****

* 1. 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.

* 1. 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.
1. **Работа с бумажными носителями (документами)**
	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 работникахОператора), переданные и сформированные при трудоустройстве работника. | 75 лет | Уничтожение |
| 2. | Документы об обучающихся (сведения, содержащие персональные данные обучающихся). | Установленные для данных документов сроки хранения | 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 |

* 1. Документы, указанные в п. 3.1., должны находиться в сейфах. Исключение составляют документы, обрабатываемые в настоящий момент на рабочем месте.
	2. 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.
1. **Работа с машинными носителями информации**

4.1. 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 компьютере

|  |  |  |  |
| --- | --- | --- | --- |
| № 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 «1 С Предприятие-Кадры».Носитель: файлы на НЖМД сервера | До создания более актуальной копии | Повторное использование носителя для записи очередной резервной копии БД, в -уничтожение носителя; удаление архивных файлов с НЖМД |
| 3. | База данных автоматизированной информационной системы «1 С Бухгалтерия».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 |

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

 4.3. 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.

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

4.4. 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.

1. **Порядок оформления документов об уничтожении носителей**

5.1. Уничтожение носителей, содержащих персональные данные, осуществляет специальная Комиссия, создаваемая приказом руководителя Оператора. Комиссию возглавляет руководитель службы информационной безопасности Оператора (пи иное уполномоченное лицо).

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

5.3. 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.

5.4. 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.