к ключевой документации.

Криптоключи, в отношении которых возникло подозрение в компрометации, а также действующие совместно с ними другие криптоключи необходимо немедленно вывести из действия.

Осмотр ключевых носителей многократного использования посторонними лицами не следует рассматривать как подозрение в

компрометации криптоключей, если при этом исключалась возможность их чтения и/или копирования. В случаях недостачи, не предъявления ключевых документов, а также неопределенности их местонахождения принимаются срочные меры к их розыску.

Мероприятия по розыску и локализации последствий компрометации информации ограниченного доступа, передававшейся (хранящейся) с использованием СКЗИ, организует и осуществляет Ответственный за организацию работ по криптографической защите информации в Организации.

5. Обязанности и ответственность лиц, допущенных к работе с СКЗИ

Лица, допущенные к работе с 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 безопасности информации ограниченного доступа;

4) Сообщать Ответственному о ставших ему известными попытках посторонних лиц получить сведения об используемых СКЗИ или ключевых документах к ним;

5) Немедленно уведомлять Ответственного о фактах утраты или недостачи СКЗИ, ключевых документов к ним и о других фактах, которые могут привести к разглашению защищаемых сведений конфиденциального характера, а также о причинах и условиях возможной утечки таких сведений;

6) В случае необходимости производить уничтожение криптоключей и ключевых документов в соответствии с требованиями пунктов 41-46 Инструкции ФАПСИ от 13 июня 2001 г. №152;

7) Не вводить номера лицензий на СКЗИ, уже вводимые на других АРМ.

Лица, допущенные к работе с 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 со СКЗИ, за неисполнение и (или) ненадлежащее исполнение своих обязанностей, предусмотренных соответствующими инструкциями (Инструкция ответственного за организацию работ по криптографической защите информации, 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.