Приложение
к приказу МБОУ «ЦО №32»
от «20» апреля 2023 г. № 31-бз

ИНСТРУКЦИЯ

ответственного за организацию работ по криптографической защите информации

1. Общие положения

Настоящая Инструкция разработана в целях регламентации действий лиц, ответственных за организацию работ по криптографической защите информации (далее – Ответственный) в МБОУ «ЦО №32» (далее-Центр) в связи с осуществлением работ с применением средств криптографической защиты информации (далее – СКЗИ).

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.

Ответственный назначается приказом директора Центра из числа его работников.

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

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. №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 Центра в рамках исполнения должностных обязанностей;

Пользователи СКЗИ – работники Центра, 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. Порядок получения допуска пользователей к работе с СКЗИ

Для работы пользователей с СКЗИ в Центре необходимо реализовать ряд мероприятий:

1) Пользователям, которым необходимо получить доступ к работе с СКЗИ, пройти обучение правилам работы с СКЗИ и тестирование на знание этих правил;
2) Издать Приказ об утверждении перечня пользователей СКЗИ;
3) Утвердить Инструкцию по обращению с СКЗИ;
4) Ознакомить всех пользователей СКЗИ с Инструкцией по обращению с СКЗИ под роспись;

Контроль над реализацией данных мероприятий возлагается на Ответственного.

4. Обязанности Ответственного

При решении всех вопросов, связанных с обеспечением в Организации безопасности хранения, обработки и передачи по каналам связи с использованием СКЗИ информации ограниченного доступа, Ответственный должен руководствоваться Инструкцией по обращению с СКЗИ, которая утверждается Приказом об обращении с СКЗИ.

На Ответственного возлагается проведение следующих мероприятий:

1) Вести Журнал поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов;
2) Вести учет актов об установке и настройке СЗИ;
3) Вести учет лицензий на право использования СКЗИ и соответствующих им Актов приема-передачи;
4) Принять СКЗИ, эксплуатационную и техническую документацию к ним, ключевые документы от пользователя при его увольнении или отстранении от исполнения обязанностей, связанных с использованием СКЗИ;

5) Осуществлять ежегодную проверку журнала учета СКЗИ, перечня пользователей СКЗИ и иных документов;

6) Сообщать директору Центра (заместителю директора по безопасности) о ставших ему известными попытках посторонних лиц получить сведения об используемых СКЗИ или ключевых документах к ним.

Ответственный обязан:

1) Не разглашать информацию ограниченного доступа, к которой он допущен, 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) Контролировать целостность печатей (пломб) на технических средствах с установленными СКЗИ;

5) Немедленно уведомлять директора Центра о фактах утраты или недостачи СКЗИ, ключевых документов к ним, ключей от помещений, хранилищ, личных печатей и о других фактах компрометации криптоключей, которые могут привести к разглашению информации ограниченного доступа, а также о причинах и условиях возможной утечки такой информации;

6) Незамедлительно принимать меры по локализации последствий компрометации защищаемых сведений конфиденциального характера;

7) Не допускать ввод одного номера лицензии на право использования СКЗИ более чем на одно рабочее место.

5. Права Ответственного

В рамках исполнения возложенных на него обязанностей, Ответственный имеет право:

1) Требовать от пользователей СКЗИ соблюдения положений Инструкции по обращению с СКЗИ;

2) Обращаться к директору Центра с требованием прекращения работы пользователя с СКЗИ при невыполнении им установленных требований по обращению с СКЗИ;

3) Инициировать проведение служебных расследований по фактам нарушения в Центра порядка обеспечения безопасности хранения, обработки и передачи по каналам связи с использованием СКЗИ информации ограниченного доступа.

6. Порядок передачи обязанностей при смене Ответственного

При смене Ответственного должны быть внесены соответствующие изменения в Приказ об обращении с СКЗИ. Вновь назначенный Ответственный должен быть ознакомлен под роспись с настоящей Инструкцией и приступить к исполнению возложенных на него обязанностей.