



Учебный центр «Перспектива-Уфа»

[www.ufa.perspekt174.ru](http://www.ufa.perspekt174.ru)

450061 Республика Башкортостан  
г. Уфа, ул. Александра Невского, д 20  
телефон: 8 (347) 21-45-241  
E-mail: Ezhova.A@perspekt174.ru


ИНН 0277942354 / КПП 027701001/ ОГРН  
1190280038200

Р/с 40702810929320001350 в АО "АЛЬФА-БАНК" К/с  
30101810200000000824 / БИК 042202824

УТВЕРЖДАЮ

Директор ООО

«УЦ «Перспектива-Уфа»

 / В.С. Макаров

«25» сентября 2024 г.



## РЕГЛАМЕНТ РЕЗЕРВНОГО КОПИРОВАНИЯ И ВОССТАНОВЛЕНИЯ ИНФОРМАЦИИ В ИСПДН

г. Уфа, 2024 г.

## 1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящий Регламент проведения резервного копирования и восстановления информации в информационных системах персональных данных (далее – ИСПДн), автоматизированных рабочих местах и серверах ООО «УЦ Перспектива-Уфа» (далее – Учреждение) разработан с целью:

1.1.1. определения порядка резервирования данных для последующего восстановления работоспособности информационной системы персональных данных (далее – ИСПДн) Учреждения при полной или частичной потере информации, вызванной сбоями или отказами аппаратного или программного обеспечения, ошибками пользователей, чрезвычайными обстоятельствами (пожаром, стихийными бедствиями и т.д.);

1.1.2. определения порядка восстановления информации в случае возникновения такой необходимости;

1.1.3. упорядочения работы должностных лиц, связанной с резервным копированием и восстановлением информации.

1.2. В настоящем документе регламентируются действия при выполнении следующих мероприятий:

1.2.1. резервное копирование;

1.2.2. контроль резервного копирования;

1.2.3. хранение резервных копий;

1.2.4. полное или частичное восстановление данных и приложений.

1.3. Резервному копированию подлежат информация следующих основных категорий:

1.3.1. персональные данные субъектов;

1.3.2. персональная информация пользователей (личные каталоги на файловых серверах);

1.3.3. групповая информация пользователей (общие каталоги отделов);

1.3.4. информация, необходимая для восстановления серверов и систем управления базами данных;

1.3.5. персональные профили пользователей сети;

1.3.6. информация автоматизированных систем, в т.ч. базы данных;

1.3.7. рабочие копии установочных компонент программного обеспечения рабочих станций;

1.3.8. регистрационная информация системы информационной безопасности.

1.4. Машинным носителям информации, содержащим резервную копию, присваивается маркировка в соответствии с «Инструкцией по учету машинных носителей и регистрации их выдачи».

## 2. ПОРЯДОК РЕЗЕРВНОГО КОПИРОВАНИЯ

2.1. Состав и объем копируемых данных, периодичность проведения резервного копирования определяется «Перечнем резервируемых данных» (*Приложение №1*). Максимальный срок хранения резервных копий 3 (три) месяца.

2.2. Система резервного копирования должна обеспечивать производительность, достаточную для сохранения информации, указанной в Перечне резервируемых данных, в установленные сроки и с заданной периодичностью. «Методика проведения резервного копирования» описана в *Приложении №2*.

2.3. О выявленных попытках несанкционированного доступа к резервируемой информации, а также иных нарушениях информационной безопасности, произошедших в процессе резервного копирования, должно быть немедленно сообщено администратору безопасности ИСПДн, либо ответственному за обеспечение безопасности персональных данных Учреждения.

### **3. КОНТРОЛЬ РЕЗУЛЬТАТОВ РЕЗЕРВНОГО КОПИРОВАНИЯ**

**3.1.** Контроль результатов всех процедур резервного копирования осуществляется администратором безопасности ИСПДн.

**3.2.** На протяжении периода времени, когда система резервного копирования находится в аварийном состоянии, должно осуществляться ежедневное копирование информации, подлежащей резервированию, с использованием средств файловых систем серверов, располагающих необходимыми объемами дискового пространства для ее хранения.

### **4. РОТАЦИЯ НОСИТЕЛЕЙ РЕЗЕРВНОЙ КОПИИ**

**4.1.** Система резервного копирования должна обеспечивать возможность периодической замены (выгрузки) резервных носителей без потерь информации на них, а также обеспечивать восстановление текущей информации ИСПДн в случае отказа любого из устройств резервного копирования. Все процедуры по загрузке, выгрузке носителей из системы резервного копирования, а также их перемещение, осуществляются администратором безопасности ИСПДн. В качестве новых носителей допускается повторно использовать те, у которых срок хранения содержащейся информации истек.

**4.2.** Носители с персональными данными, которые перестали использоваться в системе резервного копирования, должны стираться (форматироваться) с использованием специального программного обеспечения.

### **5. ВОССТАНОВЛЕНИЕ ИНФОРМАЦИИ ИЗ РЕЗЕРВНОЙ КОПИИ**

**5.1.** В случае необходимости, восстановление данных из резервных копий производится на основании заявки пользователя ИСПДн. Процедура восстановления информации из резервной копии осуществляется в соответствии с Методикой восстановления информации (*Приложение №3*). После поступления заявки, восстановление данных осуществляется в максимально сжатые сроки, ограниченные техническими возможностями системы, но не более одного рабочего дня.

**ПЕРЕЧЕНЬ РЕЗЕРВИРУЕМОЙ ДАННЫХ**

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

### **МЕТОДИКА РЕЗЕРВНОГО КОПИРОВАНИЯ**

1. Для организации системы резервного копирования используются стандартные средства операционной системы.
2. Существует еженедельная копия. Срок хранения: три месяца.  
Копии хранятся на внешнем НЖМД.
3. Различаются два принципиально разных источника информации, подлежащей резервированию:
  - Информация, хранимая непосредственно в файловой системе - MS Windows.
  - Базы данных ИСПДн.
4. Для резервирования информации, хранимой в базах данных ИСПДн Учреждения, в качестве промежуточного звена автоматизации используются средства конфигурирования ИСПДн и архиваторы. В результате работы промежуточного звена автоматизации формируется каталог с резервной копией данных ИСПДн.

### **МЕТОДИКА ВОССТАНОВЛЕНИЯ РЕЗЕРВИРУЕМЫХ ДАННЫХ**

Любое восстановление информации выполняется на основании заявки пользователя администратору безопасности ИСПДн или в случае необходимости восстановления утерянной или поврежденной информации, подлежащей резервированию. В процессе восстановления резервной копии следует руководствоваться инструкциями по восстановлению информации из резервных копий, описанных в документации, прилагающейся к системе резервного копирования ПО.