

**ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ УЧРЕЖДЕНИЕ ЗДРАВООХРАНЕНИЯ
«Камчатский краевой противотуберкулезный диспансер»
(ГБУЗ ККПТД)**

ПРИКАЗ № 1037

г. Петропавловск-Камчатский

«50» 12 2020 года

О порядке хранения и эксплуатации средств криптографической защиты информации (СКЗИ) в Филиале № 1 "ГБУЗ ККПТД" - пгт. Палана

В целях исполнения нормативных документов

- Состав и содержание 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 (утв. приказом ФСБ России от 10.07.2014 № 378);
- Положение о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (утв. приказом ФСБ России от 09.02.2005 № 66);
- Инструкция 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 (утв. приказом ФАПСИ от 13.06.2001 № 152).

ПРИКАЗЫВАЮ:

1. Ответственным за хранение и эксплуатацию СКЗИ (органом криптографической защиты – ОКЗ) в Филиале № 1 "ГБУЗ ККПТД" - пгт. Палана назначить программиста Малышева М.Н.

2. К работе с СКЗИ допускать только пользователей (далее – Пользователи), прошедших предварительное обучение работе с СКЗИ согласно утвержденному перечню лиц (Приложение № 1).

3. Пользователям и ОКЗ в своей работе, связанной с обеспечением безопасности СКЗИ, ключевых документов, ключевых носителей и эксплуатационной документации к СКЗИ руководствоваться утвержденной инструкцией по обеспечению безопасности эксплуатации СКЗИ (Приложение № 2).

4. Поэземплярный учет СКЗИ, эксплуатационной и технической документации к ним, ключевых документов вести в Журнале по форме, утвержденной в Приложении № 4 к настоящему Приказу.

5. Назначить комиссию по уничтожению криптографических ключей и ключевых носителей в составе:

Малышева М.Н., программист – председатель комиссии;

Шапкин Евгений Александрович, специалист по защите информации – член комиссии;

Варнавский Фёдор Геннадьевич, программист – член комиссии;



Приложение № 1

УТВЕРЖДЕН

О порядке хранения и эксплуатации средств криптографической защиты информации (СКЗИ) в Филиале № 1 "ГБУЗ ККПТД" - пгт. Палана

[Handwritten signature]
от «50» 12

2020г. № 1037

Перечень сотрудников Филиала № 1 "ГБУЗ ККПТД" - пгт. Палана допущенных к работе с СКЗИ

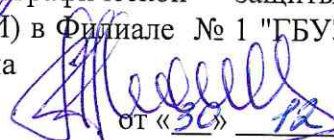
№ п/п	ФИО	Должность	СКЗИ
1	Мальшев Максим Николаевич	программист	ViPNet CSP, Crypto pro csp
2	Покалина Яна Ильмаровна	Старшая мед сестра	Crypto pro csp
3			
4			
5			
6			
7			
8			
9			
10			
11			
12			
13			
14			
15			
16			
17			
18			
19			
20			
21			
22			
23			
24			
25			
26			
27			
28			
29			
30			



Приложение № 2

УТВЕРЖДЕН

О порядке хранения и эксплуатации средств криптографической защиты информации (СКЗИ) в Филиале № 1 "ГБУЗ ККПТД" - пгт. Палана


от «30» 12 2020г. № 1037

Инструкция по обеспечению безопасности эксплуатации СКЗИ в Филиале № 1 "ГБУЗ ККПТД" - пгт. Палана

1. ОБЩИЕ ПОЛОЖЕНИЯ

- 1.1. Настоящая Инструкция определяет порядок учета, хранения и использования СКЗИ, криптографических ключей и ключевых документов, а также порядок изготовления, смены, уничтожения и компрометации криптографических ключей в целях обеспечения безопасности эксплуатации СКЗИ.
- 1.2. Настоящая Инструкция разработана в соответствии со следующими нормативными правовыми актами Российской Федерации:
 - Состав и содержание 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 (утв. приказом ФСБ России от 10.07.2014 № 378);
 - Положение о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (утв. приказом ФСБ России от 09.02.2005 № 66);
 - Инструкция 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 (утв. приказом ФАПСИ от 13.06.2001 № 152).
- 1.3. В Филиале №1 «ГБУЗ ККПТД – пгт.Палана» используются только сертифицированные ФСБ России СКЗИ, предназначенные для защиты информации, не содержащей сведений, составляющих государственную тайну.
- 1.4. В Филиале №1 «ГБУЗ ККПТД – пгт.Палана» приказом главного врача назначается ответственный за хранение и эксплуатацию СКЗИ, именуемый также органом криптографической защиты информации (далее – ОКЗ).
- 1.5. Подписывая лист ознакомления с настоящей Инструкцией, ОКЗ подтверждает, что также ознакомлен с Инструкцией 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 (утв. приказом ФАПСИ от 13.06.2001 № 152).

1.6. ОКЗ осуществляет:

- поэкземплярный учет СКЗИ, эксплуатационной и технической документации к ним, ключевых носителей и ключевых документов;
- учет пользователей СКЗИ (далее – Пользователи) и представление на утверждение главному врачу списка пользователей СКЗИ;
- контроль за соблюдением условий использования СКЗИ;
- расследования и составление заключений по фактам нарушений условий использования СКЗИ;
- разработку и обеспечение мер по предотвращению возможных нежелательных последствий таких нарушений;
- обучение Пользователей правилам работы с СКЗИ и правилам хранения СКЗИ, ключевых носителей и ключевых документов.

1.7. Список Пользователей утверждается приказом главного врача Камчатского краевого противотуберкулезного диспансера

1.8. Пользователь обязан:

- не разглашать конфиденциальную информацию, к которой он допущен, в том числе: сведения об СКЗИ, ключевых документах к ним и других мерах защиты;
- соблюдать требования по обеспечению безопасности конфиденциальной информации при использовании СКЗИ;
- хранить ключевую информацию в сейфах и помещениях, гарантирующую ее сохранность и конфиденциальность;
- сообщать ОКЗ о попытках посторонних лиц получить сведения об СКЗИ или ключевых документах к ним;
- незамедлительно уведомлять ОКЗ о фактах утраты или недостачи СКЗИ, криптографических ключей, 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;
- сдать СКЗИ, эксплуатационную и техническую документацию к ним, криптографические ключи ОКЗ, в соответствии с порядком, установленным настоящей Инструкцией, при прекращении использования СКЗИ (увольнении, переводе на другую должность и в иных подобных случаях).

1.9. К работе с СКЗИ Пользователи допускаются только после соответствующего инструктажа.

2. УЧЕТ СКЗИ, ХРАНЕНИЕ И ПЕРЕДАЧА КРИПТОГРАФИЧЕСКИХ КЛЮЧЕЙ

- 2.1. СКЗИ, эксплуатационная и техническая документация к ним, ключевые документы и ключевые носители подлежат поэкземплярному учету. Программные СКЗИ учитываются совместно с аппаратными средствами, на которых осуществляется их штатная эксплуатация. Учет осуществляется ОКЗ в Журнале поэкземплярного учета средств криптографической защиты информации, эксплуатационной и технической документации к ним, ключевых документов (далее – Журнал).
- 2.2. Единицей поэкземплярного учета ключевых документов считается отчуждаемый носитель с записанными криптографическими ключами. Если один и тот же носитель используется для записи другого криптографического ключа, его необходимо зарегистрировать снова.
- 2.3. Все полученные экземпляры СКЗИ, эксплуатационная и техническая документация к ним, ключевые документы выдаются Пользователям под роспись в Журнале. Пользователи несут персональную ответственность за сохранность СКЗИ и ключевых документов.
- 2.4. Дистрибутивы СКЗИ, эксплуатационная и техническая документация к ним хранятся у ОКЗ.
- 2.5. Ключевые носители с криптографическими ключами хранятся у Пользователей.
- 2.6. Хранение осуществляется в ящиках, шкафах, сейфах (хранилищах) индивидуального пользования в условиях, исключающих бесконтрольный доступ к ним, а также их непреднамеренное уничтожение.
- 2.7. В случае отсутствия у Пользователя индивидуального хранилища, ключевые носители с криптографическими ключами по окончании рабочего дня сдаются ОКЗ.
- 2.8. Ключевые носители с неработоспособными криптографическими ключами ОКЗ принимает от Пользователя и делает соответствующую запись в Журнале. Неработоспособные ключевые носители подлежат уничтожению.
- 2.9. Аппаратные средства, с которыми осуществляется штатное использование СКЗИ, а также аппаратные СКЗИ должны быть оборудованы средствами контроля за их вскрытием (опечатаны, опломбированы). Место опечатывания (опломбирования) СКЗИ и аппаратных средств должно быть визуально контролируемым.

3. ИСПОЛЬЗОВАНИЕ СКЗИ

- 3.1. В Филиале № 1 "ГБУЗ ККПТД" - пгт. Палана СКЗИ используется с целью обеспечения конфиденциальности и целостности электронных документов и сетевого трафика.

- 3.2. Для шифрования электронного документа и/или сетевого трафика Пользователь использует свой собственный закрытый криптографический ключ и открытый криптографический ключ.
- 3.3. В Филиал № 1 "ГБУЗ ККПТД" - пгт. Палана используются только те СКЗИ, которые реализуют стойкие криптографические алгоритмы, не позволяющие в разумные сроки вычислить закрытый ключ по открытому ключу.
- 3.4. Пользователь ежедневно проверяет сохранность технических средств и целостность печатей и пломб на них.
- 3.5. В случае обнаружения неразрешенного программного обеспечения или факта повреждения целостности печати (пломбы) на техническом средстве с СКЗИ, работа с СКЗИ на таком техническом средстве должна быть прекращена. По данному факту созывается группа реагирования на инциденты информационной безопасности (далее – ГРИИБ), которая действует в соответствии с инструкцией по реагированию на инциденты информационной безопасности.
- 3.6. Вскрытие технического средства с СКЗИ для проведения ремонта или технического обслуживания осуществляется только в присутствии ОКЗ.
- 3.7. При работе с СКЗИ запрещается:
- оставлять без присмотра (контроля) технические средства, на которых эксплуатируется СКЗИ;
 - самостоятельно вносить изменения в программную часть СКЗИ;
 - разглашать содержимое носителей ключевой информации или передавать сами носители лицам, к ним не допущенным, выводить ключевую информацию на дисплей, принтер и другие средства вывода информации;
 - использовать ключевые носители в режимах, не предусмотренных штатными функциями СКЗИ;
 - осуществлять несанкционированное копирование криптографических ключей;
 - изменять настройки или пытаться изменить настройки СКЗИ или операционной системы, сделанные ОКЗ;
 - использовать бывшие в работе ключевые носители для записи новой информации без предварительного гарантированного уничтожения на них ключевой информации;
 - осуществлять самостоятельное несанкционированное вскрытие технических средств с СКЗИ.
- 3.8. С целью обеспечения непрерывности работы Филиала №1 «ГБУЗ ККПТД – пгт.Палана» плановая замена ключевой информации должна производиться заблаговременно.

4. ДЕЙСТВИЯ ПРИ КОМПРОМЕТАЦИИ КРИПТОГРАФИЧЕСКИХ КЛЮЧЕЙ

- 4.1. Криптографические ключи считаются скомпрометированными в следующих случаях:
- потеря ключевых носителей (в том числе с последующим обнаружением);
 - увольнение сотрудников, имевших доступ к ключевым носителям;
 - возникновение подозрений на утечку информации или ее искажение в информационной системе;
 - нарушение печати на хранилище с ключевыми носителями ли на техническом средстве с СКЗИ;
 - временный бесконтрольный доступ посторонних лиц к ключевым носителям или техническим средствам с СКЗИ;
 - иные случаи подозрения компрометации криптографических ключей.
- 4.2. В случае подозрения в компрометации криптографических ключей, Пользователь должен немедленно прекратить эксплуатацию СКЗИ и продолжить ее только после замены криптографических ключей.
- 4.3. Скомпрометированные криптографические ключи подлежат уничтожению.

5. УНИЧТОЖЕНИЕ КРИПТОГРАФИЧЕСКИХ КЛЮЧЕЙ

- 5.1. Неиспользованные или выведенные из действия криптографические ключи подлежат уничтожению.
- 5.2. Уничтожение криптографических ключей на ключевых носителях производится комиссией в составе председателя и членов комиссии, назначенной главным врачом Камчатского краевого противотуберкулезного диспансера.
- 5.3. Криптографические ключи, записанные на машинные ключевые носители, уничтожаются методом гарантированного стирания информации на машинном носителе в соответствии с требованиями эксплуатационной и технической документации на СКЗИ.
- 5.4. Криптографические ключи, записанные на бумажных носителях, уничтожаются физически (сжигание, измельчение и т. д.).
- 5.5. Перед уничтожением криптографических ключей и/или ключевых носителей, комиссия обязана:
- установить наличие оригинала и количество копий криптографических ключей;
 - проверить внешнюю целостность каждого ключевого носителя;
 - идентифицировать каждый ключевой носитель в соответствии с Журналом поэкземплярного учета средств криптографической защиты информации;
 - убедиться, что криптографические ключи, находящиеся на ключевых носителях, действительно подлежат уничтожению;

- произвести уничтожение криптографических ключей на оригинале и всех копиях ключевого носителя.
- 5.6. По факту уничтожения криптографических ключей составляется Акт уничтожения (Приложение № 3).
- 5.7. Акт подписывается председателем и членами комиссии по уничтожению.
- 5.8. В Журнале поэкземплярного учета средств криптографической защиты информации делается отметка об уничтожении криптографических ключей.
- 5.9. Акты уничтожения криптографических ключей хранятся у ОКЗ.
6. ТРЕБОВАНИЯ К ПОМЕЩЕНИЯМ, В КОТОРЫХ ВЕДЕТСЯ РАБОТА С СКЗИ И/ИЛИ ХРАНЯТСЯ КРИПТОГРАФИЧЕСКИЕ КЛЮЧИ
- 6.1. Размещение, специально оборудование, охрана и организация режима в помещениях, где установлены СКЗИ и/или хранятся криптографические ключи (далее – спецпомещения), должны обеспечивать сохранность СКЗИ и криптографических ключей.
- 6.2. При оборудовании спецпомещений должны выполняться требования к размещению, монтажу СКЗИ, а также другого оборудования, функционирующего с СКЗИ.
- 6.3. Спецпомещения должны иметь прочные входные двери с замками, гарантирующими надежную защиту от проникновения посторонних лиц в нерабочее время. Окна помещений, расположенных на первых или последних этажах зданий, а также окна, находящиеся около пожарных лестниц и других мест, откуда возможно проникновение посторонних лиц, необходимо оборудовать средствами, препятствующими неконтролируемому проникновению в спецпомещения. При этом, применение нераспахиваемых железных решеток на окнах запрещено, поскольку это противоречит правилам пожарной безопасности.
- 6.4. Мониторы рабочих станций с СКЗИ должны быть повернуты задней стороной к дверям и окнам, либо должны применяться шторы, рольставни, жалюзи или другие средства для пресечения несанкционированного просмотра содержимого, отображаемого на мониторах.
- 6.5. Для хранения криптографических ключей, эксплуатационной и технической документации, дистрибутивов СКЗИ выделяется необходимое число надежных металлических хранилищ. Ключи от хранилищ хранятся у ОКЗ и у Пользователей.
- 6.6. По окончании рабочего дня спецпомещения и установленные в них хранилища должны быть закрыты на замок.
- 6.7. При обнаружении признаков, указывающих на возможное несанкционированное проникновение в спецпомещения или хранилища посторонних лиц, о случившемся должно быть немедленно сообщено ОКЗ. ОКЗ

должен оценить вероятность компрометации хранящихся криптографических ключей, составить акт и принять, при необходимости, меры к локализации последствия компрометации криптографических ключей и к их замене.



УТВЕРЖДЕН
 О порядке хранения и эксплуатации средств
 криптографической защиты информации
 СКЗИ в Филиале № 1 "ФБУЗ ККПТД" - пгт.
 Палана

[Handwritten signature]
 от «30» 12 2020г. № 1037

**АКТ № _____ от «___» _____ 20__ г.
 об уничтожении криптографических ключей и ключевых документов**

Комиссия в составе:

Мальшев М.Н., инженер программист – председатель комиссии;
 Шапкин Е.А., специалист по защите информации – член комиссии;
 Варнавский Ф.Г., ведущий инженер (программист) – член комиссии;

произвела уничтожение криптографических ключей и ключевых документов:

№ п/п	Учетный номер ключевого носителя	Номер криптографического ключа, наименование документа	Владелец ключа (документа)	Количество ключевых носителей (документов)	Номера экземпляров	Всего ключей	Примечания
1.							
2.							
3.							
4.							
5.							
6.							
7.							

Всего уничтожено _____ криптографических ключей на _____ ключевых носителях. Записи Акта сверены с записями Журнала поэкземплярного учета средств криптографической защиты информации, эксплуатационной и технической документации к ним, ключевых документов.

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

Ключевые носители списаны с учета в Журнале поэкземплярного учета средств криптографической защиты информации.

Председатель комиссии:	<hr/>	Мальшев М.Н.
Члены комиссии:	<hr/>	Шапкин Е.А.
	<hr/>	Варнавский Ф.Г.