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

ПРИКАЗ

21 сентября 2021 г. Мончегорск № 188

О допуске сотрудников к самостоятельной работе со средствами криптографической защиты информации

В целях выполнения требований «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 13.06.2001 № 152, **приказываю:**

1. Утвердить Инструкцию о порядке допуска сотрудников ГОКУ «Мончегорский межрайонный ЦСПН» (далее -Учреждение)к самостоятельной работе со средствами криптографической защиты информации (Приложение № 1).
2. Утвердить Состав комиссии по допуску к самостоятельной работе со средствами криптографической защиты информации Учреждения (Приложение № 2).
3. Утвердить Перечень сотрудников (работников), допущенных к самостоятельной работе со средствами криптографическими защиты информации в Учреждении (Приложение № 3).
4. Утвердить Инструкцию по хранению и порядку учета, выдачи средств криптографической защиты информации, эксплуатационно-технической документации к ним, ключевых документов в Учреждении (Приложение № 4).
5. Контроль за исполнением настоящего приказа оставляю за собой.

Директор В.В. Юрласова

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

ПРИЛОЖЕНИЕ №1
к приказу 188
от «21» сентября 2021 г.

Инструкция
о порядке допуска сотрудников ГОКУ «Мончегорский межрайонный ЦСПН» к самостоятельной работе со средствами криптографической защиты информации

1. Настоящая Инструкция разработана в соответствии с действующим законодательством Российской Федерации, нормативно-правовыми актами органов государственного управления Российской Федерации в области защиты информации, а также эксплуатационной документацией на используемые средства криптографической защиты информации (далее – СКЗИ),и определяет порядок допуска сотрудников ГОКУ «Мончегорский межрайонный ЦСПН»(далее – Учреждение)к самостоятельной работе с СКЗИ.

2. К самостоятельной работе с СКЗИ допускаются лица:

- принятые на работу в Учреждение приказом (распоряжением) руководителя, на основании заключенных с ними трудовых договоров и назначенные на должности, выполнение обязанностей по которым связано с использованием СКЗИ;

- прошедшие специальную подготовку (обучение) по программам, утвержденным руководителем Учреждения, и успешно сдавшие зачет на допуск к самостоятельной работе с СКЗИ комиссии по допуску к самостоятельной работе с СКЗИ, назначенной приказом (распоряжением) руководителя Учреждения.

3. Документом, подтверждающим должную специальную подготовку сотрудников Учреждения и возможность их допуска к самостоятельной работе с СКЗИ, является Заключение (Приложение № 1), составленное комиссией на основании принятого зачета по программе подготовки. Заключения о допуске сотрудников к самостоятельной работе с СКЗИ утверждаются руководителем Учреждения.

4. Программа подготовки сотрудников Учреждения к самостоятельной работе с СКЗИ (Приложение № 2) разрабатывается ответственным пользователем СКЗИ Учреждения, утверждается руководителем Учреждения и должна содержать:

- ознакомление с нормами действующего законодательства Российской Федерации, регулирующими отношения, возникающие при формировании и использовании информационных ресурсов на основе создания, сбора, обработки, накопления, хранения, поиска, распространения и предоставления документированной информации; защите информации, прав субъектов, участвующих в информационных процессах и информатизации; использовании электронной подписи в электронных документах; ответственности за нарушение указанных норм;

- ознакомление с нормативными актами органов государственного управления Российской Федерации, определяющими порядок разработки,

производства, реализации, использования СКЗИ; регламентирующими вопросы взаимодействия участников информационного обмена с использованием СКЗИ;

- изучение должностных инструкций, положений и других локальных нормативных актов Учреждения по вопросам производственной деятельности, связанной с разработкой, производством, хранением, реализацией и использованием СКЗИ;

- изучение эксплуатационно-технической документации на СКЗИ;

- приобретение практических навыков выполнения работ, предусмотренных обязанностями по занимаемой должности.

6. Методика подготовки сотрудников Учреждения к сдаче зачета на допуск к самостоятельной работе с СКЗИ определяется ответственным пользователем СКЗИ Учреждения и предусматривает как формы самостоятельного изучения и освоения программного материала сотрудником, так и формы группового или индивидуального обучения с привлечением наиболее подготовленных специалистов Учреждения в качестве преподавателей.

ПРИЛОЖЕНИЕ №2
к приказу 188
от «21» сентября 2021 г.

Состав комиссии по допуску к самостоятельной работе со средствами криптографической защиты информации ГОКУ «Мончегорский межрайонный ЦСПН»

Председатель комиссии:
1. Ломоносова Инга Ивановна

Члены комиссии:
1. Лоскутова Юлия Анатольевна
2. Стецюк Руслан Вадимович
3. Уваров Алексей Владимирович

ПРИЛОЖЕНИЕ № 4
к приказу 188
от «21» сентября 2021 г.

Инструкция
по хранению и порядку учета, выдачи средств криптографической защиты информации, эксплуатационно-технической документации к ним, ключевых документов в ГОКУ «Мончегорский межрайонный ЦСПН»

Список используемых сокращений:
СКЗИ – средство криптографической защиты информации.

1. Общие положения

1.1. Все действия с СКЗИ осуществляются в соответствии с эксплуатационной документацией на СКЗИ.

1.2. Организацию и обеспечение работ по техническому обслуживанию СКЗИ и управления криптографическими ключами осуществляет ответственный пользователь СКЗИ ГОКУ «Мончегорский межрайонный ЦСПН»(далее– Учреждение).

Ответственный пользователь СКЗИ Учреждения осуществляет:

– поэкземплярный учет используемых СКЗИ, эксплуатационной и технической документации к ним;

– учет пользователей СКЗИ;

– обучение\инструктаж лиц, использующих СКЗИ, правилам работы с ними;

– контроль за соблюдением условий использования СКЗИ в соответствии с эксплуатационной и технической документацией на СКЗИ и настоящей Инструкцией;

– расследование и составление заключений по фактам нарушения условий использования СКЗИ, которые могут привести к снижению требуемого уровня безопасности информации;

– разработку и принятие мер по предотвращению возможных негативных последствий подобных нарушений;

– разработку мероприятий по обеспечению функционирования и безопасности, применяемых СКЗИ в соответствии с условиями выданных на них сертификатов, а также в соответствии с эксплуатационной и технической документацией к этим средствам.

2. Учет и хранение СКЗИ и криптографических ключей

2.1. Хранение и учет СКЗИ, эксплуатационно-технической документации к ним, ключевых документов в Учреждении организуется в соответствии с требованиями, нормативной документацией ФСБ РФ, Правилами

использования СКЗИ, утвержденными разработчиком СКЗИ, требованиями другой нормативной документации.

2.2. СКЗИ, эксплуатационная и техническая документация к ним, криптографические ключи необходимо учитывать поэкземплярно.

2.2.1. Единицей поэкземплярного учета ключевых документов считается ключевой носитель многократного использования, ключевой блокнот. Если один и тот же ключевой носитель многократно используют для записи криптоключей, то его каждый раз следует регистрировать отдельно.

2.2.2. Единицей поэкземплярного учета СКЗИ считается инсталлирующая дискета или компакт диск (CD-ROM), либо лицензионное соглашение на право использования.

2.3. Поэкземплярный учет выдаваемых пользователям ключевых документов, дистрибутивов СКЗИ и эксплуатационно-технической документации к ним, лицензий на право пользования СКЗИ необходимо вести в соответствующих журналах поэкземплярного учета.

2.4. Учет СКЗИ, эксплуатационной и технической документации к ним, ключевых документов, может быть организован как на бумажных носителях, так и в электронном виде.

2.5. Формы журналов должны соответствовать требованиям нормативных документов и утверждаться руководителем Учреждения.

2.6. Программные СКЗИ должны учитываться совместно с аппаратными средствами, с которыми осуществляется их штатная эксплуатация. Если аппаратные или аппаратно-программные СКЗИ подключаются к системной шине или к одному из внутренних интерфейсов аппаратных средств, то такие СКЗИ учитываются также совместно с соответствующими аппаратными средствами.

2.7. Все полученные экземпляры СКЗИ, криптографических ключей должны быть выданы под роспись пользователям СКЗИ, несущим персональную ответственность за их сохранность.

2.8. Дистрибутивы СКЗИ на носителях, эксплуатационная и техническая документация к СКЗИ, инструкции хранятся у ответственного пользователя СКЗИ Учреждения. Криптографические ключи хранятся у пользователей СКЗИ.

2.9. Аппаратные средства, с которыми осуществляется штатное функционирование СКЗИ, а также аппаратные и программно-аппаратные СКЗИ должны быть оборудованы средствами контроля за их вскрытием (опечатаны, опломбированы). Место опечатывания (опломбирования) СКЗИ, аппаратных средств должно быть таким, чтобы его можно было визуально контролировать.

2.10. При необходимости, криптографические ключи могут передаваться по акту на временное хранение ответственному пользователю СКЗИ Учреждения.

3. Использование СКЗИ и криптографических ключей

3.1. Криптографические ключи используются для обеспечения конфиденциальности, авторства и целостности электронных документов.

3.2. Для обеспечения контроля доступа к СКЗИ системный блок ПЭВМ опечатывается.

3.3. Пользователи обязаны:

– 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 Учрежденияо 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.

3.4. Не допускается:

– 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.

3.5. При выявлении сбоев или отказов пользователь обязан сообщить о факте их возникновения ответственному пользователю СКЗИ Учрежденияи предоставить носители криптографических ключей для проверки их работоспособности. Проверка работоспособности носителей криптографических ключей выполняется в присутствии пользователя.

3.6. Вскрытие системного блока ПЭВМ, на которой установлено СКЗИ, для проведения ремонта или технического обслуживания должно осуществляться в присутствии ответственного пользователя СКЗИ Учреждения.