УТВЕРЖДАЮ
Директор
ГБПОУ РК «РКИГ»
_____ Пальчук М. И.
Приказ № 38 от 09.03.2023 г.

Инструкция ответственного за обеспечение функционирования и безопасности криптосредств в информационной системе персональных данных обмена информацией с ИСПДн центра обработки данных ФГБУ ФЦТ

1 Общие положения

Настоящая Инструкция разработана в целях регламентации действий лиц, ответственных за обеспечение функционирования и безопасности криптосредств (далее - Ответственный) в информационной системе персональных данных обмена информацией с ИСПДн центра обработки данных ФГБУ ФЦТ (далее - ИСПДн ОИ ФЦТ).

Ответственный назначается приказом директора ГБПОУРК «РКИГ» из числа пользователей криптосредств, или возлагается на структурное подразделение или должностное лицо (работника), ответственных за защиту информации и (или) обеспечение безопасности персональных данных.

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).

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

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.

3 Порядок получения допуска пользователей к работе с СКЗИ

Для работы пользователей с СКЗИ в ИСПДн ОИ ФЦТ необходимо реализовать ряд мероприятий:

Пользователи, которым необходимо получить доступ к работе с СКЗИ, должны быть проинструктированы и обучены правилам работы с СКЗИ;

Учёт лиц, допущенных к работе с криптосредствами, предназначенными для обеспечения защиты информации в ИСПДн ОИ ФЦТ, осуществлять в Перечне пользователей СКЗИ;

Контроль над реализацией данных мероприятий возлагается на Ответственного за обеспечение функционирования и безопасности криптосредств.

4 Обязанности Ответственного

При решении всех вопросов, связанных с обеспечением безопасности хранения, обработки и передачи по каналам связи с использованием СКЗИ информации ограниченного доступа, Ответственный должен руководствоваться Инструкцией по обращению с СКЗИ в ИСПДн ОИ ФЦТ.

На Ответственного возлагается проведение следующих мероприятий:

- ведение Журнал поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов;

- принятие СКЗИ, эксплуатационной и технической документации к ним, ключевых документов от пользователя при его увольнении или отстранении от исполнения обязанностей, связанных с использованием СКЗИ;

- осуществление периодической проверки журнала учета СКЗИ, перечня пользователей СКЗИ и иных документов.

Ответственный обязан:

- не разглашать информацию ограниченного доступа, к которой он допущен, в том числе сведения о криптоключах;
- сохранять носители ключевой информации и другие документы о ключах, выдаваемых с ключевыми носителями;
- соблюдать требования к обеспечению с использованием СКЗИ безопасности информации ограниченного доступа;
- контролировать целостность печатей (пломб) на технических средствах с установленными СКЗИ;
- немедленно уведомлять руководителя Учреждения 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;
- незамедлительно принимать меры по локализации последствий компрометации защищаемых сведений конфиденциального характера;
- 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:

- требовать от пользователей СКЗИ соблюдения положений Инструкции по обращению с СКЗИ и Инструкции пользователя СКЗИ;
- обращаться к руководителю Учреждения с требованием прекращения работы пользователя с СКЗИ при невыполнении им установленных требований по обращению с СКЗИ;
- инициировать проведение служебных расследований по фактам нарушения в Учреждении 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.

Ведущий специалист по защите информации А. О. Грибенников