Утверждено приказом
Главного врача
Республиканского Центра СПИД
_____/Санчы И.Д./
От «10» января 2023 г. № ___

Инструкция

по работе с отчуждаемыми носителями защищаемой информации, в том числе с ключевыми носителями, в информационных системах Государственного бюджетного учреждения здравоохранения Республики Тыва «Республиканский Центр по профилактике и борьбе со СПИД и инфекционными заболеваниями» (Республиканский Центр СПИД)

г. Кызыл
2023 год

1. Общие положения

1.1. Данная Инструкция содержит обязательные для всех сотрудников Республиканского Центра СПИД правила обращения с отчуждаемыми (съемными) носителями, использующимися для записи конфиденциальной информации и ключевыми носителями информации.

1.2. Под съемными носителями информации понимаются различные по физической структуре и конструктивному исполнению носители информации, используемые для записи и накопления информации с целью непосредственного ввода её в ЭВМ, обработки и передачи при помощи технических средств.

1.3. Под ключевым носителем информации понимается съемный носитель информации, на который записана уникальная секретная ключевая информация (идентификатор пользователя, закрытый ключ электронной подписи), используемая для подтверждения целостности, подлинности и авторства электронных документов, передаваемых в электронном виде.

1.4. Секретная ключевая информация, находящаяся на ключевом носителе, относится к категории сведений ограниченного распространения.

1.1. Данной инструкцией определяется порядок учета, хранения и обращения со съемными и ключевыми носителями (далее – носитель информации) информации и их утилизации. К съемным носителям информации относятся носители для однократной или многократной записи такие, как CD-R, CD-RW, DVD-R, DVD-RW, USB флеш-накопители, дискеты и т.д.

1.2. Также данная инструкция регламентирует порядок обслуживания и обеспечение безопасности несъемных электронных носителей информации, к которым относятся базы данных на жестких магнитных дисках, содержащие информацию подлежащую защите.

1.3. Под безопасностью данных на электронных носителях информации понимается сохранение конфиденциальности, исключение несанкционированного проникновения либо иных действий, в том числе не имеющих злого умысла, которые могут привести к потере, искажению, изменению, копированию и другим нежелательным действиям с данными.

1.4. Организационное и техническое обеспечение безопасности конфиденциальной информации, хранящейся на электронных носителях информации во всех информационных системах (ИС) Республиканского Центра СПИД, с использованием допустимых программно-аппаратных методов защиты, контроль за действиями сотрудников Республиканского Центра СПИД при работе с указанными носителями информации возлагается на администратора информационной безопасности.

1.5. Все находящиеся на хранении и в обращении носители информации конфиденциальной информации подлежат учёту. Каждый носитель информации с

записанными на нем защищаемыми данными должен иметь этикетку, на которой указывается его уникальный учетный номер.

1.6. Учет носителей информации осуществляет администратор информационной безопасности.

1.7. При обработке конфиденциальной информации пользователи ИС Республиканского Центра СПИД должны использовать только специально предназначенные для этого разделы (каталоги) электронных носителей информации или съемные маркированные носители информации.

1.8. При хранении носителей информации должны соблюдаться условия, обеспечивающие сохранность конфиденциальной информации и исключающие несанкционированный доступ к ней.

2. Обязанности работника

2.1. Работник обязан:

– при получении носителя информации, убедиться, что они правильно маркированы, и расписаться в соответствующем журнале.

– сдавать свой персональный ключевой носитель на временное хранение ответственному за обеспечение безопасности персональных данных на время длительного отсутствия на рабочем месте, в период отпуска и болезни и т.п.;

– сдавать свой съемный носитель на временное хранение администратору информационной безопасности на время длительного отсутствия на рабочем месте, в период отпуска и болезни и т.п.;

– в случае утери ключевого носителя немедленно сообщить об этом ответственному за обеспечение безопасности персональных данных и принять участие в служебном расследовании факта утери ключевого носителя;

– в случае утери съемного носителя немедленно сообщить об этом администратору информационной безопасности и принять участие в служебном расследовании факта утери съемного носителя;

– в случае перевода на другую работу, увольнения и т.п. он обязан сдать (сразу по окончании последнего сеанса работы) свой носитель информации администратору информационной безопасности и/или ответственному за обеспечение безопасности персональных данных под роспись в соответствующих журналах;

– хранить носитель конфиденциальной информации только в личном сейфе, либо в сейфе уполномоченного сотрудника.

2.2. Работникам запрещается:

– хранить носители конфиденциальной информации вместе с носителями открытой информации, на рабочих столах, либо оставлять их без присмотра в незапертом помещении или передавать на хранение другим лицам;

– выносить учтенные носители информации из служебных помещений для работы с ними на дому и т. д.

– передавать свой носитель информации другим лицам (кроме как для хранения уполномоченному лицу);

– оставлять носитель информации без личного присмотра;

– делать неучтенные копии с носителей информации.

2.3. При отправке или передаче конфиденциальных данных адресатам на съемные носители записываются только предназначенные адресатам данные.

2.4. Вынос съемных носителей, не содержащих персональных данных, для непосредственной передачи адресату осуществляется только с письменного разрешения администратора информационной безопасности на основании запроса сторонней организации.

2.5. Вынос съемных носителей персональных данных для непосредственной передачи адресату осуществляется только с письменного разрешения ответственного за обеспечение безопасности персональных данных в ИС Республиканского Центра СПИД на основании запроса сторонней организации с обязательной регистрацией в Журнале регистрации запросов на предоставление персональных данных.

2.6. Для защиты носителей информации от несанкционированного доступа, использования или повреждения во время транспортировки из одной организации в другую необходимо использовать надежных курьеров и транспорт, а также упаковку, защищающую носители от постороннего вмешательства и позволяющую выявить попытки ее вскрытия.

2.7. О фактах утраты носителей конфиденциальной информации либо разглашения содержащихся на них сведений немедленно ставится в известность руководителя Республиканского Центра СПИД, администратора информационной безопасности и ответственного за обеспечение безопасности персональных данных. На утраченные носители составляется акт. Соответствующие отметки вносятся в журнал учета носителей информации.

2.8. Съемные носители персональных данных, пришедшие в негодность, или отслужившие установленный срок, подлежат уничтожению. Уничтожение съемных носителей конфиденциальной информации осуществляется уполномоченной комиссией. По результатам уничтожения носителей составляется акт по форме (Приложение №1 к настоящей инструкции).

2.9. При изменении полномочий работника, его увольнения либо компрометации ключевого носителя, уничтожается все ключевая информация и подписывается акт об уничтожения ключевой информации с ключевых носителей (Приложение №2).

2.10. Носители, на которые осуществляется резервное копирование защищаемой информации, должны регулярно (не реже одного раза в 6 месяцев)

проверяться на отсутствие сбоев уполномоченными сотрудниками.

2.11. При повторном использовании носителей информации предыдущее содержимое должно надежно удаляться администратором информационной безопасности.

2.12. Повседневный и периодический контроль за действиями сотрудников Республиканского Центра СПИД при работе с носителями информации возлагается на администратора информационной безопасности.

3. Требования по работе с ключевым носителем

3.1. Для получения доступа к защищённым данным, хранящимся в памяти ключевого носителя, требуется ввести PIN-код (Personal Identification Number), являющегося аналогом пароля.

3.2. Пользователь должен выполнять следующие требования:

– изменить PIN-код сразу после получения ключевого носителя (USB-ключ/смарт-карту eToken). PIN-код необходимо хранить в тайне;

– соблюдать требования к ПИН-коду ключевого носителя, к его периодической смене.

3.3. При последовательном вводе более пяти неправильных PIN-кодов ключевой носитель блокируется. Для разблокировки ключевого носителя необходимо обратиться к администратору информационной безопасности.

3.4. В случае утраты ключевого носителя закрытый ключ восстановить невозможно. **Зашифрованная с помощью утерянного закрытого ключа информация восстановлению не подлежит.**

4. Ответственность

4.1. Сотрудник Республиканского Центра СПИД несет персональную ответственность за сохранность и правильное использование вверенного ему носитель информации.

4.2. За нарушение положений данной Инструкции к сотруднику может быть применена дисциплинарная ответственность, а так же ответственность, предусмотренная действующим законодательством РФ.

Разработал
Администратор информационной безопасности _____ / Сандаков З.Н.

«09» января 2023 г.

Приложение №1
к инструкции по работе с отчуждаемыми носителями
защищаемой информации, в том числе
с ключевыми носителями, в информационных
системах Республиканского Центра СПИД

УТВЕРЖДАЮ
Главный врач
_____/ **Санчы И.Д./**
« 10 » января **2023 г.**

АКТ
уничтожения съемных носителей персональных данных

Комиссия в составе:
1._____
2. _____
3. _____
провела отбор съемных носителей персональных данных, не подлежащих дальнейшему хранению:

№п/п	Дата	Учетный номер съемного носителя	Пояснения
1			
2			
…			

Всего съемных носителей_____
(цифрами и прописью)

На съемных носителях уничтожена конфиденциальная информация путем стирания ее на устройстве гарантированного уничтожения информации _____(механического уничтожения, сжигания и т.п.).

Перечисленные съемные носители уничтожены путем_____ (разрезания, демонтажа и т.п.).

Председатель комиссии _____/Ф.И.О./
Члены комиссии _____/Ф.И.О./
_____/Ф.И.О./

Приложение №2
к инструкции по работе с отчуждаемыми носителями
защищаемой информации, в том числе
с ключевыми носителями, в информационных
системах Республиканского Центра СПИД

УТВЕРЖДАЮ
Главный врач
_____/ Санчы И.Д./
« 10 » января 2023 г.

АКТ № _____
уничтожения ключевой информации с ключевых носителей

Проведено уничтожение ключевой информации с ключевых носителей :

Порядковый номер	Регистрационный номер	Вид ключевой информации (Э/Р)

С перечисленных ключевых носителей уничтожена ключевая информация посредством: _____
(программы _____, разрезания, сжигания)

В журнале регистрации ключевых носителей сделаны соответствующие записи.

Пользователь_____ /_____/
«___» _____20__г.

Администратор информационной безопасности _____/_____
«___» _____20__г.