«СОГЛАСОВАНО»
Председатель Управляющего совета
ГБОУ НШ «Гармония»
п.г.т. Безенчук
_____Н.А. Жесткова
«10» января 2023г.

C=RU, O="ГБОУ НШ ""Гармония""
п.г.т. Безенчук", CN=Директор -
Шишкина В.И.,
E=garmoniya_nsds_bzn@samara.edu.ru
008d6da80728a89db9
2023.03.31 14:48:34+04'00'

«УТВЕРЖДАЮ»
Директор
ГБОУ НШ «Гармония»
п.г.т. Безенчук
_____В.И. Шишкина
«10» января 2023г.

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 организациях, которые осуществляют работы с применением СКЗИ (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 с 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.

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 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.

2. Работа с СКЗИ

Размещение и монтаж СКЗИ, а также другого оборудования, функционирующего с СКЗИ, в помещениях пользователей СКЗИ должны свести 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 должны быть обеспечены условия хранения ключевых носителей, исключающие возможность доступа к ним посторонних лиц, несанкционированного использования 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 и (или) сотрудниками 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 должна быть прекращена и организуются мероприятия по анализу и ликвидации негативных последствий данного нарушения.

3. 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) нарушение целостности печатей на сейфах с носителями ключевой информации, если используется процедура опечатывания сейфов;
6) утрата ключей от сейфов в момент нахождения в них носителей ключевой информации;
7) утрата ключей от сейфов в момент нахождения в них носителей ключевой информации с последующим обнаружением;
8) доступ посторонних лиц к ключевой информации;
9) 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, 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 Организация (обладатель скомпрометированной информации ограниченного доступа).

4. 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 с использованием СКЗИ безопасности информации ограниченного доступа;
4) Немедленно уведомлять 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;
5) В случае необходимости производить уничтожение криптоключей и ключевых документов в соответствии с требованиями пунктов 41-46 Инструкции ФАПСИ от 13 июня 2001 г. №152;
6) 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 с 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.

Ознакомлен:

Ответственный по информационной безопасности

Заместитель директора Н.Г. Поваляева

Приложение 1

Журнал поэкземплярного учета СКЗИ (форма)

Журнал начат «____» _____ 20__ г.

Журнал завершен «____» _____ 20__ г.

На _____ листах

№ п/п	Наименование СКЗИ	Лицензионный/серийный номер СКЗИ	Учетный номер дистрибутива СКЗИ	Отметка о получении		Отметка о подключении (установке СКЗИ)				Отметка об изъятии СКЗИ из аппаратных средств, уничтожении ключевых документов		Примечание
				Наименование организации, передавшей СКЗИ	Номер и дата документа, подтверждающего получение СКЗИ	Ф.И.О. пользователя СКЗИ	Ф.И.О. сотрудника, установившего СКЗИ	Дата подключения (установки) СКЗИ, расписка об установке	Инв. номер аппаратных средств,на которые установлены СКЗИ	Ф.И.О. сотрудника, производившего изъятие (уничтожение) СКЗИ	Дата изъятия (удаления) СКЗИ, расписка об уничтожении (удалении)	
1	2	3	4	5	6	7	8	9	10	11	12	13

Приложение 2

АКТ № _____ от «__» _____ 20__ г.
об уничтожении криптографических ключей, содержащихся на ключевых носителях, и ключевых документов

Комиссия сотрудников _____ в составе:
(название организации)
_____
_____
_____
произвела уничтожение криптографических ключей, содержащихся на ключевых носителях, и ключевых документов:

№	Учетный номер ключевого носителя (документа)	Номер (идентификатор) криптографического ключа, наименование документа	Владелец ключа (документа)	Количество ключевых носителей (документов)	Номера экземпляров	Всего уничтожается ключей (документов)

Всего уничтожено _____ криптографических ключей на _____ ключевых носителях.

Уничтожение криптографических ключей выполнено путем их стирания (разрушения) по технологии, принятой для ключевых носителей многократного использования в соответствии с требованиями эксплуатационной и технической документации на соответствующие СКЗИ.

Записи Акта сверены с записями в Журнале поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов.

Факт списания с учета ключевых носителей в Журнале поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов **подтверждаю**:

Ответственный за организацию работ по криптографической защите информации _____/_____

Члены комиссии:
_____/_____
_____/_____
_____/_____