

**Частное образовательное учреждение  
дополнительного профессионального образования  
«Учебно-методический центр» Федерации профсоюзов Приморского края  
(ЧОУ ДПО УМЦ ФППК)**

**УТВЕРЖДАЮ**

Директор

\_\_\_\_\_ М.А.Воробьева

«\_\_\_» января 2023 г.

Приказ № \_\_\_ от \_\_\_\_\_ 2023 г.

**Порядок  
уничтожения, блокирования персональных данных  
Частного образовательного учреждения  
дополнительного профессионального образования  
«Учебно-методический центр» Федерации профсоюзов Приморского края**

Владивосток  
2023

## **1. Общие положения**

Настоящий Порядок определяет условия и способы:

- уничтожения бумажных носителей (документов), содержащих персональные данные по достижению цели обработки этих персональных данных;
- персональных данных в машинных носителях информации, в том числе персональных данных, и при необходимости самих машинных носителей информации.

## **2. Блокирование и уничтожение персональных данных, содержащихся в машинных носителях информации**

Блокирование информации, содержащей персональные данные субъекта персональных данных, производится в случаях:

- если персональные данные являются неполными, устаревшими, недостоверными;
- если сведения являются незаконно полученными или не являются необходимыми для заявленной оператором персональных данных цели обработки.

В случае подтверждения факта недостоверности персональных данных уполномоченное Оператором лицо на основании документов, представленных субъектом персональных данных, уполномоченным органом по защите прав субъектов персональных данных или полученных в ходе самостоятельной проверки, обязано уточнить персональные данные и снять их блокирование.

В случае выявления неправомерных действий с персональными данными уполномоченное Оператором лицо обязано устранить (организовать устранение) допущенные нарушения. В случае невозможности устранения допущенных нарушений необходимо в срок, не превышающий трех рабочих дней с даты выявления неправомерности действий с персональными данными, уничтожить персональные данные.

Об устранении допущенных нарушений или об уничтожении персональных данных уполномоченное Оператором лицо обязано уведомить субъекта персональных данных, а в случае, если обращение или запрос были направлены уполномоченным органом по защите прав субъектов персональных данных, также указанный орган.

Уполномоченное Оператором лицо обязано уничтожить персональные данные субъекта персональных данных в случаях:

- достижения цели обработки персональных данных оператор;
- отзыва субъектом согласия на обработку своих персональных данных.

Уничтожение персональных данных должно быть осуществлено в течение трех дней с указанных моментов. В согласии субъекта персональных данных на обработку его персональных данных могут быть установлены иные сроки уничтожения персональных данных при достижении цели обработки персональных данных. Уполномоченное Оператором лицо должно направить уведомление о факте уничтожения персональных данных субъекту персональных данных.

## **3. Работа с бумажными носителями (документами)**

3.1. Виды и периоды уничтожения бумажных носителей, содержащих персональные данные, представлены в таблице 1:

Таблица 1 Виды и периоды уничтожения бумажных носителей, содержащих

персональные данные

п/п	Документ	Срок хранения	Действия по окончании срока хранения
1.	Документы (сведения, содержащие персональные данные о работниках Оператора), переданные и сформированные при трудоустройстве работника.	75 лет	Уничтожение
2.	Документы об обучающихся (сведения, содержащие персональные данные обучающихся).	Установленные для данных документов сроки	Уничтожение
3.	Другие документы с грифом «Конфиденциально» и «Для служебного пользования» (Журналы учёта, списки доступа, эксплуатационная документация ит.п.)	хранятся до замены на новые, если не указан конкретный срок	Уничтожение

3.2 Документы, указанные в п. 3.1., должны находиться в сейфах, опечатываемых печатями сотрудника отдела кадров или учебной части. Исключение составляют документы, обрабатываемые в настоящий момент на рабочем месте.

3.3. По окончании срока хранения документы, указанные в п. 3.1., уничтожаются путём измельчения на мелкие части (или иным способом), исключающие возможность последующего восстановления информации или сжигаются.

#### 4. Работа с машинными носителями информации

Виды и периоды уничтожения персональных данных, хранимых в электронном виде («файлах») на жестком диске компьютера (далее – НЖМД) и машинных носителях: компакт дисках (далее – CD-R/RW, DVD-R/RW в зависимости от формата), дискетах 3,5“ 1.4Mb (далее – FDD), FLASH-накопителях.

*Пример видов и периодов уничтожения персональных данных, хранимых в электронном виде на НЖМД, представлен в таблице 2.*

Таблица 2 Виды и периоды уничтожения персональных данных, хранимых в электронном виде на жестком диске компьютера

№п/п	Информация, вид носителя	Срок хранения	Действия по окончании срока хранения
1.	База данных автоматизированной информационной системы Оператора. Носитель: файлы на НЖМД сервера	До создания более актуальной копии	Повторное использование носителя для записи очередной резервной копии БД, в случае невозможности – уничтожение носителя; удаление архивных

			файлов с НЖМД
2.	База данных автоматизированной информационной системы «1С/Предприятие- Кадры». Носитель: файлы на НЖМД сервера	До создания более 1Сактуальной копии	Повторное использование носителя для записи очередной резервной копии БД, в случае невозможности – уничтожение носителя; удаление архивных файлов с НЖМД
3.	База данных автоматизированной информационной системы «1С/Бухгалтерия». Носитель: файлы на НЖМД сервера	До создания более 1Сактуальной копии	Повторное использование носителя для записи очередной резервной копии БД, в случае невозможности – уничтожение носителя; удаление архивных файлов с НЖМД

Машинные носители информации (за исключением НЖМД), перечисленные в п.п. 3.1. должны находиться в сейфе, опечатываемом печатью ответственного сотрудника (кроме формируемых или обрабатываемых в данный момент на рабочем месте).

По окончании указанных сроков хранения, машинные носители информации, подлежащие уничтожению, физически уничтожаются с целью невозможности восстановления и дальнейшего использования. Это достигается путём деформирования, нарушения единой целостности носителя или его сжигания.

Подлежащие уничтожению файлы, расположенные на жестком диске ПЭВМ, удаляются средствами операционной системы с последующим «очищением корзины».

В случае допустимости повторного использования носителя формата FDD, CD-RW, DVD-RW, FLASH применяется программное удаление («затирание») содержимого диска путём его форматирования с последующей записью новой информации на данный носитель.

## 5. Порядок оформления документов об уничтожении носителей

Уничтожение носителей, содержащих персональные данные, осуществляет специальная Комиссия, создаваемая приказом руководителя Оператора. Комиссию возглавляет руководитель службы информационной безопасности Оператора (*или иное уполномоченное лицо*). В состав Комиссии должен входить сотрудник отдела автоматизированных информационных систем и руководитель соответствующего подразделения Оператора.

В ходе процедуры уничтожения персональных данных носителей необходимо присутствие членов Комиссии, осуществляющей уничтожение персональных данных и иной конфиденциальной информации, находящейся на технических средствах.

Комиссия составляет и подписывает Акт (2экземпляра) об уничтожении носителей. В течение трёх дней после составления акты об уничтожении направляются на утверждение

руководителю Оператора. После утверждения один экземпляр Акта хранится в сейфе у руководителя соответствующего подразделения Оператора, второй экземпляр Акта хранится у руководителя службы информационной безопасности Оператора.

Факт уничтожения носителя с персональными данными фиксируется в «Журнале регистрации носителей информации, содержащих персональные данные и иную конфиденциальную информацию», где в графе «Дата и номер акта уничтожения» заносятся соответствующие данные. Данный журнал является документом конфиденциального характера и вместе с актами уничтожения хранится в сейфе.