Утверждено
И.о. директора ГБОУ СОШ №1 «ОЦ»
им. В.И. Фокина с. Большая Глушица
_____ Соколова О.А.
«01» сентября 2021 г.

ЭП

C=RU, O="ГБОУ СОШ №1 ""ОЦ"" им. В.И. Фокина с. Большая Глушица", CN=И.о. директора школы Соколова Ольга Александровна, E=shool1_bgl@samara.edu.ru
00a5938c76835cedd6
2021.11.26 19:22:31+04'00'

Инструкция
пользователя средств криптографической защиты информации
ГБОУ СОШ №1 «ОЦ» им. В.И. Фокина с. Большая Глушица

Данная инструкция разработана для практического применения пользователем средств криптографической информации «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 РФ от 13.06.2001 №152.

1. Термины и определения

Средства криптографической защиты конфиденциальной информации, сертифицированные ФСБ, именуются – СКЗИ. К СКЗИ относятся криптографические
алгоритмы преобразования информации, программные средства, обеспечивающие безопасность информации при ее обработке, хранении и передаче по каналам связи включая СКЗИ, защиту от несанкционированного доступа к информации и навязывания ложной информации, включая средства имитозащиты и «электронной подписи».

Пользователи СКЗИ–физические и юридические лица, непосредственно допущенные к работе с СКЗИ.

Криптографический ключ (криптоключ) – совокупность данных, обеспечивающая
выбор одного конкретного криптографического преобразования из числа всех возможных в данной криптографической системе.

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

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

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

Компрометация криптоключей – хищение, утрата, разглашение, несанкционированное копирование и другие происшествия, в результате которых криптоключи могут стать доступными несанкционированным лицам и (или) процессам.

2. Обязанности пользователя

Пользователи средств криптографической защиты обязаны:
- не разглашать конфиденциальную информацию, к которой они допущены;
- соблюдать требования по обеспечению безопасности конфиденциальной информации с использованием СКЗИ;
- выполнять инструкции пользователя СКЗИ;
- своевременно сообщать в ответственному пользователю СКЗИ о нарушениях порядка использования и хранения СКЗИ и ключевых носителей;
- сдать СКЗИ, эксплуатационную и техническую документацию к ним, ключевые документы и ключевые носители при увольнении или отстранении от исполнения обязанностей, связанных с использованием СКЗИ.
- немедленно уведомлять ответственного пользователя СКЗИ о фактах утраты или недостачи СКЗИ, ключевых документов к ним, ключевых носителей, 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.

3. Допуск и работа с СКЗИ

Непосредственно к работе с СКЗИ пользователи допускаются только после соответствующего обучения. Документом, подтверждающим должную специальную подготовку пользователей и возможность их допуска к самостоятельной работе с СКЗИ, является заключение, составленное комиссией на основании принятых от этих лиц зачетов по программе обучения.

4. Учет, выдача и уничтожение СКЗИ и ключевых носителей

4.1. Все СКЗИ и ключевые носители передаются пользователю СКЗИ с отметкой в соответствующих журналах и в его лицевом счете, в котором указывается тип и регистрационный номер экземпляра СКЗИ или ключевого носителя, нанесенный на корпус единицы поэкземплярного учета. Вместе с СКЗИ выдаются Правила их использования.

4.2. Ключевые документы для работы с СКЗИ изготавливаются и выдаются пользователю СКЗИ в его присутствии. При этом изготавливаются два экземпляра секретного ключа (основной и дубликат) на двух дискетах, сертификат ключа (содержит открытый ключ и прочую удостоверяющую информацию о владельце) на одной дискете, а также два бумажных экземпляра сертификата ключа. Основной секретный ключ хранится у пользователя СКЗИ. Дубликат секретного ключа передается на хранение ответственному пользователю СКЗИ. Сертификаты должны быть заверены подписями пользователя СКЗИ и скреплены печатью. Один экземпляр
сертификата ключа в организации пользователя СКЗИ, второй экземпляр сертификата передается лицензиату ФСБ, осуществляющему электронный документооборот с владельцем ключевого документа.

4.3. Поэкземплярный учет СКЗИ и ключевых носителей, ведется в соответствующем журнале поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов и журнале техническом (аппаратном), которые ведет ответственный пользователь СКЗИ.

4.4. Учет СКЗИ, эксплуатационной и технической документации, ключевых документов должен быть организован на бумажных носителях и в электронном виде. СКЗИ необходимо учитывать поэкземплярно. Единицей поэкземплярного учета СКЗИ считается инсталлирующая дискета или компакт диск (CD-ROM).

4.5. Неиспользованные или выведенные из действия ключевые документы подлежат возвращению ответственному пользователю СКЗИ. Уничтожение криптографических ключей пользователя СКЗИ производится с отметкой в журнале поэкземплярного учета СКЗИ или с составлением соответствующего акта, если уничтожается большое количество ключей.

4.6. Криптографические ключи, в отношении которых возникло подозрение в компрометации, а также действующие совместно с ними другие криптографические ключи необходимо немедленно вывести из действия, если иной порядок не оговорен в эксплуатационной и технической документации к СКЗИ.

5. Действия при компрометации ключевой информации

5.1. В случае подозрения на компрометацию секретного ключа пользователь СКЗИ обязан уведомить ответственного пользователя СКЗИ о данном факте. Учитывая обстоятельства факта компрометации секретного ключа, ответственный пользователь
СКЗИ принимает решение о кратковременном продолжении использования секретного ключа или вывода его из эксплуатации и сообщает об этом пользователю СКЗИ.

5.2. Пользователь СКЗИ после принятия решения о компрометации секретного ключа обязан сдать все имеющиеся у него экземпляры секретных ключей, поставив отметку в соответствующих журналах о сдаче ключевого носителя.

5.3. В особых случаях, когда немедленная замена секретного ключа невозможна и существует острая необходимость в эксплуатации секретного ключа, пользователь СКЗИ может обратиться с просьбой о приостановке вывода секретного ключа из обращения. При этом пользователь СКЗИ должен до минимума сократить объем и важность электронного документооборота с использованием данного секретного ключа.

6. Хранение СКЗИ и ключевой информации

6.1. Пользователи СКЗИ должны хранить инсталлирующие носители СКЗИ, эксплуатационную и техническую документацию к СКЗИ, ключевые документы в шкафах (ящиках, хранилищах) индивидуального пользования в условиях, исключающих бесконтрольный доступ к ним, а также их непреднамеренное уничтожение. Пользователи СКЗИ должны предусмотреть также раздельное безопасное хранение действующих и резервных ключевых документов, предназначенных для применения в случае выхода из строя действующих криптоключей. Резервные ключевые носители хранятся в спецхранилищах ответственного пользователя СКЗИ.

6.2. В спецпомещениях пользователей СКЗИ для хранения выданных им ключевых документов, эксплуатационной и технической документации, инсталлирующих СКЗИ носителей необходимо иметь достаточное число надежно запираемых шкафов (ящиков, хранилищ) индивидуального пользования, оборудованных приспособлениями для опечатывания замочных скважин. Ключи от этих хранилищ должны находиться у соответствующих пользователей СКЗИ и должны сдаваться охране вместе с ключами от спецпомещения в отдельных опечатываемых пеналах (тубусах) в конце рабочего дня.

Приложение 1
к Инструкции пользователя
средств криптографической
защиты информации

Обязательства
пользователя средств криптографической защиты информации

Я,_____,
становясь пользователем средств криптографической защиты информации, добровольно беру на себя следующие обязательства:

- не разглашать и не передавать посторонним лицам сведения конфиденциального характера, которые мне будут доверены или станут известны по работе;
- не распространять сведения о функционировании и порядке обеспечения безопасности СКЗИ и ключевых документах к ним, а также иной конфиденциальной информации, ставшей мне известной в процессе выполнения своих служебных обязанностей;
- неукоснительно выполнять относящиеся к моей деятельности требования по обеспечению безопасности конфиденциальной информации;
- немедленно сообщать ответственному пользователю СКЗИ о ставших мне известных попытках посторонних лиц получить сведения о защищаемой конфиденциальной информации, об используемых СКЗИ или ключевых документах к ним;
- не использовать знания о защищаемой конфиденциальной информации, СКЗИ, криптоключах к ним для занятий любым видом деятельности, которая может нанести ущерб администрации района;
- в случае увольнения или отстранения от исполнения возложенных обязанностей сдать ответственному пользователю СКЗИ, ключевые документы и все носители конфиденциальной информации, которые находились в моём распоряжении;
- немедленно докладывать ответственному пользователю об утрате или недостаче СКЗИ, ключевых документов к ним, удостоверений, пропусков, ключей от помещений, хранилищ, сейфов (металлических шкафов), 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.

_____ _____
подпись дата