Приложение 12
к приказу МБУ ДО «ЦДОД»
от «08» декабря 2022 г. № 105

ИНСТРУКЦИЯ
по организации резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации в информационных системах персональных данных МБУ ДО «ЦДОД»

1. Термины и определения

1.1. Автоматизированное рабочее место – программно-технический комплекс, предназначенный для автоматизации деятельности определенного вида.
1.2. Информационная система персональных данных – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.
1.3. 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.
1.4. Конфиденциальность информации – обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя.
1.5. Персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).
1.6. Пользователь информационной системы персональных данных – работник, осуществляющий обработку персональных данных в информационной системе персональных данных.
1.7. 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.
1.8. Средство защиты информации – программное обеспечение, программно-аппаратное обеспечение, аппаратное обеспечение, вещество или материал, предназначенные или используемые для защиты информации.

2. Общие положения

2.1. Настоящая Инструкция по организации резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации в информационных системах персональных данных МБУ ДО «ЦДОД» (далее – Инструкция) устанавливает основные требования к организации резервного копирования (восстановления) программ и данных, хранящихся в базах данных информационных систем персональных данных (далее – ИСПДн) МБУ ДО «ЦДОД» (далее – Учреждение), а также к резервированию аппаратных средств.
2.2. 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.

2.3. 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;

2.4. 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.

2.5. 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 серверов и 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.

2.6. 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.

3. Общие требования к резервному копированию

3.1. 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.

3.2. Архивное копирование резервируемой информации производится при помощи специализированных программно-аппаратных систем резервного копирования. Система резервного копирования должна обеспечить производительность,

достаточную для сохранения информации, указанной в п. 2.5, в установленные сроки и с заданной периодичностью.

3.3. Требования к техническому обеспечению систем резервного копирования:
- комплекс взаимосвязанных технических средств на единой технологической платформе, обеспечивающих процессы сбора, передачи, обработки и хранения информации;
- имеет возможность расширения (замены) состава технических средств, входящих в комплекс, для улучшения их эксплуатационно-технических характеристик по мере возрастания объемов обрабатываемой информации;
- обеспечивает выполнение функций, перечисленных в п. 3.1.

3.4. Требования к программному обеспечению систем резервного копирования:
- лицензионное системное программное обеспечение и программное обеспечение резервного копирования;
- программное обеспечение резервного копирования обеспечивает простоту процесса инсталляции, конфигурирования и сопровождения.

3.5. Хранение отдельных магнитных носителей архивных копий организуется в отдельном хранилище. Физический доступ к архивным копиям строго ограничен.

3.6. Доступ к носителям архивных копий имеют только уполномоченные работники, которые несут персональную ответственность за сохранность архивных копий и невозможность ознакомления с ними лиц, не имеющих на то полномочий.

3.7. Уничтожение отделяемых магнитных носителей архивных копий производится установленным порядком в случае прихода их в негодность или замены типа носителя с обязательным составлением акта об уничтожении.

4. Ответственность за состояние резервного копирования

4.1. Ответственность за контроль над своевременным осуществлением резервного копирования и соблюдением соответствующей Инструкции, а также за выполнением требований по хранению архивных копий и предотвращению несанкционированного доступа к ним возлагается на ответственного за обеспечение безопасности ПДн в ИСПДн и администраторов ИСПДн.

4.2. В случае обнаружения попыток несанкционированного доступа к носителям архивной 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.

5. Периодичность резервного копирования

5.1. 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.

5.2. Резервное копирование открытой информации делается не позднее чем через сутки после ее изменения, но не реже одного раза в месяц.

5.3. 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.

5.4. 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.).

6. Восстановление информации из резервных копий

6.1. В случае необходимости, восстановление данных из резервных копий производится ответственными работниками.

6.2. 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.

6.3. Восстановление системного программного обеспечения и программного обеспечения общего назначения производится с их носителей в соответствии с инструкциями производителя.

6.4. Восстановление специализированного программного обеспечения производится с дистрибутивных носителей или их резервных копий в соответствии с инструкциями по установке или восстановлению данного программного обеспечения.

6.5. Восстановление информации, не относящейся к постоянно изменяемым базам данных, производится с резервных носителей. При этом используется последняя копия информации.

6.6. 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.

7. Срок действия и порядок внесения изменений

7.1. Настоящая Инструкция вступает в силу с момента ее утверждения и действует бессрочно.

7.2. Настоящая Инструкция подлежит пересмотру не реже одного раза в три года.

7.3. Изменения и дополнения в настоящую Инструкцию вносятся приказом Директора Учреждения.