Государственное областное казенное учреждение
«Мончегорский межрайонный центр социальной поддержки населения»
(ГОКУ «Мончегорский межрайонный ЦСПН»)

ПРИКАЗ

21 сентября 2021 г. Мончегорск № 187

Об утверждении перечня мер, направленных на выполнение требований законодательства Российской Федерации в области защиты информации с использованием средств криптографической защиты

В целях выполнения требований законодательства Российской Федерации в области защиты информации при ее передаче по открытым каналам связи с использованием средств криптографической защиты, приказа ФАПСИ от 13 июня 2001 г. № 152 «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», приказа ФСБ России от 10 июля 2014 г. № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности», **п р и к а з ы в а ю** :

1. Назначить ответственным пользователем средств криптографической защиты информации(далее – СКЗИ) начальника информационно-аналитического отдела ГОКУ «Мончегорский межрайонный ЦСПН (далее – Учреждение) Лоскутову Юлию Анатольевну.

2. На время длительного отсутствия (отпуска, командировки) назначить исполняющей обязанности ответственного пользователяСКЗИ заместителя директора Ломоносову Ингу Ивановну.Утвердить Инструкцию ответственного пользователя СКЗИ(Приложение № 1).

3. Утвердить Инструкцию пользователя СКЗИ (Приложение № 2).

4. Утвердить Перечень помещений ГОКУ «Мончегорский межрайонный ЦСПН», где размещены используемые СКЗИ, хранятся СКЗИ и (или) носители ключевой, аутентифицирующей и парольной информации СКЗИ (Приложение № 3).

5. Утвердить Перечень лиц, имеющих доступ в помещения ГОКУ «Мончегорский межрайонный ЦСПН», где размещены используемые СКЗИ, хранятся СКЗИ и (или) носители ключевой, аутентифицирующей и парольной информации СКЗИ (Приложение № 4).

6. Утвердить Порядок доступа в помещения, где размещены

используемые СКЗИ, хранятся СКЗИ и (или) носители ключевой, аутентифицирующей и парольной информации СКЗИ (Приложение № 5).

7. Утвердить форму Журнала поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов (Приложение № 6).

8. Контроль за исполнением настоящего приказа оставляю за собой.

Директор В.В. Юрласова

Делопроизводитель Поленкова-Романович М.К.
В дело № 3

ПРИЛОЖЕНИЕ № 2
к приказу №187
от «21» сентября 2021 г.

Инструкция пользователя СКЗИ ГОКУ «Мончегорский межрайонный ЦСПН»

1. Общие положения

1.1. Настоящая Инструкция пользователя средств криптографической защиты информации(далее – СКЗИ)(далее–Инструкция) определяет права и обязанности пользователей СКЗИ, порядок обращения с СКЗИ, а также определяет порядок восстановления связи в случае компрометации действующих ключей к СКЗИ.

1.2. Пользователем СКЗИявляется сотрудник ГОКУ «Мончегорский межрайонный ЦСПН»(далее – Учреждение), включенный в перечень сотрудников, допущенных к работе с СКЗИ, предназначенными для обеспечения безопасности защищаемой информации, не содержащей сведения, составляющие государственную тайну, в информационных системах Учреждения, утвержденный нормативным актом Учреждения иназначенные на должности, выполнение обязанностей по которым связано с использованием СКЗИ.

1.3. Непосредственно к работе с СКЗИ, предназначенными для обеспечения безопасности защищаемой информации, не содержащей сведения, составляющие государственную тайну, в информационных системах Учреждения, пользователи допускаются только после прохождения специальной подготовки (обучения). Документом, подтверждающим должную специальную подготовку сотрудников Учрежденияи возможность их допуска к самостоятельной работе с СКЗИ, является заключение, составленное комиссией на основании принятого зачета по программе подготовки.

1.4. Пользователь СКЗИдолжен знать нормы действующего законодательства Российской Федерации в сфере (области) обработки и обеспечения безопасности защищаемой информации, не содержащей сведения, составляющие государственную тайну (далее – защищаемая информация), а также в области защиты информации при ее передаче по открытым каналам связи с использованием средств криптографической защиты.

1.5. В своей деятельности, связанной с обработкой защищаемой информации с использованием СКЗИ, пользователь СКЗИруководствуется настоящей Инструкцией.

1.6. Пользователи СКЗИнесут персональную ответственность за обеспечение конфиденциальности ключевой информации и защиту СКЗИот несанкционированного использования.

2. Обязанности и права пользователя СКЗИ

2.1. Пользователь СКЗИобязан:

– не разглашать конфиденциальную информацию, к которой они допущены, и сведения о криптографических ключах;

– соблюдать требования по обеспечению безопасности информации с использованием СКЗИ;

– сообщать ответственному пользователю СКЗИ Учреждения о ставших им известными попытках посторонних лиц получить сведения об используемых СКЗИ или ключевых документах;

– сдать сотруднику ответственному пользователю СКЗИ Учреждения СКЗИ, эксплуатационную и техническую документацию к ним, ключевые документы при увольнении или отстранении от исполнения обязанностей, связанных с использованием СКЗИ;

– немедленно уведомлять ответственного пользователя СКЗИ Учреждения о фактах утраты или недостачи СКЗИ, ключевых документов, ключей от помещений, сейфов, личных печатей.

2.2. Пользователю СКЗИзапрещается:

– производить несанкционированное копирование ключевых документов;

– знакомить или передавать ключевые документы лицам, к ним не допущенным;

– выводить ключевые документы на дисплей или принтер;

– вставлять носители ключевой информации в считывающие устройства других компьютеров;

– оставлять носители ключевой информации без присмотра на рабочем месте.

– хранить носители ключевой информации вне хранилищ и помещений, гарантирующих их сохранность и конфиденциальность;

– хранить на носителях ключевой информации какую-либо информацию, кроме ключевой;

– использовать в помещениях, где применяются СКЗИ, личные технические средства, позволяющие осуществлять копирование ключевой информации.

2.3. Пользователь имеет право:

– вносить предложения руководству Учрежденияпо вопросам использования СКЗИ;

– повышать уровень квалификации по использованию СКЗИ.

3. Восстановление связи в случае компрометации действующих ключей к СКЗИ

3.1. Под компрометацией криптографического ключа понимается утрата доверия к тому, что данный ключ обеспечивает однозначную идентификацию владельца носителя ключевой информации и конфиденциальность информации, обрабатываемой с его помощью. К событиям, связанным с компрометацией действующих криптографических ключей, относятся:

– утрата (хищение) носители ключевой информации, в том числе – с последующим их обнаружением;

– увольнение (переназначение) сотрудников, имевших доступ к носителям ключевой информации;

– передача секретных ключей по линии связи в открытом виде;

– нарушение правил хранения носителей ключевой информации;

– вскрытие фактов утечки передаваемой информации или её искажения (подмены, подделки);

– ошибки при совершении криптографических операций;

– несанкционированное или безучётное копирование ключевой информации;

– все случаи, когда нельзя достоверно установить, что произошло с носителем ключевой информации (в том числе случаи, когда носитель ключевой информациивышел из строя и доказательно не опровергнута вероятность того, что данный факт произошел в результате злоумышленных действий).

3.2. При наступлении любого из перечисленных выше событий пользователь СКЗИдолжен немедленно прекратить связь с другими абонентами и сообщить о факте компрометации (или предполагаемом факте компрометации) ответственному пользователю СКЗИлично, по телефону, электронной почте или другим доступным способом. В любом случае пользователь СКЗИобязан убедиться, что его сообщение получено и прочтено.

3.3. При подтверждении факта компрометации действующих ключей пользователь СКЗИобязан обеспечить немедленное изъятие из обращения скомпрометированных криптографических ключей и сдачу ответственному пользователю СКЗИ в течение 3 рабочих дней.

3.4. Для восстановления конфиденциальной связи после компрометации действующих ключей пользователь СКЗИполучает у ответственного пользователя СКЗИновые ключи.

ПРИЛОЖЕНИЕ № 3
к приказу№187
от «21» сентября 2021 г.

Перечень помещений, где размещены используемые СКЗИ, хранятся СКЗИ и (или) носители ключевой, аутентифицирующей и парольной информации СКЗИ

№ п/п	Адрес места расположения	Наименование структурного подразделения	Наименование помещения
1.	Мурманская область,г.Мончегорск,ул.Комсомольская,д.7а	г.Мончегорск	Кабинеты № 7,8,10,11,15

ПРИЛОЖЕНИЕ № 5
к приказу №187
от «21» сентября 2021 г.

Порядок доступа в помещения, где размещены используемые СКЗИ, хранятся СКЗИ и (или) носители ключевой, аутентифицирующей и парольной информации СКЗИ

1. Настоящий Порядок регламентирует условия и порядок осуществления доступа в помещения ГОКУ «Мончегорский межрайонный ЦСПН»(далее – Учреждение), где размещены используемые средств криптографической защиты информации(далее – СКЗИ), хранятся СКЗИи (или) носители ключевой, аутентифицирующей и парольной информации СКЗИ(далее – Помещения) в целях организации режима, препятствующего возможности неконтролируемого проникновения или пребывания в Помещениях лиц, не имеющих прав доступа в Помещения.

2. Настоящий Порядок разработан в соответствии с требованиями постановления Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», приказа ФСБ России от 10 июля 2014 г. № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности», приказа ФАПСИ от 13 июня 2001 г. № 152 «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».

3. Для Помещений организуется режим, препятствующий возможности неконтролируемого проникновения или пребывания в Помещениях лиц, не имеющих прав доступа в Помещения.

4. Помещения, где размещены используемые СКЗИ, хранятся СКЗИ, должны быть оснащены входными дверьми с замками, должно обеспечиваться постоянное закрытие дверей таких Помещений на замок и их открытие только для санкционированного прохода.

5. Доступ в Помещения в рабочее (служебное) время имеют сотрудники, включенные в Перечень лиц, имеющих доступ в Помещения, утвержденный нормативным актом Учреждения.

6. В нерабочее (неслужебное) время пребывание вышеуказанных сотрудников разрешается на основании служебных записок (или иных видов разрешающих документов), подписанных руководителем Учреждения.

7. Нахождение в Помещениях посторонних лиц в рабочее (служебное) и нерабочее (неслужебное) время запрещается.

8. Уборка и техническое обслуживание Помещений допускаются только в присутствии Сотрудников Учреждения.

9. Руководитель и лица, его замещающие, могут находиться в Помещениях в любое время, в том числе в нерабочие и праздничные дни.

10. О попытках неконтролируемого проникновения посторонних лиц в Помещения необходимо незамедлительно сообщать руководителю Учреждения.

11. В случае возникновения нештатной ситуации необходимо незамедлительно сообщать руководителюУчреждения.

12. Сотрудники органов МЧС и аварийных служб, врачи «скорой помощи» допускаются в Помещения для ликвидации нештатной ситуации, иных чрезвычайных ситуаций или оказания медицинской помощи в сопровождении руководителя Учреждения.

ПРИЛОЖЕНИЕ № 6
к приказу №187
от «21» сентября 2021 г.

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

№ п/п	Наименование СКЗИ, эксплуатационной и технической документации к ним, ключевых документов	Серийные номера СКЗИ, эксплуатационной и технической документации к ним, номера серий ключевых документов	Номера экземпляров (криптографические номера) ключевых документов	Отметка о получении		Отметка о выдаче		Отметка о подключении (установке) СКЗИ			Отметка об изъятии СКЗИ из аппаратных средств, уничтожении ключевых документов			Примечание
				От кого получены	Дата и номер сопроводительного письма	Ф.И.О. пользователя СКЗИ	Дата и расписка в получении	Ф.И.О. сотрудников органа криптографической защиты, пользователя СКЗИ, произведших подключение (установку)	Дата подключения (установки) и подписи лиц, произведших подключение (установку)	Номера аппаратных средств, в которые установлены или к которым подключены СКЗИ	Дата изъятия (уничтожения)	Ф.И.О. сотрудников органа криптографической защиты, пользователя СКЗИ, производивших изъятие (уничтожение)	Номер акта или расписка об уничтожении	
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15