ПРИЛОЖЕНИЕ 11
к распоряжению администрации
Белоярского района
от 16 августа 2016 года № 262-р

# РЕГЛАМЕНТ
# организации резервного копирования и восстановления данных

## I. Общие положения

1.1. Настоящий Регламент резервного копирования и восстановления данных, хранящихся на серверах и автоматизированных рабочих местах администрации Белоярского района разработан в соответствии с требованиями Приказа ФСТЭК России от 18.02.2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

1.2. Настоящий Регламент разработан с целью:

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

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

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

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

1.3.1. резервное копирование;

1.3.2. контроль резервного копирования;

1.3.3. хранение резервных копий;

1.3.4. полное или частичное восстановление данных и приложений.

1.4. Если резервирование предполагает выгрузку на съемные носители информации, то такие носители должны учитываться в порядке, установленном «Инструкцией администратора безопасности информационных систем персональных данных».

## II. Термины и определения

2.1. **Автоматизированное рабочее место (АРМ)** – персональный компьютер и подключенные к нему периферийные устройства – принтер, многофункциональные устройства, сканеры и т.д.

2.2. **Информация** – сведения (сообщения, данные) независимо от формы их представления *(Федеральный закон от 27.07.2006 N 149-ФЗ «Об информации, информационных технологиях и о защите информации»)*

2.3. **Информационная система персональных данных (ИСПДн)** – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств *(ст. 3 ФЗ РФ от 27.07.2006 г. N 152-ФЗ «О персональных данных»).*

2.4. **Носитель информации** – любой материальный объект или среда, используемый для хранения или передачи информации.

2.5. **Программное обеспечение** – все или часть программ, процедур, правил и соответствующей документации системы обработки информации *(ISO/IEC 2382-1:1993)*

2.6. **Персональные данные** – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных) (*ст. 3 ФЗ РФ от 27.07.2006 г. N 152-ФЗ «О персональных данных»).*

2.7. **Резервное копирование** – процесс создания копии данных на носителе (дисковом массиве, магнитной ленте и т. д.), предназначенном для восстановления данных в оригинальном месте их расположения в случае их повреждения или разрушения.

2.8. **Система резервного копирования** – совокупность программного и аппаратного обеспечения, выполняющая задачу резервного копирования информации.

2.9. **Субъект персональных данных** – физическое лицо, которое прямо или косвенно определено или определяемо с помощью персональных данных.

## III. Порядок резервного копирования

3.1. Резервному копированию подлежит информация следующих основных категорий:

3.1.1. базы данных, содержащие персональные данные субъектов;

3.2. Система резервного копирования должна обеспечивать производительность, достаточную для сохранения информации, в установленные сроки и с заданной периодичностью.

3.3. 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 администрации Белоярского района.

3.4. Организация системы резервного копирования осуществляется штатными средствами Windows.

3.5. Существуют следующие наборы резервных копий:

3.5.1. Месячный набор. Записывается информация на первое число текущего месяца. Срок хранения – 1 (Один) месяц.

3.5.2. Недельная копия. Записывается в ночь на среду и в ночь на субботу. Срок хранения – субботняя копия – до следующей среды, вторничная копия – до субботы.

3.5.3. Суточная копия. Записывается ежедневно в 12:00. Срок хранения – сутки.

3.6. Копии хранятся на жестком диске.

3.7. Для резервирования информации, хранимой непосредственно в файловых системах, используются штатные средства Windows.

3.8. Для резервирования информации, хранимой в базах данных, в качестве промежуточного звена автоматизации используются средства конфигурирования ИСПДн и архиваторы. В результате работы промежуточного звена автоматизации формируется каталог с резервной копией данных ИСПДн. Посредством штатных средств Windows формируются задания на проведение резервного копирования этого каталога.

3.9. При резервировании информации следует руководствоваться инструкциями, описанными в документации, прилагающейся к системе резервного копирования.

## IV. Контроль результатов резервного копирования

4.1. Контроль результатов всех процедур резервного копирования осуществляется администратором безопасности ИСПДн.

4.2. 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 её хранения.

## V. Ротация носителей резервной копии

5.1. 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.

5.2. Носители с персональными данными, которые перестали использоваться в системе резервного копирования, должны стираться (форматироваться) с использованием специального программного обеспечения, реализующим полное физическое уничтожение данных.

## VI. Восстановление информации из резервной копии

6.1. В случае необходимости, восстановление данных из резервных копий производится на основании заявки пользователя ИСПДн. После поступления заявки, восстановление данных осуществляется в максимально сжатые сроки, ограниченные техническими возможностями системы, но не более 1 (одного) рабочего дня.

6.2. Любое восстановление информации выполняется на основании заявки пользователя администратору безопасности ИСПДн или в случае необходимости восстановления утерянной или повреждённой 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.