Подписано цифровой подписью: Пальчук М.И.
DN: cn=Пальчук М.И., o=ГБПОУ РК "Романовский колледж индустрии гостеприимства", ou=Директор, email=043@crimeaedu.ru, c=RU
Дата: 2023.05.16 09:58:09 +03'00'

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

ИНСТРУКЦИЯ
пользователей средств криптографической защиты информации в информационной системе персональных данных обмена информацией с ИСПДн центра обработки данных ФГБУ ФЦТ

1 Общие положения

Настоящая Инструкция разработана в целях регламентации действий пользователей, допущенных к работе со средствами криптографической защиты информации (далее - СКЗИ) в информационной системе персональных данных обмена информацией с ИСПДн центра обработки данных ФГБУ ФЦТ (далее - ИСПДн ОИ ФЦТ).

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.

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.

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;

Пользователи СКЗИ - работники организации или 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.

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 с СКЗИ привлекаются физические лица, включенные в перечень пользователей СКЗИ, утвержденного соответствующим приказом руководителя организации. Основанием для включения в перечень является Заключение о допуске к самостоятельной работе с СКЗИ. Решение о готовности пользователя к самостоятельной работе с СКЗИ принимает Ответственный за обеспечение функционирования и безопасности криптосредств 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:

Федерального закона «Об электронной подписи» № 63-ФЗ от 06.04.2011; Приказа ФАПСИ N 152 от 13.06.2001 «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»;

Настоящей инструкции;

Инструкцией о порядке применения средств межсетевого экранирования;

Инструкцией по обращению со средствами криптографической защиты информации;

Эксплуатационной документацией на СКЗИ;

2) Пройти зачет на знание правил работы с СКЗИ.

3) При успешном прохождении тестирования, Ответственным за обеспечение функционирования и безопасности криптосредств оформляется Заключение о допуске пользователя к самостоятельной работе с СКЗИ, которое утверждается руководителем организации.

4) 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 Ответственному за функционирование и обеспечение безопасности криптосредств 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 Ответственного за функционирование и обеспечение безопасности криптосредств 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 и организованы 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 функционирование и обеспечение безопасности криптосредств.

5 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.

Ведущий специалист по защите информации А. О. Грибенников