

## ПОРЯДОК

# ПОРЯДОК УНИЧТОЖЕНИЯ И БЛОКИРОВАНИЯ ПЕРСОНАЛЬНЫХ ДАННЫХ ГОСУДАРСТВЕННОГО БЮДЖЕТНОГО ОБЩЕОБРАЗОВАТЕЛЬНОГО УЧРЕЖДЕНИЯ СРЕДНЕЙ ОБЩЕОБРАЗОВАТЕЛЬНОЙ ШКОЛЫ № 51 ПЕТРОГРАДСКОГО РАЙОНА САНКТ-ПЕТЕРБУРГА

## 1. Общие положения

Настоящий Порядок определяет условия и способы уничтожения бумажных и машинных носителей (документов), содержащих персональные данные по достижению цели обработки этих персональных данных и персональных данных в машинных носителях информации, в том числе персональных данных, и при необходимости самих машинных носителей информации Государственного бюджетного общеобразовательного учреждения средней общеобразовательной школы № 51 Петроградского района Санкт-Петербурга (далее – ГБОУ), согласно Федеральному закону от 27.07.2006 г. № 152-ФЗ «О персональных данных».

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

2.1. 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.

2.2. В случае подтверждения факта недостоверности персональных данных уполномоченное ГБОУ 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.

2.3. В случае выявления неправомерных действий с персональными данными уполномоченное ГБОУ 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.

2.4. Об устранении допущенных нарушений или об уничтожении персональных данных уполномоченное ГБОУ 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.

2.5. Уполномоченное ГБОУ лицо обязано уничтожить персональные данные субъекта персональных данных в случаях:

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

2.6. 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 ГБОУ 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 ГБОУ), 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 и т.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

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, BD-R/RW в зависимости от формата), USB-FLASH накопителях, внешних жестких дисках.

Пример видов и периодов уничтожения персональных данных, хранимых в электронном виде на НЖМД, представлен в Таблице 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 ГБОУ «АИСУ ПАРАГРАФ». 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 ГБОУ «ИС ТБДУ «МЕТРО»». 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
3	База данных автоматизированной информационной системы ГБОУ «АС УНСД «ТОРИС»». 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, опечатываемом печатью ответственного сотрудника (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 CD-RW, DVD-RW, BD-RW, USB-FLASH, внешний жесткий диск применяется программное удаление («затирание») содержимого диска путём его форматирования с последующей записью новой информации на данный носитель.

## 5. Порядок оформления документов об уничтожении носителей

5.1. Уничтожение бумажных и машинных носителей (далее – носитель), содержащих персональные данные, осуществляет специальная Комиссия, создаваемая приказом руководителя ГБОУ. Комиссию возглавляет руководитель службы информационной безопасности ГБОУ (или иное уполномоченное лицо). В состав Комиссии должен входить

сотрудник отдела автоматизированных информационных систем и руководитель соответствующего подразделения ГБОУ.

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 (2 экземпляра) об уничтожении носителей (Приложение №1 – бумажные носители; Приложение №2 – машинные носители). В течение трёх дней после составления акты об уничтожении направляются на утверждение руководителю ГБОУ. После утверждения один экземпляр Акта хранится в сейфе у руководителя соответствующего подразделения ГБОУ, второй экземпляр Акта хранится у руководителя службы информационной безопасности ГБОУ.

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.

**ПОРЯДОК**  
**УНИЧТОЖЕНИЯ, БЛОКИРОВАНИЯ ПЕРСОНАЛЬНЫХ ДАННЫХ**  
**ГОСУДАРСТВЕННОГО БЮДЖЕТНОГО ОБЩЕОБРАЗОВАТЕЛЬНОГО**  
**УЧРЕЖДЕНИЯ СРЕДНЕЙ ОБЩЕОБРАЗОВАТЕЛЬНОЙ ШКОЛЫ № 51**  
**ПЕТРОГРАДСКОГО РАЙОНА САНКТ-ПЕТЕРБУРГА**

**6. Общие положения**

Настоящий Порядок определяет условия и способы уничтожения бумажных и машинных носителей (документов), содержащих персональные данные по достижению цели обработки этих персональных данных и персональных данных в машинных носителях информации, в том числе персональных данных, и при необходимости самих машинных носителей информации **Государственного бюджетного общеобразовательного учреждения средней общеобразовательной школы № 51 Петроградского района Санкт-Петербурга** (далее – ГБОУ), согласно Федеральному закону от 27.07.2006 г. № 152-ФЗ «О персональных данных».

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

2.1. 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.

2.2. В случае подтверждения факта недостоверности персональных данных уполномоченное ГБОУ 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.

2.3. В случае выявления неправомерных действий с персональными данными уполномоченное ГБОУ 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.

2.4. Об устранении допущенных нарушений или об уничтожении персональных данных уполномоченное ГБОУ 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.

2.5. Уполномоченное ГБОУ лицо обязано уничтожить персональные данные субъекта персональных данных в случаях:

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

2.6. 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 ГБОУ лицо должно направить уведомление о факте уничтожения персональных данных субъекту персональных данных.

## **8. 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 ГБОУ), 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 и т.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.

## **9. 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, BD-R/RW в зависимости от формата), USB-FLASH накопителях, внешних жестких дисках.

Пример видов и периодов уничтожения персональных данных, хранимых в электронном виде на НЖМД, представлен в Таблице 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 ГБОУ «АИСУ ПАРАГРАФ». 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 ГБОУ «ИС ТБДУ «МЕТРО»». 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
3	База данных автоматизированной информационной системы ГБОУ «АС УНСД «ТОРИС»». 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, опечатываемом печатью ответственного сотрудника (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 CD-RW, DVD-RW, BD-RW, USB-FLASH, внешний жесткий диск применяется программное удаление («затирание») содержимого диска путём его форматирования с последующей записью новой информации на данный носитель.

## 10. Порядок оформления документов об уничтожении носителей

5.1. Уничтожение бумажных и машинных носителей (далее – носитель), содержащих персональные данные, осуществляет специальная Комиссия, создаваемая приказом руководителя ГБОУ. Комиссию возглавляет руководитель службы информационной безопасности ГБОУ (или иное уполномоченное лицо). В состав Комиссии должен входить

сотрудник отдела автоматизированных информационных систем и руководитель соответствующего подразделения ГБОУ.

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 (2 экземпляра) об уничтожении носителей (Приложение №1 – бумажные носители; Приложение №2 – машинные носители). В течение трёх дней после составления акты об уничтожении направляются на утверждение руководителю ГБОУ. После утверждения один экземпляр Акта хранится в сейфе у руководителя соответствующего подразделения ГБОУ, второй экземпляр Акта хранится у руководителя службы информационной безопасности ГБОУ.

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.

**АКТ  
УНИЧТОЖЕНИЯ ИНФОРМАЦИИ  
НА БУМАЖНЫХ НОСИТЕЛЯХ ИНФОРМАЦИИ  
ГОСУДАРСТВЕННОГО БЮДЖЕТНОГО ОБЩЕОБРАЗОВАТЕЛЬНОГО  
УЧРЕЖДЕНИЯ СРЕДНЕЙ ОБЩЕОБРАЗОВАТЕЛЬНОЙ ШКОЛЫ № 51  
ПЕТРОГРАДСКОГО РАЙОНА САНКТ-ПЕТЕРБУРГА**

Комиссия, наделенная полномочиями приказом Государственного бюджетного общеобразовательного учреждения средней общеобразовательной школы №51 Петроградского района Санкт-Петербурга \_\_\_\_\_ от \_\_\_\_\_ № \_\_\_\_\_, в составе:

\_\_\_\_\_  
(должности, ФИО)

\_\_\_\_\_  
(должности, ФИО)

\_\_\_\_\_  
(должности, ФИО)

составила настоящий Акт о том, что информация, зафиксированная на перечисленных в нем бумажных носителях информации, подлежит уничтожению.

Учетный номер (при наличии)	Причина уничтожения носителя информации; уничтожение/обезличивания информации	Тип носителя информации	Производимая операция (уничтожение, обезличивание)	Дата	Примечание

Правильность произведенных записей в акте проверена.

Регистрационные данные на бумажных носителях информации перед их уничтожением сверены с записями в акте и полностью уничтожены путем

Отметки о стирании информации (уничтожении носителей информации) в учетных формах произведены.

Председатель комиссии:

Члены комиссии:

\_\_\_\_\_  
(ФИО) \_\_\_\_\_  
(подпись)

\_\_\_\_\_  
(ФИО) \_\_\_\_\_  
(подпись)

\_\_\_\_\_  
(ФИО) \_\_\_\_\_  
(подпись)

« \_\_\_\_ » \_\_\_\_\_ 20\_\_ г.

**АКТ  
УНИЧТОЖЕНИЯ ИНФОРМАЦИИ  
НА МАШИННЫХ НОСИТЕЛЕЙ ИНФОРМАЦИИ  
ГОСУДАРСТВЕННОГО БЮДЖЕТНОГО ОБЩЕОБРАЗОВАТЕЛЬНОГО  
УЧРЕЖДЕНИЯ СРЕДНЕЙ ОБЩЕОБРАЗОВАТЕЛЬНОЙ ШКОЛЫ № 51  
ПЕТРОГРАДСКОГО РАЙОНА САНКТ-ПЕТЕРБУРГА**

Комиссия, наделенная полномочиями приказом Государственного бюджетного общеобразовательного учреждения средней общеобразовательной школы №51 Петроградского района Санкт-Петербурга \_\_\_\_\_ от \_\_\_\_\_ № \_\_\_\_\_, в составе:

\_\_\_\_\_ (должности, ФИО)

\_\_\_\_\_ (должности, ФИО)

\_\_\_\_\_ (должности, ФИО)

составила настоящий Акт о том, что информация, зафиксированная на перечисленных в нем машинных носителях информации, подлежит уничтожению.

Учетный номер (при наличии)	Причина уничтожения носителя информации; стирания/обезличивания информации	Тип носителя информации	Производимая операция (стирание, уничтожение, обезличивание)	Дата	Примечание

Правильность произведенных записей в акте проверена.

Регистрационные данные на машинных носителях информации перед уничтожением с них информации, сверены с записями в акте, произведено уничтожение содержащейся на носителях информации путем

Отметки о стирании информации (уничтожении носителей информации) в учетных формах произведены.

Председатель комиссии:

Члены комиссии: \_\_\_\_\_ (ФИО) \_\_\_\_\_ (подпись)

\_\_\_\_\_ (ФИО) \_\_\_\_\_ (подпись)

\_\_\_\_\_ (ФИО) \_\_\_\_\_ (подпись)

« \_\_\_\_ » \_\_\_\_\_ 20\_\_ г.