



Совет депутатов Вачского муниципального округа Нижегородской области

РАСПОРЯЖЕНИЕ

от 27.01.2023 г.

№ 15-х

Об утверждении Правил резервного копирования и восстановления информации, содержащей персональные данные, обрабатываемые с использованием средств вычислительной техники в Совете депутатов Вачского муниципального округа Нижегородской области

В соответствии с требованиями Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных», постановления Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»:

1. Утвердить прилагаемые Правила резервного копирования и восстановления информации, содержащей персональные данные, обрабатываемые с использованием средств вычислительной техники в Совете депутатов Вачского муниципального округа Нижегородской области.

2. Настоящее распоряжение вступает в силу со дня его подписания.

3. Контроль за исполнением настоящего распоряжения оставляю за собой.

Председатель Совета депутатов

С.Е. Липов

УТВЕРЖДЕНЫ
распоряжением Совета депутатов
Вачского муниципального округа
Нижегородской области
от 27.01.2023 года № 15-х

ПРАВИЛА

резервного копирования и восстановления информации, содержащей персональные данные, обрабатываемые с использованием средств вычислительной техники в Совете депутатов Вачского муниципального округа Нижегородской области

1. Основные понятия, термины и определения

Информация – сведения (сообщения, данные) независимо от формы их представления;

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

Автоматизированная обработка персональных данных – обработка персональных данных с помощью средств вычислительной техники;

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

2. Общие положения

Настоящие Правила определяют порядок резервного копирования и восстановления информации, содержащей персональные данные, обрабатываемой с использованием средств вычислительной техники.

Настоящие Правила разработаны на основании требований Федерального закона от 19 декабря 2005 г. № 160-ФЗ «О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных», Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных», постановления Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» и иных нормативных правовых актов Российской Федерации.

Требования настоящих Правил распространяются на работников, в функциональные обязанности которых входит резервирование и восстановление информации, содержащей персональные данные, обрабатываемой с использованием средств вычислительной техники.

Настоящие Правила о резервном копировании и восстановлении информации, содержащей персональные данные, обрабатываемой с использованием средств вычислительной техники, разработано с целью:

- определения порядка резервного копирования информации, содержащей персональные данные для последующего восстановления работоспособности информационных систем персональных данных при полной или частичной потере информации, содержащей персональные данные, вызванной сбоями или отказами аппаратного или программного обеспечения, ошибками пользователей, чрезвычайными обстоятельствами (пожаром, стихийными бедствиями и т.д.);

- определения порядка восстановления информации, содержащей персональные данные в случае возникновения такой необходимости;

- упорядочения работы должностных лиц, связанной с резервным копированием и восстановлением информации, содержащей персональные данные.

В настоящем документе регламентируются действия ответственных лиц при выполнении следующих мероприятий:

- резервное копирование;
- контроль резервного копирования;
- хранение резервных копий; полное или частичное восстановление данных и приложений.

Резервному копированию подлежит информация, обрабатываемая в информационных системах персональных данных, содержащая персональные данные физических лиц (субъектов персональных данных).

Машинным носителям информации, содержащим резервную копию, присваивается степень конфиденциальности, соответствующая той, к которой отнесены персональные данные.

3. Порядок резервного копирования

Резервное копирование информации, содержащей персональные данные, производится на основании следующих данных:

- максимальный срок хранения резервных копий – 10 лет;
- хранение 4-х следующих архивов;
- архив, сделанный на текущий день;
- архив на конец текущей недели;
- архив на 1-е число текущего месяца;
- архив, сделанный на конец года.

Резервное копирование информации, содержащей персональные данные, производится Администратором информационной системы персональных данных.

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

Технология создания резервных копий определяется правилами эксплуатации технических и программных средств.

Для создания резервных копий данных могут использоваться жесткие диски серверов и ПЭВМ, сменные (съёмные) носители информации, зарегистрированные в соответствии с правилами работы с документами, содержащими информацию ограниченного доступа.

Носители созданных резервных копий данных должны быть промаркированы Администратором информационной системы персональных данных. Маркировка должна содержать номер копии, дату ее создания, наименование информационной системы персональных данных.

При создании резервных копий допускается их архивирование специальными программными средствами.

4. Контроль результатов резервного копирования

Контроль результатов всех процедур резервного копирования осуществляется совместно Администратором информационной системы персональных данных и Администратором информационной безопасности, в срок до 17 часов рабочего дня, следующего за установленной датой выполнения этих процедур.

В случае обнаружения ошибки при осуществлении резервного копирования, лица, ответственные за контроль результатов, осуществляют все необходимые действия по устранению ошибки. При необходимости резервное копирование осуществляется повторно.

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.

5. Замена носителей резервной копии

Система резервного копирования должна обеспечивать возможность периодической замены (выгрузки) резервных носителей без потерь информации на них, а также обеспечивать восстановление текущей информации информационных систем персональных данных в случае отказа любого из устройств резервного копирования.

В случае необходимости замены испорченных носителей информации новыми, Администратор информационной системы персональных данных заблаговременно за 10 рабочих дней согласовывает спецификации новых носителей информации с Администратором информационной безопасности.

Все процедуры по загрузке, выгрузке носителей из системы резервного копирования, а также их перемещение осуществляются Администратором информационной системы персональных данных по запросу и в присутствии Администратора информационной безопасности.

В качестве новых носителей допускается повторно использовать те, у которых срок хранения содержащейся информации истек.

Конфиденциальная информация с носителей, которые перестают использоваться в системе резервного копирования, должна быть гарантированно уничтожена. Для гарантированного уничтожения информации допускается использование специального программного обеспечения.

Для хранения носителей резервных копий должны использоваться хранилища, создающие оптимальные условия для физической сохранности и защиты от воздействия неблагоприятных факторов.

6. Восстановление информации из резервных копий

Основанием для инициирования процедуры восстановления служит мотивированная заявка руководителя структурного подразделения на имя Администратора информационной безопасности. Восстановление данных производится после согласования с Администратором информационной безопасности.

После согласования заявки, восстановление данных осуществляется в максимально сжатые сроки, ограниченные техническими возможностями системы.

Восстановление данных из резервной копии осуществляется Администратором информационной системы персональных данных на специализированных рабочих местах, оснащенных необходимыми техническими средствами.

Восстановление утраченных данных производится из резервной копии, обеспечивающей минимальную потерю данных, содержащихся в информационном ресурсе.

7. Методика резервного копирования

С целью оптимизации расходов на развертывание системы резервного копирования, запись резервной копии осуществляется на внешний отчуждаемый носитель.

С помощью используемого ПО выполняются такие действия, как задание режимов и составление расписания резервного копирования клиентов, осуществляются операции по загрузке и выгрузке носителей информации, проводится контроль за состоянием выполнения заданий, запускаются процедуры восстановления информации.

Для снижения совокупной нагрузки на информационную систему все операции по резервированию информации необходимо проводить в вечернее время (на окончание рабочего дня). Резервные копии записываются ежедневно до 17 часов. Срок хранения – 10 лет. Резервные копии хранятся на внешнем отчуждаемом носителе, определенных для решения этой задачи, установленных в помещениях администрации Вачского муниципального округа Нижегородской области.

Источником информации, подлежащей резервированию, являются базы данных информационных систем персональных данных.

В результате работы встроенных средств формируется каталог с резервной копией данных информационной системы.
