

Утверждаю  
Директор Н.А. Попова  
Приказ № 134 от «08» 09 2011 г.

**Регламент  
резервного копирования персональных данных  
в МБОУ г.Шахты «Гимназия №10»**

**1. ТЕРМИНЫ И СОКРАЩЕНИЯ**

**Персональные данные (ПДн)** – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

**Оператор** – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке,

действия (операции), совершаемые с персональными данными.

**Обработка персональных данных** – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение,

использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

**Автоматизированная обработка персональных данных** – обработка персональных данных с помощью средств вычислительной техники.

**Распространение персональных данных** – действия, направленные на раскрытие персональных данных неопределенному кругу лиц.

**Предоставление персональных данных** - действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.

**Блокирование персональных данных** – временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных).

**Уничтожение персональных данных** – действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных.

**Обезличивание персональных данных** – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.

**Информационная система персональных данных (ИСПДн)** – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

**Трансграничная передача персональных данных** - передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

**Типовая информационная система** – информационная система, в которой требуется обеспечение только конфиденциальности персональных данных.

**Специальная информационная система** – информационная система, в которой вне зависимости от необходимости обеспечения конфиденциальности персональных данных требуется обеспечить хотя бы одну из характеристик безопасности персональных данных, отличную от конфиденциальности (защищенность от уничтожения, изменения, блокирования, а также иных несанкционированных действий).

## **2. ОБЩИЕ ПОЛОЖЕНИЯ**

Настоящий Регламент определяет порядок резервирования персональных данных

(далее – ПДн) в МБОУ г.Шахты «Гимназия №10» для последующего восстановления работоспособности информационных систем персональных данных (далее – ИСПДн) при полной или частичной потере информации, определение порядка восстановления персональных данных.

Ответственными за выполнение требований данного Регламента и реализацию указанных в нем процедур являются Администратор безопасности информационных систем персональных данных (далее – Администратор безопасности ИСПДн).

## **3. ПОРЯДОК РЕЗЕРВНОГО КОПИРОВАНИЯ**

### **МАССИВЫ ПЕРСОНАЛЬНЫХ ДАННЫХ, ПОДЛЕЖАЩИЕ РЕЗЕРВИРОВАНИЮ**

Резервному копированию подлежит информация, хранящаяся на серверах:

- базы данных;
- каталоги данных на файловых серверах;
- общие каталоги отделов и подразделений.

### **МЕТОДЫ И СПОСОБЫ СОЗДАНИЯ РЕЗЕРВНЫХ КОПИЙ**

Резервирование ПДн, хранящихся на серверах, осуществляется путем копирования резервируемой информации на магнитные ленты, RAID-массивы, магнитооптические накопители, съемные диски, дисковые накопители и облачные сервисы.

При резервировании ПДн, хранящихся на серверах, используются две стратегии резервирования:

□ *горячее резервирование (hotstandby)* – копирование данных основного сервера на резервный сервер при включенных сервисах автоматизированной системы, входящей в состав ИСПДн;

□ *холодное резервирование (standby backup)* – копирование данных основного сервера на резервный сервер при выключенных сервисах автоматизированной системы,

входящей в состав ИСПДн.

Используются следующие методы резервного копирования:

□ *полное резервирование* – периодически создается полная копия массивов данных;

□ *добавочное резервирование* – на первом этапе создается полная копия массивов данных, а на последующих этапах в данную копию вносятся изменения в соответствии с произошедшими изменениями.

Также используются следующие способы создания резервных копий:

□ *ручной* – резервные копии создаются простым копированием массивов данных ответственным работником;

□ *автоматизированный* – резервные копии создаются ответственным работником с использованием специализированного программного обеспечения;

□ *автоматический* – резервные копии создаются с использованием специализированного программного обеспечения в соответствии с предварительно настроенным расписанием.

Указанные методы могут использоваться как при создании резервных копий в соответствии с Планом резервного копирования ПДн, так и при создании резервных копий по запросу. Форма Плана приведена в Приложении 1 настоящего Регламента.

#### ПЛАН РЕЗЕРВНОГО КОПИРОВАНИЯ

В МБОУ г.Шахты «Гимназия №10» определены следующие режимы функционирования ИСПДн:

□ *штатный режим функционирования*, при котором клиентское, серверное программное обеспечение, технические средства пользователей и администратора системы обеспечивают возможность круглосуточного и ежедневного функционирования;

□ *аварийный режим функционирования*, при котором произошло нарушение функционирования одного или нескольких компонент программного и (или) технического обеспечения.

Резервное копирование ПДн в штатном режиме производится в соответствии с Планом резервного копирования ПДн.

На протяжении периода времени, когда ИСПДн находится в аварийном состоянии, осуществляется ежедневное полное копирование, подлежащее резервированию, с использованием средств файловых систем серверов, располагающих необходимыми объемами дискового пространства для ее хранения.

#### 4. УЧЕТ И ХРАНЕНИЕ РЕЗЕРВНЫХ КОПИЙ

Учету подлежат следующие типы носителей резервных копий:

- магнитные ленты;
- магнитооптические накопители;
- съемные диски;
- дисковые накопители.

#### ПОРЯДОК УЧЕТА РЕЗЕРВНЫХ КОПИЙ

Учет резервных копий, созданных автоматизированными средствами системы резервного копирования, производится в электронном журнале системы.

Резервные копии персональных данных маркируются следующим образом: <Название базы данных / каталога>\_<Дата и время резервной копии>.

Учет резервных копий, созданных вручную, осуществляется в Журнале восстановления, учета создания и использования резервных копий ПДн. с указанием даты, времени начала и окончания операций копирования или восстановления данных, а также с приведением комментариев в случае их необходимости. Также в Журнале резервного копирования учитывается:

- создание копии по запросу;
- полное копирование в случае возникновения аварийных ситуаций.

Форма Журнала представлена в Приложении 2 настоящего Регламента.

Ответственным за ведение Журнала является Администратор безопасности ИСПДн.

#### ПОРЯДОК ХРАНЕНИЯ РЕЗЕРВНЫХ КОПИЙ

Хранение носителей, содержащих ПДн, осуществляется в условиях, исключающих возможность хищения, изменения целостности или уничтожения содержащейся на них информации.

Носители резервных копий краткосрочного хранения хранятся в помещениях, доступ в которых ограничен.

Срок хранения резервных копий определяется согласно Плану резервного копирования. В случае необходимости долгосрочного хранения резервных копий по истечении 3 месяцев носители резервных копий перемещаются в сейфы, (металлические шкафы), запираемые на ключ или на отдельные сервера, для долгосрочного хранения, под ответственность Администратору безопасности ИСПДн.

Отметка о передаче носителей резервных копий для долгосрочного хранения резервных копий проставляется в Журнале восстановления, учета создания и использования резервных копий персональных данных.

Допускается повторное использование носителей резервных копий по истечении срока хранения ПДн.

### 5. КОНТРОЛЬ РЕЗЕРВНОГО КОПИРОВАНИЯ

Машинные носители, предназначенные для долгосрочного хранения информации, периодически проверяются на их пригодность и отсутствие сбойных секторов.

При появлении сбойных секторов на машинных носителях информация с этих носителей переносится на исправные. Неисправные носители уничтожаются согласно Регламента по учету, хранению и уничтожению носителей персональных данных.

Контроль результатов всех процедур резервного копирования осуществляется Администратором безопасности ИСПДн. В случае обнаружения ошибки в процессе резервного копирования выполняется повторное резервное копирование.

Администратором безопасности ИСПДн несет ответственность за корректное ведение Журнала восстановления, учета создания и использования резервных копий персональных данных.

## **6. ВОССТАНОВЛЕНИЕ ПЕРСОНАЛЬНЫХ ДАННЫХ**

Восстановление ПДн проводится в случае нарушения ее целостности вследствие несанкционированного доступа в систему, воздействия вирусов, программных ошибок, ошибок персонала, аппаратных сбоев и пр.

В случае необходимости восстановления ПДн из резервных копий Пользователь ИСПДн, который работает с этими данными, сообщает о случившемся своему руководителю.

Руководитель Пользователя ИСПДн оформляет запрос в форме служебной записки или электронной заявки и направляет ее Администратору безопасности ИСПДн. В заявке должны быть указаны:

- данные, которые необходимо восстановить;
- дата и время, по состоянию на которые должны быть восстановлены данные;
- желательный срок восстановления;
- описание причины, по которой произошла потеря персональных данных (ошибка пользователя, программный сбой и т.п.).

В зависимости от обстоятельств, по которым произошло нарушение целостности ПДн, Администратор безопасности ИСПДн принимает решение о необходимости полного или частичного восстановления потерянных данных.

Кроме того, Администратор безопасности ИСПДн, получив запрос на восстановление данных, принимает решение о реагировании на данный инцидент в соответствии с Регламентом по проведению контрольных мероприятий и реагированию на инциденты информационной безопасности.

Администратор безопасности ИСПДн несет ответственность за восстановление утраченных данных. Восстановление данных осуществляется в максимально сжатые сроки, ограниченные техническими возможностями системы, но не более трех рабочих дней.

Факт восстановления ПДн регистрируется в Журнале восстановления, учета создания и использования резервных копий ПДн.

## **7. ПЕРЕСМОТР И ВНЕСЕНИЕ ИЗМЕНЕНИЙ**

Пересмотр положений настоящего документа проводится в следующих

случаях:

- на регулярной основе, но не реже одного раза в полгода;
- при появлении новых требований к обработке и обеспечению безопасности персональных данных со стороны российского законодательства и контролирующих органов исполнительной власти РФ;
- по результатам проверок контролирующих органов исполнительной власти Российской Федерации, выявивших несоответствия требованиям по обеспечению безопасности ПДн;
- по результатам внутреннего контроля (аудита) системы защиты ПДн в случае выявления существенных нарушений;
- по результатам расследования инцидентов информационной безопасности, связанных с обработкой и обеспечением безопасности ПДн и выявивших недостатки в правилах предоставления доступа ПДн.

Пересмотр и внесение изменений в настоящий документ регламентируется Регламентом по проведению контрольных мероприятий и реагированию на инциденты информационной безопасности.

Ответственным за пересмотр настоящего Регламента является Администратор безопасности ИСПДн.

Внесение изменений производится на основании соответствующего приказа по школе.

## ПРИЛОЖЕНИЕ 1

### Форма плана резервного копирования персональных данных

#### ПЛАН резервного копирования персональных данных

№ п/п	Наименование резервируемой информации	Периодичность	Место хранения
1	Персональные данные субъектов	ежемесячно	Каб. №44
2	Технологическая информация ИСПДн (профили пользователей, регистрационная и служебная информация)	ежемесячно	Каб. №44
3	Рабочие копии установочных компонент программного обеспечения рабочих станций (операционные системы, штатное и специальное программное обеспечение, программные средства защиты)	ежемесячно	Каб. №44





муниципальное бюджетное общеобразовательное учреждение  
г. Шахты Ростовской области  
«Гимназия №10 имени В.М. Шаповалова»

## ЖУРНАЛ

восстановления, учета создания и использования резервных копий  
персональных данных

Журнал начат \_\_\_\_\_

Журнал завершен \_\_\_\_\_

Ответственный \_\_\_\_\_

На \_\_\_\_\_ листах

