Приложение 4

к приказу **[ОРГАНИЗАЦИЯ]**

от «\_\_\_» \_\_\_\_\_\_\_\_\_\_ 202\_ г. № \_\_\_\_\_\_

**ИНСТРУКЦИЯ**

**по организации резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации**

**в информационных системах персональных данных**

**[ОРГАНИЗАЦИЯ]**

1. **Термины и определения**
2. Автоматизированное рабочее место – программно-технический комплекс, предназначенный для автоматизации деятельности определенного вида.
3. Информационная система персональных данных – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.
4. 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.
5. Конфиденциальность информации – обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя.
6. Персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).
7. Пользователь информационной системы персональных данных – работник, осуществляющий обработку персональных данных в информационной системе персональных данных.
8. Средство антивирусной защиты – программное средство, реализующее функции обнаружения компьютерных программ либо иной компьютерной информации, предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты информации, а также реагирования на обнаружение этих программ и информации.
9. Средство защиты информации – программное обеспечение, программно-аппаратное обеспечение, аппаратное обеспечение, вещество или материал, предназначенные или используемые для защиты информации.
10. **Общие положения**
11. Настоящая Инструкция по организации резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации в информационных системах персональных данных **[ОРГАНИЗАЦИЯ]** (далее – Инструкция) устанавливает основные требования к организации резервного копирования (восстановления) программ и данных, хранящихся в базах данных информационных систем персональных данных (далее – ИСПДн) **[ОРГАНИЗАЦИЯ]** (далее – Учреждение), а также к резервированию аппаратных средств.
12. Настоящая Инструкция разработана с целью:
* определения категории информации, подлежащей обязательному резервному копированию;
* определения процедуры резервирования данных для последующего восстановления работоспособности ИСПДн при полной или частичной потере информации, вызванной сбоями или отказами аппаратного или программного обеспечения, ошибками пользователей, чрезвычайными обстоятельствами (пожаром, стихийными бедствиями и т.д.);
* определения порядка восстановления информации в случае возникновения такой необходимости;
* упорядочения работы и определения ответственности должностных лиц, связанной с резервным копированием и восстановлением информации.
1. Действие настоящей Инструкции распространяется на всех пользователей ИСПДн Учреждения, а также на основные системы обеспечения непрерывности работы и восстановления ресурсов при возникновении аварийных ситуаций, в том числе:
* системы жизнеобеспечения технических средств;
* системы обеспечения отказоустойчивости;
* системы резервного копирования и хранения данных;
1. Под резервным копированием информации понимается создание избыточных копий защищаемой информации в электронном виде для быстрого восстановления работоспособности ИСПДн в случае возникновения аварийной ситуации, повлекшей за собой повреждение или утрату данных.
2. Резервному копированию подлежит информация следующих основных категорий:
* информация, обрабатываемая пользователями в ИСПДн, а также информация, необходимая для восстановления работоспособности ИСПДн, в т.ч. систем управления базами данных (далее – СУБД) общего пользования и справочно-информационных систем общего использования;
* рабочие копии установочных компонентов программного обеспечения общего назначения и специализированного программного обеспечения серверов и рабочих станций;
* информация, необходимая для восстановления систем управления базами данных ИСПДн, локальной вычислительной сети, системы электронного документооборота;
* регистрационная информация систем защиты информации;
* другая информация ИСПДн, по мнению пользователей, администраторов ИСПДн и ответственного за обеспечение безопасности персональных данных (далее – ПДн) в ИСПДн, являющаяся критичной для работоспособности ИСПДн.
1. Настоящая Инструкция является дополнением к действующим локальным нормативным актам (внутренним документам) по вопросам обеспечения безопасности сведений конфиденциального характера, в том числе и ПДн, и не исключает обязательного выполнения их требований.
2. **Общие требования к резервному копированию**
3. В Инструкции резервного копирования описываются действия при выполнении следующих мероприятий:
* резервное копирование с указанием конкретных резервируемых данных и аппаратных средств (в случае необходимости);
* контроль резервного копирования;
* хранение резервных копий;
* полное или частичное восстановление данных.
1. **Ответственность за состояние резервного копирования**
2. Ответственность за контроль над своевременным осуществлением резервного копирования и соблюдением соответствующей Инструкции, а также за выполнением требований по хранению резервных копий и предотвращению несанкционированного доступа к ним возлагается на ответственного за обеспечение безопасности ПДн в ИСПДн и администраторов ИСПДн.
3. В случае обнаружения попыток несанкционированного доступа к носителям резервной информации, а также иных нарушениях информационной безопасности, произошедших в процессе резервного копирования, сообщается ответственному за обеспечение безопасности ПДн в ИСПДн в течение рабочего дня после обнаружения указанного события.
4. **Периодичность резервного копирования**
5. Резервное копирование специализированного программного обеспечения производится при его получении (если это предусмотрено инструкцией по его применению и не противоречит условиям его распространения), а также при его обновлении и получении исправленных и обновленных версий.
6. Информация, содержащаяся в постоянно изменяемых базах данных, сохраняется в соответствии со следующим графиком:
* ежедневно проводится копирование измененной и дополненной информации (носители с ежедневной информацией должны храниться в течение недели);
* еженедельно проводится резервное копирование всей базы данных (носители с еженедельными копиями хранятся в течение месяца);
* ежемесячно производится резервное копирование на специально выделенный носитель длительного хранения, информация на котором хранится постоянно.
1. Не реже одного раза в год на носители длительного хранения записывается информация, не относящаяся к постоянно изменяемым базам данных (приказы, распоряжения, открытые издания и т.д.).
2. **Восстановление информации из резервных копий**
3. В случае необходимости, восстановление данных из резервных копий производится ответственными работниками.
4. Восстановление данных из резервных копий происходит в случае ее исчезновения или нарушения вследствие несанкционированного доступа в систему, воздействия вирусов, программных ошибок, ошибок работников и аппаратных сбоев.
5. Восстановление системного программного обеспечения и программного обеспечения общего назначения производится с их носителей в соответствии с инструкциями производителя.
6. Восстановление специализированного программного обеспечения производится с дистрибутивных носителей или их резервных копий в соответствии с инструкциями по установке или восстановлению данного программного обеспечения.
7. Восстановление информации, не относящейся к постоянно изменяемым базам данных, производится с резервных носителей. При этом используется последняя копия информации.
8. При частичном нарушении или исчезновении записей баз данных восстановление производится с последней ненарушенной ежедневной копии. Полностью информация восстанавливается с последней еженедельной копии, которая затем дополняется ежедневными частичными резервными копиями.
9. **Срок действия и порядок внесения изменений**
10. Настоящая Инструкция вступает в силу с момента ее утверждения и действует бессрочно.
11. Настоящая Инструкция подлежит пересмотру не реже одного раза в три года.
12. Изменения и дополнения в настоящую Инструкцию вносятся приказом Директора Учреждения.