Согласовано
Председатель профкома:
_____ Касаткина О.В.
Протокол № 11 от 29.08.2014г.

Утверждаю
Директор МОУ Иванковской СОШ:
_____ Г.В. Жаренова
Приказ № 175 от 01.09.2014г

ИНСТРУКЦИЯ ПО ОРГАНИЗАЦИИ РЕЗЕРВНОГО КОПИРОВАНИЯ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ

1. Общие положения

1.1. Настоящая Инструкция устанавливает основные требования к организации резервного копирования (восстановления) программ и данных, хранящихся в АРМ, а также к резервированию аппаратных средств.

1.2. Настоящая Инструкция разработана с целью:

- определения категории информации, подлежащей обязательному резервному копированию;
- определения процедуры резервирования данных для последующего восстановления работоспособности информационных систем 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.

1.3. Под резервным копированием информации понимается создание избыточных копий защищаемой информации в электронном виде для быстрого восстановления работоспособности информационных систем персональных данных (ИСПДн) в случае возникновения аварийной ситуации, повлекшей за собой повреждение или утрату данных.

1.4. Резервному копированию подлежит информация следующих основных категорий:

- персональная информация пользователей (личные каталоги) и групповая информация (общие каталоги подразделений) на файловых серверах;
- информация, обрабатываемая пользователями в ИСПДн, а также информация, необходимая для восстановления работоспособности ИСПДн, в т.ч. систем управления базами данных (СУБД) общего пользования и справочно-информационные системы общего использования;
- рабочие копии установочных компонент программного обеспечения общего назначения и специализированного программного обеспечения ИСПДн, СУБД, серверов и рабочих станций;
- информация, необходимая для восстановления серверов и систем управления базами данных ИСПДн, локальной вычислительной сети, системы электронного документооборота;
- регистрационная информация системы информационной безопасности ИСПДн;
- другая информация ИСПДн, по мнению пользователей и Администратора безопасности информации, являющаяся критичной для работоспособности ИСПДн.

1.5. Для каждой ИСПДн разрабатывается отдельный Регламент резервного копирования в зависимости от следующих требований:

- состав и объем копируемых данных, необходимая периодичность проведения резервного копирования (по форме, приведенной в Приложении № 1);
- максимальный срок хранения резервных копий;
- требований к надежности и защищенности хранения резервных копий;
- требований к резервируемым аппаратным средствам ИСПДн (при необходимости, в случае предъявления высоких требований к обеспечению доступности данных, обрабатываемых в

ИСПДн и значительного ущерба Учреждению при нарушении заданных характеристик безопасности ПДн).

Допускается составление одного Регламента для нескольких ИСПДн в случае идентичности требований к их резервированию.

1.6. Машинным носителям информации, содержащим резервную копию, присваивается гриф конфиденциальности по наивысшему грифу содержащихся на них сведений.

1.7. Резервные копии хранятся вне пределов серверного помещения, доступ к резервным копиям ограничен. К носителям информации, содержащим резервные копии, а также к резервируемым программным и аппаратным средствам допускаются только работники Учреждения, указанные в Списке лиц, имеющих доступ к резервируемым программным и аппаратным средствам ИСПДн (форма приведена в Приложении № 2). Список лиц формируется на основании письменной Заявки руководителя подразделения, согласованной с Администратором безопасности информационной системы персональных данных (далее - Администратор безопасности ИСПДн). Изменение прав доступа к резервируемым техническим средствам, массивам и носителям информации производится на основании Заявки руководителя подразделения, согласованной с Администратором безопасности ИСПДн .

О выявленных попытках несанкционированного доступа к резервируемой информации и аппаратным средствам, а также иных нарушениях ИБ, произошедших в процессе резервного копирования, сообщается директору Учреждения служебной запиской в течение рабочего дня после обнаружения указанного события.

2. Общие требования к резервному копированию

2.1. В Регламенте 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.

2.2. Архивное копирование резервируемой информации производится при помощи специализированных программно-аппаратных систем резервного копирования, программный и аппаратный состав которых обеспечивает выполнение требования к резервному копированию, приведенные в п. 1.5. Система резервного копирования обеспечивает производительность, достаточную для сохранения информации, указанной в п. 1.4, в установленные сроки и с заданной периодичностью.

2.3. Требования к техническому обеспечению систем резервного копирования:

- это комплекс взаимосвязанных технических средств, обеспечивающих процессы сбора, передачи, обработки и хранения информации, основывающийся на единой технологической платформе;
- 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. 2.1;
- средства вычислительной техники отвечают действующим на момент сертификации российским и международным стандартам и рекомендациям.

2.4. 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.

2.5. Сопровождение системы резервного копирования возлагается на Администратора информационной системы персональных данных (далее – Администратор информационной

системы), который обязан следить за работоспособностью программных и аппаратных средств, осуществляющих архивное копирование, в соответствии с инструкцией по эксплуатации.

2.6. Предварительный учет магнитных носителей архивных копий производится в отдельном журнале учета магнитных носителей для архивного копирования, который находится у Администратора безопасности ИСПДн (форма журнала приведена в Приложении № 3). Все магнитные носители с архивными копиями маркируются, на них указывается предназначение носителя.

В случае неотделимости носителей архивной информации от системы резервного копирования допускается их не маркировать и учитывать всю систему как одно целое.

2.7. Хранение отдельных магнитных носителей архивных копий организуется в отдельном от используемых данных помещении. Физический доступ к архивным копиям строго ограничен.

Контроль за физическим доступом возлагается на Администратора безопасности ИСПДн.

2.8. Доступ к носителям архивных копий имеют только Администратор безопасности ИСПДн и и Администратор информационной системы, которые несут персональную ответственность за сохранность архивных копий и невозможность ознакомления с ними лиц, не имеющих на то права.

2.9. Магнитные носители для архивных копий изымаются для работы только работником, непосредственно осуществляющим резервное копирование, под роспись в журнале учета магнитных носителей архивных копий. Передача магнитных носителей с архивными копиями кому бы то ни было, без документального оформления не допускается.

2.10. Уничтожение отделяемых магнитных носителей архивных копий производится установленным порядком в случае прихода их в негодность или замены типа носителя с обязательной записью в журнале их учета.

3. Ответственность за состояние резервного копирования

3.1. Ответственность за периодичность и полноту резервного копирования, а также состояние системы резервного копирования возлагается на Администратора информационной системы, осуществляющего резервное копирование.

3.2. Ответственность за контроль над своевременным осуществлением резервного копирования и соблюдением соответствующего Регламента, а также за выполнением требований по хранению архивных копий и предотвращению несанкционированного доступа к ним возлагается на Администратора безопасности ИСПДн.

3.3. В случае обнаружения попыток несанкционированного доступа к носителям архивной информации, а также иных нарушениях ИБ, произошедших в процессе резервного копирования, сообщается директору Учреждения служебной запиской в течение рабочего дня после обнаружения указанного события.

4. Периодичность резервного копирования

4.1. 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.

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

4.3. Информация (ПДн), содержащаяся в постоянно изменяемых базах данных Учреждения, сохраняется в соответствии со следующим графиком:

- ежедневно проводится копирование изменённой 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.

4.4. 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.).

5. Контроль результатов резервного копирования

5.1. Контроль результатов всех процедур резервного копирования осуществляется Администратором безопасности ИСПДн и Администратором информационной системы, в срок до 16 часов рабочего дня, следующего за установленной датой выполнения этих процедур. В случае обнаружения ошибки лицо, ответственное за контроль результатов, сообщает директору Учреждения до 17 часов текущего рабочего дня.

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

6. Ротация носителей резервной копии

6.1. Система резервного копирования обеспечивает 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.

6.2. Все процедуры по загрузке, выгрузке носителей из системы резервного копирования осуществляются Администратором информационной системы. В качестве новых носителей допускается повторно использовать те, у которых срок хранения содержащейся информации истек. Информация ограниченного доступа с носителей, которые перестают использоваться в системе резервного копирования, уничтожается.

7. Восстановление информации из резервных копий

7.1. В случае необходимости восстановление данных из резервных копий производится Администратором информационной системы.

7.2. Восстановление данных из резервных копий происходит в случае её исчезновения или нарушения вследствие несанкционированного доступа в систему, воздействия вирусов, программных ошибок, ошибок работников и аппаратных сбоев.

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

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

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

7.6. 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.

Принято на заседании общего собрания
работников МОУ Иванковской СОШ
Протокол № 1 от 27.08. 2014г

Приложение № 1

Перечень
резервируемой информации

№ п/п	Резервируемые ресурсы	Оценочный объем данных, Гб	Адрес хранения информации	Срок хранения резервной копии	Примечание*
1					
2					

* Описание резервируемой информации

Приложение № 2

Список
лиц, имеющих доступ к резервируемым программным и аппаратным средствам ИСПДн

№ п/п	Выполняемая роль	ФИО ответственного работника
1	Первоначальная настройка системы резервного копирования (создание медиа-сетов, расписаний, selection lists, оповещений). Запуск в промышленную эксплуатацию системы резервного копирования	
2	Внесение существенных изменений в настройку системы резервного копирования	
3	Анализ логов резервного копирования, отслеживание необходимости изменений настроек резервного копирования, обеспечение ротации носителей	
4	Ротация носителей, проверка корректности резервной копии, обеспечения хранения резервной копии вне офиса на случай катастрофы	

Приложение № 3

Журнал
учета магнитных носителей для архивного копирования информации

№ п/п	Носитель (маркировка)	Кому выдан (ФИО работника, должность, подразделение)	Получен (дата, подпись)	Возвращен (дата, подпись)	Уничтожен (причина, ФИО работника, должность, подразделение, дата, подпись)
1					
2					