

Муниципальное бюджетное общеобразовательное учреждение
для обучающихся с ограниченными возможностями здоровья
основная общеобразовательная школа № 10
г. Чебаркуля

Российская Федерация, 456440, г. Чебаркуль Челябинской области, ул. Мира 21 Б.

Телефон: (8-35168) 2-46-08

ПРИКАЗ

«18» 12 2020 г.

№ 169-д

Об организации работ по обеспечению
безопасности персональных данных

С целью организации работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных Муниципального бюджетного общеобразовательного учреждения для обучающихся с ограниченными возможностями здоровья основной общеобразовательной школы № 10 (далее - Учреждение) в соответствии с требованиями Федерального Закона РФ «О персональных данных» от 27.07.2006 №152-ФЗ

ПРИКАЗЫВАЮ:

1. Назначить ответственным за организацию обработки персональных данных в Учреждении заместителя директора по учебно-воспитательной работе Баженову Ольгу Петровну.
2. Возложить на Баженову Ольгу Петровну следующие обязанности:
 - 2.1. представление на утверждение списка лиц, доступ которых к персональным данным необходим для выполнения служебных (трудовых) обязанностей, а также изменений к нему;
 - 2.2. организацию работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных;
 - 2.3. проведение разбирательств по фактам несоблюдения условий хранения носителей персональных данных, нарушения правил работы с техническими и программными средствами информационной системы, в том числе со средствами защиты информации, или по другим нарушениям, которые могут привести к несанкционированному доступу к персональным данным;
 - 2.4. приостановку предоставления персональных данных пользователям информационной системы при обнаружении нарушений порядка обработки персональных данных.
3. Назначить администратором безопасности информационных систем персональных данных системного администратора Зозуленко Сергея Владимировича.
4. В рамках проведения работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных возложить на Зозуленко С.В. следующие функции:
 - 4.1. учёт лиц, допущенных к работе с персональными данными в информационных системах Учреждения;
 - 4.2. учёт съёмных машинных носителей, используемых для хранения и передачи сведений, составляющих персональные данные в соответствии с «Инструкцией администратора безопасности ИСПДн»;
 - 4.3. администрирование средств и систем защиты информации в информационных системах персональных данных.
5. Ответственному за организацию обработки персональных данных в срок до 30.12.2020 подготовить и представить на утверждение «Список лиц, доступ которых к персональным данным необходим для выполнения служебных обязанностей».

6. Ответственному за организацию обработки персональных данных организовать учет носителей персональных данных.

7. Использование для хранения и обработки персональных данных машинных носителей информации, не поставленных на учет в установленном порядке, ЗАПРЕЩАЕТСЯ.

8. С целью проведения классификации информационных систем персональных данных создать комиссию в составе:

Председатель: заместитель заведующего по УВР – Баженова О.П.

Члены комиссии: делопроизводитель – Глинских О.В..

Председатель профкома – Лягинова И.В.

Комиссии в срок до 30.12.2020 осуществить классификацию информационных систем персональных данных, эксплуатирующихся в учреждении.

9. Работы по обеспечению безопасности персональных данных проводить в соответствии с «Планом мероприятий по защите персональных данных» (Приложение).

10. Приказ довести до всех сотрудников Учреждения.

11. Контроль исполнения приказа ~~оставляю~~ за собой.

Директор школы:



Е.А.Кривоносова

С приказом ознакомлены

Муниципальное бюджетное общеобразовательное учреждение
для обучающихся с ограниченными возможностями здоровья
основная общеобразовательная школа № 10
г. Чебаркуля

Российская Федерация, 456440, г. Чебаркуль Челябинской области, ул. Мира 21 Б.
Телефон: (8-35168) 2-46-08



Утверждаю
Директор МБОУ ООШ № 10
Е.А.Кривоносова
Приказ от 18.12.2020 г. №169-д

Политика
обработки и защиты персональных данных МБОУ ООШ № 10
I. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. В целях гарантирования выполнения норм федерального законодательства в полном объеме **Муниципальное бюджетное общеобразовательное учреждение для обучающихся с ограниченными возможностями здоровья основной общеобразовательной школы № 10** (далее – **Оператор**) считает своими задачами соблюдение принципов законности, справедливости и конфиденциальности при обработке персональных данных, а также обеспечение безопасности процессов их обработки.

1.2. Настоящая политика в области обработки и защиты персональных данных в МБОУ ООШ № 10 Чебаркульского городского округа (далее – **Политика**) характеризуется следующими признаками:

1.2.1. Разработана в целях обеспечения реализации требований законодательства РФ в области обработки персональных данных субъектов персональных данных.

1.2.2. Раскрывает основные категории персональных данных, обрабатываемых Оператором, цели, способы и принципы обработки Оператором персональных данных, права и обязанности Оператора при обработке персональных данных, права субъектов персональных данных, а также включает перечень мер, применяемых Оператором в целях обеспечения безопасности персональных данных при их обработке.

1.2.3. Является общедоступным документом, декларирующим концептуальные основы деятельности Оператора при обработке персональных данных.

II. ИНФОРМАЦИЯ ОБ ОПЕРАТОРЕ

2.1. Наименование: **Муниципальное бюджетное общеобразовательное учреждение для обучающихся с ограниченными возможностями здоровья основной общеобразовательной школы № 10**

2.2. ИНН: 7420004353

2.3. Фактический адрес:
456440, Челябинская область, г. Чебаркуль, ул. Мира, 21-Б;

456440, Челябинская область, г. Чебаркуль, ул. Электростальская, 36-Б;
Тел.: 8(35168)24608;24478

2.4. Сайт: <http://school10-cheb.ucoz.ru/>

III. ПРАВОВЫЕ ОСНОВАНИЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

3.1. Политика Оператора в области обработки персональных данных определяется со следующими основными нормативными правовыми актами РФ:

- 3.1.1. Конституцией Российской Федерации.
- 3.1.2. Трудовым кодексом Российской Федерации.
- 3.1.3. Гражданским кодексом российской Федерации.
- 3.1.4. Федеральным законом от 19.12.2005 №160-ФЗ «О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных».
- 3.1.5. Федеральным законом от 27.07.2006 №152-ФЗ «О персональных данных».
- 3.1.6. Федеральным законом от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации».
- 3.1.7. Федеральным законом от 29.12.2012 №273-ФЗ «Об образовании в Российской Федерации».
- 3.1.8. Федеральным законом от 27.07.2010 № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг».
- 3.1.9. Постановлением Правительства РФ от 10 июля 2013 г. №582 «Об утверждении правил размещения на официальном сайте образовательной организации в информационно-коммуникационной сети «интернет» и обновления информации об образовательной организации».
- 3.1.10. Постановлением Правительства РФ от 01 ноября 2012 г. №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» и др.

3.2. Во исполнение настоящей Политики руководящим органом Оператора утверждены следующие локальные нормативные правовые акты:

- 3.2.1. Положение об **обработке** персональных данных с использованием **средств** автоматизации.
- 3.2.2. Положение об обработке персональных данных без использования средств автоматизации.
- 3.2.3. Инструкция ответственного за организацию обработки персональных данных.
- 3.2.4. Инструкция администратора безопасности ИСПДн.

- 3.2.5. Инструкция пользователя ИСПДн.
- 3.2.6. Инструкция о порядке работы с персональными данными.
- 3.2.7. Инструкция по организации антивирусной защиты.
- 3.2.8. Инструкция по организации парольной защиты.
- 3.2.9. Форма обязательства о неразглашении информации ограниченного доступа.
- 3.2.10. Форма согласия сотрудников на обработку персональных данных.
- 3.2.11. Форма согласия кандидата на вакансию на обработку персональных данных
- 3.2.12. Форма согласия родителей (законных представителей) на обработку персональных данных.
- 3.2.13. Форма согласия практиканта на обработку персональных данных.
- 3.2.14. Журнал учета обращений субъектов персональных данных.
- 3.2.15. Журнал учета ключей от помещений и хранилищ.
- 3.2.16. Журнал учета машинных носителей информации.
- 3.2.17. Журнал учета работ в информационных системах персональных данных и др.

IV. ЦЕЛИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

4.1. Оператор обрабатывает персональные данные исключительно в следующих целях:

4.1.1. Заключение и выполнения обязательств по трудовым договорам.

4.1.2. Осуществления возложенных на МБОУ ООШ № 10 функций в соответствии с Положением, другими нормативными правовыми актами Российской Федерации, Ярославской области, подлежащими применению при осуществлении деятельности.

V. КАТЕГОРИИ ОБРАБАТЫВАЕМЫХ ПЕРСОНАЛЬНЫХ ДАННЫХ, ИСТОЧНИКИ ИХ ПОЛУЧЕНИЯ

5.1. В информационных системах персональных данных Оператора обрабатываются следующие категории персональных данных:

5.1.1. Персональные данные сотрудников.

5.1.2. Персональные данные обучающихся, их родителей (законных представителей).

VI. ОСНОВНЫЕ ПРИНЦИПЫ ОБРАБОТКИ, ПЕРЕДАЧИ И ХРАНЕНИЯ ПЕРСОНАЛЬНЫХ ДАННЫХ

6.1. Оператор в своей деятельности обеспечивает соблюдение принципов обработки персональных данных, указанных в ст.5 Федерального закона 152-ФЗ «О персональных данных».

6.2. Оператор не осуществляет обработку биометрических персональных данных (сведения, которые характеризуют физиологические и биологические особенности человека, на основании

которых можно установить его личность и которые используются Оператором для установления личности субъекта персональных данных).

6.3. Оператор выполняет обработку специальных категорий персональных данных, касающихся состояния здоровья.

6.4. Оператор не производит трансграничную (на территории иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу) передачу персональных данных.

6.5. Оператором созданы общедоступные источники персональных данных: официальный сайт школы.

VII. СВЕДЕНИЯ О ТРЕТЬИХ ЛИЦАХ, УЧАСТВУЮЩИХ В ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

7.1. В целях соблюдения законодательства РФ, для достижения целей обработки, а также в интересах и с согласия субъектов персональных данных Оператор в ходе своей деятельности предоставляет персональные данные следующим организациям:

7.1.1. Пенсионному фонду РФ;

7.1.2. Негосударственным пенсионным фондам;

7.1.3. Федеральной налоговой службе РФ;

7.1.4. ФБГУ «Федеральный центр тестирования»;

7.1.5. Федеральной службе по надзору в сфере образования и науки;

7.1.6. ПАО «Сбербанк России»;

7.1.7. ПАО «Челиндбанк»;

7.1.8. Управлению образования Чебаркульского городского округа;

7.1.9. АИС «Аттестация»;

7.1.10. АИС ГИА;

7.1.11. АИС «Образование Челябинской области»;

7.1.12. Централизованной бухгалтерии Управления образования Администрации Чебаркульского городского округа;

7.1.13. Центру занятости населения Чебаркульского городского округа;

7.1.14. Управлению социальной защиты населения Чебаркульского городского округа;

7.1.15. ГБУЗ ОБЛАСТНАЯ БОЛЬНИЦА Г. ЧЕБАРКУЛЯ и другим медицинским учреждениям;

7.1.16. Военному комиссариату Чебаркульского городского округа;

7.1.17. Учреждения дополнительного образования.

VIII. МЕРЫ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ОБРАБОТКЕ

8.1. Оператор при обработке персональных данных принимает все необходимые правовые, организационные и технические меры для их защиты от неправомерного или случайного доступа, уничтожения, изменения, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении них. Обеспечение безопасности персональных данных достигается, в частности, следующими способами:

8.1.1. Назначением ответственных за организацию обработки персональных данных.

8.1.2. Осуществлением внутреннего контроля и/или аудита соответствия обработки персональных данных ФЗ от 27.07.2006 №152-ФЗ «О персональных данных» и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, локальным актам.

8.1.3. Ознакомлением работников Оператора, непосредственно осуществляющих обработку персональных данных, с положениями законодательства РФ о персональных данных, в том числе с требованиями к защите персональных данных, локальными актами в отношении обработки персональных данных, и (или) обучением указанных сотрудников.

8.1.4. Определением угроз безопасности персональных данных при их обработке в информационных системах персональных данных.

8.1.5. Применением организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимых для выполнения требований к защите персональных данных.

8.1.6. Оценкой эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных.

8.1.7. Учетом машинных носителей персональных данных.

8.1.8. Выявлением фактов несанкционированного доступа к персональным данным и принятием соответствующих мер.

8.1.9. Восстановлением персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним.

8.1.10. Установлением правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечением регистрации и учета всех действий, совершаемых с персональными данными в информационной системе персональных данных.

8.1.11. Контролем за принимаемыми мерами по обеспечению безопасности персональных данных и уровнем защищенности информационной системы персональных данных.

IX. ПРАВА СУБЪЕКТОВ ПЕРСОНАЛЬНЫХ ДАННЫХ

9.1. Субъект персональных данных имеет право на получение сведений об обработке его персональных данных Оператором.

9.2. Субъект персональных данных вправе требовать от Оператора, который их обрабатывает, уточнения этих персональных данных, их блокирования или уничтожения в случае, если они являются неполными, устаревшими, неточными, незаконно полученными или не могут быть признаны необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

9.3. Право субъекта персональных данных на доступ к его персональным данным может быть ограничено в соответствии с федеральными законами.

9.4. Для реализации своих прав и защиты законных интересов субъект персональных данных имеет право обратиться к Оператору. Тот рассматривает любые обращения и жалобы со стороны субъектов персональных данных, тщательно расследует факты нарушений и принимает все необходимые меры для их немедленного устранения, наказания виновных лиц и урегулирования спорных и конфликтных ситуаций в досудебном порядке.

9.5. Субъект персональных данных вправе обжаловать действия или бездействие Оператора путем обращения в уполномоченный орган по защите прав субъектов персональных данных.

9.6. Субъект персональных данных имеет право на защиту своих прав и законных интересов, в том числе на возмещение убытков и/или компенсацию морального вреда в судебном порядке.

X. КОНТАКТНАЯ ИНФОРМАЦИЯ

10.1. Ответственным за организацию обработки персональных данных в МБОУ ООШ № 10 назначен – директор, Кривоносова Елена Александровна, ответственным за обеспечение безопасности обработки персональных данных (администратором безопасности ИСПДн) назначен – системный администратор, Зозуленко Сергей Владимирович, Уполномоченным органом по защите прав субъектов персональных данных является федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор), управление по защите прав субъектов персональных данных.

XI. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

11.1. Настоящая Политика является внутренним документом Оператора, общедоступной и подлежит размещению на официальном сайте Оператора.

11.2. Настоящая Политика подлежит изменению, дополнению в случае появления новых законодательных актов и специальных нормативных документов по обработке и защите персональных данных, но не реже одного раза в три года.

11.3. Контроль исполнения требований настоящей Политики осуществляется ответственным за организацию обработки персональных данных Оператора.

11.4. Ответственность должностных лиц Оператора, имеющих доступ к персональным данным, за невыполнение требований норм, регулирующих обработку и защиту персональных данных, определяется в соответствии с законодательством Российской Федерации и внутренними документами Оператора.

Приложение
к приказу МБОУ ООШ № 10
от 18.12.2020 года № 169-д
Директор школы: Крук Е.А. Кривоносова



Перечень персональных данных,
обрабатываемых в МБОУ ООШ № 10
в связи с реализацией трудовых отношений,
а также в связи с оказанием муниципальных услуг и
осуществлением муниципальных функций

N п/п	Наименование документов, содержащих персональные данные	Перечень персональных данных, используемых в документе	Регламентирующие документы	Цель обработки персональных данных
1	2	3	4	5
1.	Заявление о приеме на работу	Фамилия, имя, отчество	Трудовой кодекс РФ	Оформление трудового договора, приказа
2.	Трудовой договор	Фамилия, имя, отчество, паспортные данные или данные иного документа, удостоверяющего личность (серия, номер, дата выдачи, наименование органа, выдавшего документ, код подразделения), адрес места жительства (по паспорту)	Трудовой кодекс РФ	Оформление приказа
3.	Трудовые книжки работников ОУ	Фамилия, имя, отчество, дата рождения, образование, профессия, специальность, подпись владельца трудовой книжки, сведения о приеме на работу и переводах на другую должность и об увольнении (дата) с указанием причин и со ссылкой на статью, пункт закона, сведения о присвоении классного чина, сведения об аттестации руководителей ОУ, ДОУ, УДО, сведения о поощрениях и награждениях, дата и номер документа, на основании которого внесена запись	Трудовой кодекс РФ от 30.12.2001 № 197-ФЗ; Постановление Правительства РФ от 16.04.2003 N 225 (ред. от 25.03.2013) "О трудовых книжках" (вместе с "Правилами ведения и хранения трудовых книжек, изготовления бланков трудовой книжки и обеспечения ими работодателей")	Исполнение трудового договора, исполнение обязанностей, возложенных на организацию Трудовым Кодексом, Федеральными законами РФ

N п/п	Наименование документов, содержащих персональные данные	Перечень персональных данных, используемых в документе	Регламентирующие документы	Цель обработки персональных данных
1	2	3	4	5
4.	Личная карточка работника ОУ	<p>Фамилия, имя, отчество, дата и место рождения, гражданство, идентификационный номер налогоплательщика (ИНН), номер страхового свидетельства государственного пенсионного страхования, паспорт (серия, номер, дата выдачи, наименование органа выдавшего документ), адрес места жительства (по паспорту и фактический), дата регистрации по месту жительства, номер телефона;</p> <p>сведения о (об):</p> <ul style="list-style-type: none"> - образовании, квалификации и наличии специальных знаний или специальной подготовки; - послевузовском профессиональном образовании; - учёной степени; - знании иностранных языков и степени владения ими; - повышении квалификации и профессиональной переподготовке; - стаже работы; - состоянии в браке; - составе семьи (семьи (степени родства, ФИО, годе рождения); - воинском учете; - трудовой деятельности (характер и вид работы, прием на работу и переводы на другую работу; основании прекращения трудового договора (увольнения), номере и дате приказа об увольнении, дате увольнения); - присвоенном квалификационном разряде (до 2014 г.), классном чине; - аттестации и оценке работника; - государственных и ведомственных наградах, почетных званиях; - отпусках (ежегодных, учебных, без сохранении заработной платы и др.); - социальных льготах, на которые работник имеет право в соответствии с законодательством 	Трудовой кодекс РФ Постановление Госкомстата России от 05.01.2004 № 1	Оформление личной карточки работника ОУ

N п/п	Наименование документов, содержащих персональные данные	Перечень персональных данных, используемых в документе	Регламентирующие документы	Цель обработки персональных данных
1	2	3	4	5
5.	Приказы об оплате	Должностной оклад, доплаты и надбавки, премии (разовые, квартальные, по итогам полугодия и календарного года), материальная помощь	Трудовой кодекс РФ	Формирование заработной платы
6.	Листок нетрудоспособности	Фамилия, имя, отчество, страховой стаж, дата рождения, ИНН, номер страхового свидетельства государственного пенсионного страхования	Федеральный закон РФ от 29.12.2006 № 255-ФЗ «Об обязательном социальном страховании на случай временной нетрудоспособности и в связи с материнством»	Оплата труда работников в период нетрудоспособности
7.	Обращения граждан	Фамилия, имя, отчество, адрес проживания, E-mail, номер телефона и другие персональные данные, указанные в обращении	Федеральный закон РФ от 02.05.2006 № 59-ФЗ «О порядке рассмотрения обращения граждан РФ»	Рассмотрение обращения и подготовка ответа
8.	Справка о заработной плате и трудовом стаже	Фамилия, имя, отчество, адрес, номер телефона, место работы, периоды работы, должность	ФЗ от 22.10.2004 № 125-ФЗ «Об архивном деле в РФ»	Оформление пенсии работников
9.	Приказы МБОУ ООШ № 10	Ф.И.О., должность работника ОУ, Ф.И.О., должность руководителя ОУ и другие персональные данные, указанные в согласии на обработку персональных данных		Реализация функций ОУ
10.	Заявление о приеме в 1 класс ребенка	Ф.И.О, дата рождения ребенка, Ф.И.О., место жительства, паспортные данные родителя (законного представителя)	Федеральный закон от 29.12.2012 № 273-ФЗ «Об образовании в РФ» (ст. 67, ч.1)	Учет детей, подлежащих обучению
11.	Сведения об учащихся, зачисленных в ОУ, отчисленных из ОУ	Ф.И.О., дата рождения, место учебы учащегося	Федеральный закон от 29.12.2012 № 273-ФЗ «Об образовании в РФ» (ст. 9, ч.1, п.6)	Учет детей, подлежащих обучению по образовательным программам начального общего, основного общего образования
12.	Сведения о несовершеннолетних, не посещающих или систематически пропускающих по неуважительным причинам занятия в ОУ	Ф.И.О.	Федеральный закон от 24.06.1999 № 120-ФЗ «Об основах системы профилактики безнадзорности и правонарушений несовершеннолетних» (ст.14, ч.1 п. 4)	Учет несовершеннолетних, не посещающих или систематически пропускающих по неуважительным причинам занятия
13.	Информация о победителях и призерах конкурсов школьного уровня	Ф.И.О. учащегося, возраст	Приказы управления образования Чебаркульского городского округа	Подведение итогов конкурсов школьного уровня, составление списков победителей и призеров для церемонии награждения

N п/п	Наименование документов, содержащих персональные данные	Перечень персональных данных, используемых в документе	Регламентирующие документы	Цель обработки персональных данных
1	2	3	4	5
4.	Личная карточка работника ОУ	<p>Фамилия, имя, отчество, дата и место рождения, гражданство, идентификационный номер налогоплательщика (ИНН), номер страхового свидетельства государственного пенсионного страхования, паспорт (серия, номер, дата выдачи, наименование органа выдавшего документ), адрес места жительства (по паспорту и фактический), дата регистрации по месту жительства, номер телефона;</p> <p>сведения о (об):</p> <ul style="list-style-type: none"> - образовании, квалификации и наличии специальных знаний или специальной подготовки; - послевузовском профессиональном образовании; - учёной степени; - знании иностранных языков и степени владения ими; - повышении квалификации и профессиональной переподготовке; - стаже работы; - состоянии в браке; - составе семьи (семьи (степени родства, ФИО, годе рождения); - воинском учете; - трудовой деятельности (характер и вид работы, прием на работу и переводы на другую работу; основании прекращения трудового договора (увольнения), номере и дате приказа об увольнении, дате увольнения); - присвоенном квалификационном разряде (до 2014 г.), классном чине; - аттестации и оценке работника; - государственных и ведомственных наградах, почетных званиях; - отпусках (ежегодных, учебных, без сохранения заработной платы и др.); - социальных льготах, на которые работник имеет право в соответствии с законодательством 	Трудовой кодекс РФ Постановление Госкомстата России от 05.01.2004 № 1	Оформление личной карточки работника ОУ

N п/п	Наименование документов, содержащих персональные данные	Перечень персональных данных, используемых в документе	Регламентирующие документы	Цель обработки персональных данных
1	2	3	4	5
14.	Заявление на участие в основном государственном экзамене от учащегося 9 класса	Ф.И.О., серия и номер паспорта	<p>Федеральный закон от 29.12.2012 № 273-ФЗ «Об образовании в РФ» Постановление Правительства РФ от 31.08.2013 № 755 «О федеральной информационной системе обеспечения проведения государственной итоговой аттестации обучающихся, освоивших основные образовательные программы основного общего и среднего общего образования, и приема граждан в образовательные организации для получения среднего профессионального и высшего образования и региональных информационных системах обеспечения проведения государственной итоговой аттестации обучающихся, освоивших основные образовательные программы основного общего и среднего общего образования»</p> <p>Порядок проведения государственной итоговой аттестации по образовательным программам основного общего образования (приказ Минобрнауки РФ от 25.12.2013г. № 1394)</p>	Формирование муниципального сегмента ФИС и РИС
15.	Заявление на участие в государственном выпускном экзамене от учащегося 9 класса	Ф.И.О., серия и номер паспорта, справка о состоянии здоровья (МСЭ или заключение ПМПК)	<p>Федеральный закон от 29.12.2012 № 273-ФЗ «Об образовании в РФ» Постановление Правительства РФ от 31.08.2013 № 755 «О федеральной информационной системе обеспечения проведения государственной итоговой аттестации обучающихся, освоивших основные образовательные программы основного общего и среднего общего образования, и приема граждан в образовательные организации для получения среднего профессионального и высшего образования и региональных информационных системах обеспечения проведения государственной итоговой аттестации обучающихся, освоивших основные образовательные программы основного общего и среднего общего образования»</p> <p>Порядок проведения государственной итоговой аттестации по образовательным программам среднего общего образования (приказ Минобрнауки РФ от 26.12.2013г. № 1400)</p> <p>Порядок проведения государственной итоговой аттестации по образовательным программам основного общего образования (приказ Минобрнауки РФ от 25.12.2013г. № 1394)</p>	Формирование муниципального сегмента ФИС и РИС

N п/п	Наименование документов, содержащих персональные данные	Перечень персональных данных, используемых в документе	Регламентирующие документы	Цель обработки персональных данных
1	2	3	4	5
16.	Сведения о педагогах, выполняющих на едином государственном экзамене, основном государственном экзамене функции организаторов ППЭ	Ф.И.О., серия и номер паспорта, год рождения, уровень профессионального образования, квалификация, предметная специализация, должность, стаж работы	Федеральный закон от 29.12.2012 № 273-ФЗ «Об образовании в РФ» Постановление Правительства РФ от 31.08.2013 № 755 «О федеральной информационной системе обеспечения проведения государственной итоговой аттестации обучающихся, освоивших основные образовательные программы основного общего и среднего общего образования, и приема граждан в образовательные организации для получения среднего профессионального и высшего образования и региональных информационных системах обеспечения проведения государственной итоговой аттестации обучающихся, освоивших основные образовательные программы основного общего и среднего общего образования»	Формирование муниципального сегмента ФИС И РИС
17.	Протокол результатов государственной итоговой аттестации в форме ГВЭ	Ф.И.О., серия и номер паспорта, результаты ЕГЭ	Федеральный закон от 29.12.2012 № 273-ФЗ «Об образовании в РФ» Постановление Правительства РФ от 31.08.2013 № 755 «О федеральной информационной системе обеспечения проведения государственной итоговой аттестации обучающихся, освоивших основные образовательные программы основного общего и среднего общего образования, и приема граждан в образовательные организации для получения среднего профессионального и высшего образования и региональных информационных системах обеспечения проведения государственной итоговой аттестации обучающихся, освоивших основные образовательные программы основного общего и среднего общего образования»	Ознакомление участников единого государственного экзамена, их родителей с результатами экзаменов
18.	Информация о несчастных случаях с учащимися, воспитанниками учреждения образования в образовательном процессе, дорожно-транспортных происшествиях и несчастных случаях со смертельным исходом	Ф.И.О., год рождения (возраст) пострадавших, место учебы, медицинский диагноз, Ф.И.О. педагогов, учащихся и др. очевидцев, участников несчастных случаев	Приказ Гособразования СССР от 01.10.1990 № 639	Обеспечение контроля за расследованием несчастных случаев. Составление акта формы Н-2. Учет несчастных случаев, выполнение мероприятий по устранению причин несчастных случаев
19.	Акт формы Н-2	Ф.И.О., год рождения, место учебы, класс (группа), медицинское заключение о НС, Ф.И.О. педагогов, учащихся и др. очевидцев, участников НС	Приказ Гособразования СССР от 01.10.1990 № 639 (п.п. 1.4., 1.6., 2.4.2.)	Обеспечение контроля расследования несчастных случаев

N п/п	Наименование документов, содержащих персональные данные	Перечень персональных данных, используемых в документе	Регламентирующие документы	Цель обработки персональных данных
1	2	3	4	5
20.	Материалы расследований несчастных случаев	Ф.И.О. пострадавших, педагогов, учащихся и др. очевидцев, участников несчастных случаев	Приказ Гособразования СССР от 01.10.1990 № 639 (п.2.4.2.)	Обеспечение контроля расследования несчастных случаев, выполнение мероприятий по устранению причин несчастных случаев
21.	Информация для официального сайта МБОУ ООШ № 10	Фамилия, имя, отчество, место работы (учебы) и другая информация, указанная в согласии на обработку персональных данных		Размещение информации на официальном сайте МБОУ ООШ № 10

Муниципальное бюджетное общеобразовательное учреждение
для обучающихся с ограниченными возможностями здоровья
основная общеобразовательная школа № 10
г. Чебаркуля

Российская Федерация, 456440, г. Чебаркуль Челябинской области, ул. Мира 21 Б.
Телефон: (8-35168) 2-46-08

Приложение
К приказу по школе № 169-д
от 18.12.2020 года

**Правила
осуществления внутреннего контроля соответствия обработки
персональных данных требованиям к защите персональных данных, политике
оператора в отношении обработки персональных данных**

1. Настоящие правила определяют основания, форму и порядок осуществления в МБОУ ООШ № 10 (далее – Организация или Оператор) внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных и политике оператора в отношении обработки персональных данных, установленным Федеральным законом от 27.07.2006 №152-ФЗ «О персональных данных» (далее – Федеральный закон № 152-ФЗ) и принятыми в соответствии с ним нормативными правовыми актами.

2. Настоящие правила разработаны в соответствии с Федеральным законом № 152-ФЗ, постановлением Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» (далее – постановление Правительства № 1119).

3. Основные понятия и термины, используемые в настоящих правилах, применяются в значениях, определенных статьей 3 Федерального закона № 152-ФЗ.

4. Основанием для проведения внутреннего контроля являются требования Федерального закона № 152-ФЗ (часть 1, статья 18,1) и постановления Правительства № 1119 (п. 17).

5. Внутренний контроль осуществляется путем проведения проверок не чаще 1 раза в год.

6. Проверку проводит Комиссия, назначенная приказом директора Организация или на договорной основе юридическое лицо (индивидуальный предприниматель), имеющее лицензию на осуществление деятельности по технической защите конфиденциальной информации.

7. Состав Комиссии не менее 3-х человек, включая лицо, ответственное за организацию обработки персональных данных. Все члены комиссии при принятии решения обладают равными правами.

8. Комиссия при проведении проверки обязана:

- провести анализ реализации мер, направленных на обеспечение выполнения Оператором обязанностей, предусмотренных Федеральным законом от 27.07.2006 №152-ФЗ «О персональных данных» (ст.18.1, ст. 19) и принятыми в соответствии с ним локальными актами Оператора, определяющими его политику в отношении обработки персональных данных;

- провести анализ выполнения оператором требований по определению и обеспечению уровня защищенности персональных данных, утвержденных постановлением Правительства № 1119;

- провести анализ реализации Оператором организационных и технических мер по обеспечению безопасности персональных данных, утвержденных приказом ФСТЭК России от 18.02.2013г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

- провести анализ состава оборудования, программных средств, включая средства защиты, входящих в состав информационной системы персональных данных на соответствие Техническому паспорту информационной системы;

-своевременно и в полной мере исполнять предоставленные полномочия по предупреждению, выявлению и пресечению нарушений требований к защите персональных данных, установленных законодательными и нормативными актами РФ;

- при проведении проверки соблюдать законодательство РФ, права и законные интересы Оператора.

9. Комиссия при проведении проверки вправе:

-запрашивать и получать необходимые документы (сведения) для достижения целей проведения внутреннего контроля;

- получать доступ к информационным системам персональных данных в части касающейся ее полномочий;

- принимать меры по приостановлению или прекращению обработки персональных данных, осуществляемой с нарушением требований к защите персональных данных;

- вносить директору Организации предложения о привлечении к дисциплинарной ответственности лиц, виновных в нарушении требований к защите персональных данных, установленных законодательными и нормативными правовыми актами Российской Федерации.

10. При проведении проверки члены Комиссии не вправе:

- требовать представления документов и сведений, не относящихся к предмету проверки;

- распространять информацию и сведения конфиденциального характера, полученные при проведении проверки.

11. По результатам проверки составляется Акт проверки, который подписывается членами комиссии и представляется руководителю организации для принятия соответствующего решения.

12. В Акте отражаются сведения о результатах проверки, в том числе о выявленных нарушениях обязательных требований законодательных и нормативных правовых актов Российской Федерации в области защиты персональных данных, об их характере и о лицах, допустивших указанные нарушения.

13. Акт должен содержать заключение о соответствии или несоответствии обработки персональных данных требованиям к защите персональных данных и политике оператора в отношении обработки персональных данных, установленным Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами.

Муниципальное бюджетное общеобразовательное учреждение
для обучающихся с ограниченными возможностями здоровья
основная общеобразовательная школа № 10
г. Чебаркуля

Российская Федерация, 456440, г. Чебаркуль Челябинской области, ул. Мира 21 Б.
Телефон: (8-35168) 2-46-08

Утверждаю
Директор МБОУ ООШ № 10
М.А. Кривоносова Е.А. Кривоносова
(приказ от 18.12.2020 № 169 -д)



План
Проведения внутренних проверок режима защиты персональных данных
Информационной системы персональных данных

1. Общие положения

- 1.1. План внутренних проверок режима защиты персональных данных, содержит перечень внутренних проверок.
1.2. План составляется для мероприятий в соответствии с Положением об обработке ПД и определяет периодичность проведения проверок.
1.3. План внутренних проверок содержит следующую информацию:
-название проверяемого мероприятия;
-периодичность;
-исполнитель мероприятия;
1.4. План внутренних проверок распространяется на все информационные системы персональных данных Учреждения.

2. План внутренних проверок

Мероприятие	Периодичность	исполнитель
Контроль соблюдения режима обработки ПД	еженедельно	Ответственный за обработку и защиту ПД
Контроль соблюдения режима защиты ПД	ежедневно	Ответственный за обработку и защиту ПД
Контроль выполнения антивирусной защиты	еженедельно	Ответственный за обработку и защиту ПД
Контроль соблюдения режима защиты при подключении к сетям общего пользования и (или) международного обмена	еженедельно	Ответственный за обработку и защиту ПД
Проведение внутренних проверок на предмет выявления изменений в режиме обработки и защиты ПД	ежегодно	Ответственный за обработку и защиту ПД
Контроль обновления программного обеспечения и единообразия применяемого ПО на всех элементах ИСПД	еженедельно	Ответственный за обработку и защиту ПД
Контроль обеспечения резервного копирования	ежемесячно	Ответственный за обработку и защиту ПД
Организация анализа и пересмотра имеющихся угроз безопасности ПД, а	ежегодно	Ответственный за обработку и защиту ПД

также предсказание появления новых, еще неизвестных угроз		
Поддержание в актуальном состоянии систему защиты ПД	ежемесячно	Ответственный за обработку и защиту ПД
Контроль за разработкой и внесением изменений в программное обеспечение собственной разработки или штатное ПО специально дорабатываемое собственными разработчиками или сторонними организациями.	Ежемесячно	Ответственный за обработку и защиту персональных данных

Муниципальное бюджетное общеобразовательное учреждение
для обучающихся с ограниченными возможностями здоровья
основная общеобразовательная школа № 10
г. Чебаркуля

Российская Федерация, 456440, г. Чебаркуль Челябинской области, ул. Мира 21 Б.
Телефон: (8-35168) 2-46-08

Утверждаю
Директор МБОУ ООШ № 10
Е.А.Кривonosова
(приказ от 18.12.20 № 169-д)

Правила
Рассмотрения запросов субъектов персональных данных или их представителей

1. Настоящие Правила определяют порядок учета (регистрации), рассмотрения запросов субъектов персональных данных или их представителей в МБОУ ООШ № 10 (далее- Организация или Оператор).

2. Настоящие Правила разработаны в соответствии с Федеральным законом от 27.07.2006 г. № 152-ФЗ «О персональных данных» (далее Федеральный закон № 152-ФЗ), постановлением Правительства РФ от 15.09.2008г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

3. Основные понятия и термины, используемые в настоящих Правилах, применяются в значениях, определенных статьей 3 Федерального закона № 152-ФЗ.

4. Субъект персональных данных имеет право на получение информации в Учреждении, касающейся обработки его персональных данных (часть 7 статьи 14 Федерального закона № 152-ФЗ), в том числе содержащей:

- 1) подтверждение факта обработки его персональных данных Оператором;
- 2) правовые основания и цели обработки его персональных данных;
- 3) цели и применяемые Оператором способы обработки его персональных данных;
- 4) наименование и место нахождения Оператора, сведения о лицах (за исключением работников Оператора), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с Оператором или на основании федерального закона;
- 5) обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;
- 6) сроки обработки персональных данных, в том числе сроки их хранения;
- 7) порядок осуществления субъектом персональных данных прав, предусмотренных Федеральным законом № 152-ФЗ;
- 8) информацию об осуществленной или о предполагаемой трансграничной передаче данных;
- 9) наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению оператора, если обработка поручена или будет поручена такому лицу;
- 10) иные сведения, предусмотренные Федеральным законом № 152-ФЗ или другими федеральными законами.

5. Сведения, указанные в п. 4, должны предоставляться субъекту персональных данных или его представителю Оператором при обращении либо при получении запроса субъекта персональных данных или его представителя.

Запрос должен содержать номер основного документа, удостоверяющего личность субъекта персональных данных или его представителя, сведения о дате выдачи указанного документа и выдавшем его органе, сведения, подтверждающие участие субъекта

персональных данных в отношениях с Оператором, либо сведения, иным образом подтверждающие факт обработки персональных данных Оператором, подпись субъекта персональных данных или его представителя. Запрос может быть направлен в форме электронного документа и подписан электронной подписью в соответствии с законодательством Российской Федерации.

6. Сведения, указанные в п. 4, должны быть предоставлены субъекту персональных данных Оператором в доступной форме, и в них не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных, за исключением случаев, если имеются законные основания для раскрытия таких персональных данных.

7. Все поступившие запросы регистрируются в день их поступления. На запросе указывается входящий номер и дата регистрации.

8. Рассмотрение запросов и подготовка ответов осуществляется по поручению председателя Организации или его заместителей.

9. Организация приема и обработки запросов субъектов персональных данных или их представителей и (или) осуществление контроля приема и обработки таких обращений и запросов возлагается на лицо, ответственное за организацию обработки персональных данных в Организации (п. 3, часть 4, статья 22.1 Федерального закона №152-ФЗ).

10. Рассмотрение запросов и подготовку ответов могут осуществлять работники Организации, обрабатывающие персональные данные, в соответствии с их должностными инструкциями.

11. Ответы на запросы печатаются на официальном бланке Организации, согласовываются с ответственным за организацию обработки персональных данных, подписываются председателем или его заместителями и регистрируются.

Муниципальное бюджетное общеобразовательное учреждение
для обучающихся с ограниченными возможностями здоровья
основная общеобразовательная школа № 10
г. Чебаркуля

Российская Федерация, 456440, г. Чебаркуль Челябинской области, ул. Мира 21 Б.
Телефон: (8-35168) 2-46-08

Утверждаю
Директор МБОУ ООШ № 10
Кривеносова Е.А. Кривеносова
(приказ от 18.12.20 № 169 -д)

Правила
работы с обезличенными персональными данными в МБОУ ООШ № 10

1. Общие положения

Настоящие Правила работы с обезличенными персональными данными в МБОУ ООШ № 10 (Учреждение) разработаны с учетом требований Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных» и постановления Правительства РФ от 21.03.2012 г. № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных ФЗ «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами» и определяют порядок работы с обезличенными данными в Учреждении.

2. Термины и определения

В соответствии с Федеральным законом от 27.07.2006 г. № 152-ФЗ «О персональных данных» в настоящих Правилах используются следующие понятия:

- персональные данные- любая информация, относящаяся прямо или косвенно к определенному или определяемому физическому лицу (субъекту персональных данных);
- 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;
- обезличивание персональных данных- действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных.

3. Условия обезличивания

3.1. Обезличивание персональных данных может быть проведено с целью ведения статистических данных, снижения ущерба от разглашения защищаемых персональных данных, снижения класса информационных систем персональных данных Учреждения и по достижению целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

3.2. Способы обезличивания при условии дальнейшей обработки персональных данных:

- уменьшение перечня обрабатываемых сведений;
- замена части сведений идентификаторами;
- обобщение- понижение точности некоторых сведений;
- понижение точности некоторых сведений (например, «место жительства» может состоять из страны, индекса, города, улицы, дома и квартиры, а может быть указан только населенный пункт);
- деление сведений на части и обработка в разных информационных системах;
- другие способы.

3.3. Способом обезличивания в случае достижения целей обработки или в случае утраты необходимости в достижении этих целей является сокращение перечня персональных данных.

3.4. Директор школы принимает решение о необходимости обезличивания персональных данных.

4. ПОРЯДОК РАБОТЫ С ОБЕЗЛИЧЕННЫМИ ПЕРСОНАЛЬНЫМИ ДАННЫМИ

4.1. Обезличенные персональные данные не подлежат разглашению и нарушению конфиденциальности.

4.2. Обезличенные персональные данные могут обрабатываться с использованием и без использования средств автоматизации.

4.3. При обработке обезличенных персональных данных с использованием средств автоматизации необходимо соблюдение:

- инструкции по организации парольной защиты;
- инструкции по проведению антивирусного контроля;
- правил работы со съемными носителями (если они используются);
- правил резервного копирования;
- правил доступа в помещения, где расположены элементы информационных систем.

4.4. При обработке обезличенных персональных данных без использования средств автоматизации необходимо соблюдение:

- правил хранения бумажных носителей;
- правил доступа к ним и в помещения, где они хранятся.

Муниципальное бюджетное общеобразовательное учреждение
для обучающихся с ограниченными возможностями здоровья
основная общеобразовательная школа № 10
г. Чебаркуля

Российская Федерация, 456440, г. Чебаркуль Челябинской области, ул. Мира 21/Б.
Телефон: (8-35168) 2-46-08

Утверждаю
Директор МБОУ ООШ № 10
Кривоносова Е.А.
(приказ от 18.11.2020 № 169-д)

Положение

об обработке и обеспечении безопасности персональных данных, обрабатываемых в информационных системах персональных данных Муниципального бюджетного общеобразовательного учреждения для обучающихся с ограниченными возможностями здоровья основной общеобразовательной школы № 10

1. Общие положения

- 1.1. Настоящее Положение разработано в соответствии с Федеральным законом от 27.07.2006г. № 152 «О персональных данных», Положением об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденным Постановлением Правительства РФ от 01.11.2012г. № 1119, и Положением об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации, утвержденным Постановлением Правительства РФ от 15.09.2008г. № 687.
- 1.2. Настоящим Положением определяется порядок обработки и обеспечения безопасности персональных данных, обрабатываемых в информационных системах персональных данных с использованием средств автоматизации и без использования средств автоматизации в Муниципальном бюджетном общеобразовательном учреждении для обучающихся с ограниченными возможностями здоровья основной общеобразовательной школе № 10 (далее- Учреждение).
- 1.3. В настоящем Положении используются следующие понятия:
 - 1.3.1. Блокирование персональных данных- временное прекращение сбора, систематизации, накопления, использования, распространения персональных данных, в том числе их передачи.
 - 1.3.2. Информационная система персональных данных (далее- Информационная система)- информационная система, представляющая собой совокупность персональных данных, содержащаяся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств.
 - 1.3.3. Использование персональных данных- действия (операции) с персональными данными, совершаемые оператором в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта персональных данных или других лиц либо иным образом затрагивающих права и свободы субъекта персональных данных или других лиц.
 - 1.3.4. Конфиденциальность персональных данных- обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространения без согласия субъекта персональных данных или наличия иного законного основания.
 - 1.3.5. Обезличивание персональных данных- действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных.
 - 1.3.6. Обработка персональных данных- действия (операции) с персональными данными, включая сбор, систематизацию, накопление, использование, распространение(в том числе их передачу), обезличивание, блокирование, уничтожение персональных данных.
 - 1.3.7. Обработка персональных данных без использования средств автоматизации (далее – Неавтоматизированный способ) – действия с персональными данными, такие как сбор, систематизация, накопление, хранение, использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, осуществляются при непосредственном участии человека.

1.3.8. Общедоступные персональные данные – персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта персональных данных или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности.

1.3.9. Оператор – Учреждение, юридическое или физическое лицо, организующие и осуществляющие обработку персональных данных, а также определяющие цели и содержание обработки персональных данных.

1.3.10. Персональные данные – любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.

1.3.11. Распространение персональных данных – действия, направленные на передачу персональных данных определенному кругу лиц (передача персональных данных) или на ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных данных в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к персональным данным каким-либо иным способом.

1.3.12. Специальные категории персональных данных – персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни субъекта персональных данных.

1.3.13. Уничтожение персональных данных – действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных.

2. Порядок обработки персональных данных

2.1. Обработка персональных данных в Информационных системах Учреждения должна осуществляться на основе принципов:

- законности целей и способов обработки персональных данных и добросовестности;
- соответствия целей обработки персональных данных целям, заранее определенным и заявленным при сборе персональных данных, а также полномочиям оператора;
- соответствия объема и характера обрабатываемых персональных данных, способов обработки персональных данных целям обработки персональных данных;
- достоверности персональных данных, их достаточности для целей обработки, недопустимости обработки персональных данных, избыточных по отношению к целям, заявленным при сборе персональных данных;
- недопустимости объединения созданных для несовместимых между собой целей баз данных информационных систем персональных данных.

2.2. Обработка персональных данных в Информационных системах Учреждения может осуществляться оператором с письменного согласия субъектов персональных данных, за исключением следующих случаев, когда такого согласия не требуется, если:

- обработка персональных данных осуществляется на основании федерального закона, устанавливающего её цель, условия получения персональных данных и круг субъектов, персональные данные которых подлежат обработке, а также определяющего полномочия оператора;
- обработка персональных данных осуществляется в целях исполнения договора, одной из сторон которого является субъект персональных данных;
- обработка персональных данных осуществляется для статистических или иных научных целей при условии обязательного обезличивания персональных данных;
- обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных, если получение согласия субъекта персональных данных невозможно.

2.3. Обработка оператором специальных категорий персональных данных в Информационных системах Учреждения допускается если:

- субъект персональных данных дал согласие в письменной форме на обработку своих персональных данных;

— персональные данные являются общедоступными;

— персональные данные относятся к состоянию здоровья субъекта персональных данных и их обработка необходима для защиты его жизни, здоровья или иных жизненно важных интересов либо жизни, здоровья или иных жизненно важных интересов других лиц, и получение согласия субъекта

персональных данных невозможно;

обработка персональных данных осуществляется в медико-профилактических целях, в целях установления медицинского диагноза, оказания медицинских и медико-социальных услуг при условии, что обработка персональных данных осуществляется лицом, профессионально занимающимся медицинской деятельностью и обязанным в соответствии с законодательством Российской Федерации сохранять врачебную тайну.

2.4. В случае если оператор на основании договора поручает обработку персональных данных другому лицу, существенным условием договора является обязанность обеспечения указанным лицом конфиденциальности персональных данных и безопасности персональных данных при их обработке.

2.5. Оператор, получающий доступ к персональным данным, должен обеспечивать конфиденциальность таких данных, за исключением случаев:

— в случае обезличивания персональных данных;

— в отношении общедоступных персональных данных.

2.6. Обработка персональных данных в Информационных системах Учреждения осуществляется только с согласия в письменной форме субъекта персональных данных, за исключением случаев, предусмотренных федеральными законами, которыми предусматриваются случаи обязательного предоставления субъектом персональных данных своих персональных данных в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства.

2.7. Письменное согласие субъекта персональных данных на обработку своих персональных данных в Информационных системах Учреждения должно включать в себя:

— фамилию, имя, отчество, адрес субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;

— наименование (фамилию, имя, отчество) и адрес оператора, получающего согласие субъекта персональных данных;

— цель обработки персональных данных;

— перечень персональных данных, на обработку которых дается согласие субъекта персональных данных;

— перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых оператором способов обработки персональных данных;

— срок, в течение которого действует согласие, а также порядок его отзыва.

2.8. Обязанность предоставить доказательство получения согласия субъекта персональных данных на обработку его персональных данных, а в случае обработки общедоступных персональных данных в Информационных системах Учреждения обязанность доказывания того, что обрабатываемые персональные данные являются общедоступными, возлагается на оператора.

2.9. В случае недееспособности субъекта персональных данных согласие на обработку его персональных данных в Информационных системах Учреждения дает в письменной форме законный представитель субъекта персональных данных.

2.10. В случае смерти субъекта персональных данных согласие на обработку его персональных данных в Информационных системах Учреждения дают в письменной форме наследники субъекта персональных данных, если такое согласие не было дано субъектом персональных данных при его жизни.

2.11. Субъект персональных данных имеет право на получение сведений об обработке своих персональных данных в Информационных системах Учреждения, а оператор обязан их предоставить в соответствии со статьями 14 и 20 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

3. Меры по обеспечению безопасности персональных данных при их обработке

3.1. Безопасность персональных данных, обрабатываемых в Информационных системах Учреждения, достигается путем исключения несанкционированного, в том числе случайного, доступа к персональным

данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий.

3.2. Для обеспечения безопасности персональных данных при их обработке в Информационных системах Учреждения осуществляется защита:

- информации, обрабатываемой с использованием технических средств;
- информации, содержащейся на бумажной, магнитной, магнитно-оптической и иной основе (носителях).

3.3. Работы по обеспечению безопасности персональных данных при их обработке в Информационных системах Учреждения являются неотъемлемой частью работ по созданию Информационных систем.

3.4. Информационные системы Учреждения классифицируются оператором. Проведение классификации Информационных систем определено Порядком проведения классификации информационных систем персональных данных, утвержденным совместным приказом Федеральной службы по техническому и экспортному контролю, Федеральной службы безопасности Российской Федерации, Министерством информационных технологий и связи Российской Федерации от 13.02.2008 № 55/86/20.

3.5. Обмен персональными данными при их обработке в Информационных системах Школы осуществляется по каналам связи, защита которых обеспечивается путем реализации соответствующих организационных мер и (или) путем применения технических и программных средств.

3.6. Размещение Информационных систем Учреждения, специальное оборудование и охрана помещений, в которых ведется работа с персональными данными, организация режима обеспечения безопасности в этих помещениях должны обеспечивать сохранность носителей персональных данных и средств защиты информации, а также исключать возможность неконтролируемого проникновения или пребывания в этих помещениях посторонних лиц.

3.7. Безопасность персональных данных при их обработке в Информационных системах Учреждения обеспечивает оператор или лицо, которому на основании договора оператор поручает обработку персональных данных (далее – Уполномоченное лицо). Существенным условием договора является обязанность Уполномоченного лица обеспечить конфиденциальность персональных данных и безопасность персональных данных при их обработке в информационной системе.

3.8. При обработке персональных данных в Информационных системах Учреждения безопасность обеспечивается:

- проведением мероприятий, направленных на предотвращение несанкционированного доступа к персональным данным и(или) передачи их лицам, не имеющим права доступа к такой информации;
- своевременным обнаружением фактов несанкционированного доступа к персональным данным;
- недопущением воздействия на технические средства автоматизированной обработки персональных данных, в результате которого может быть нарушено их функционирование;
- возможностью незамедлительного восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- постоянным контролем за обеспечением уровня защищенности персональных данных.

3.9. Защита персональных данных, обрабатываемая в Информационных системах Учреждения, обеспечивается за счет средств Учреждения в порядке, установленном федеральными законами.

3.10. Доступ сотрудников Учреждения к персональным данным, обрабатываемым в Информационных системах Учреждения, для выполнения своих должностных обязанностей производится к соответствующим персональным данным на основании списка, утвержденного оператором.

4. Особенности обработки персональных данных, осуществляемых без использования средств автоматизации

4.1. Персональные данные при их обработке, осуществляемой Неавтоматизированным способом, должны обособляться от иной информации. фиксацией их на отдельных материальных носителях персональных данных (далее — Материальные носители), в специальных разделах книг (журналов) или на полях форм (бланков).

4.2. При фиксации персональных данных на Материальных носителях не допускается фиксация на одном материальном носителе персональных данных, цели обработки которых заведомо не совместимы. Для обработки различных категорий персональных данных, осуществляемой Неавтоматизированным

способом, для каждой категории персональных данных должен использоваться отдельный Материальный носитель.

4.3. При использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них персональных данных (далее – Типовая форма), должны соблюдаться следующие условия:

4.3.1. Типовая форма или связанные с ней документы (инструкция по ее заполнению, карточки, реестры и журналы) должны содержать:

- сведения о цели обработки персональных данных, осуществляемой Неавтоматизированным способом;
- имя (наименование) и адрес оператора;
- фамилию, имя, отчество и адрес субъекта персональных данных;
- источник получения персональных данных;
- сроки обработки персональных данных;
- перечень действий с персональными данными, которые будут совершаться в процессе их обработки;
- общее описание используемых оператором способов обработки персональных данных.

4.3.2. Типовая форма должна предусматривать поле, в котором субъект персональных данных может поставить отметку о своем согласии на обработку персональных данных, осуществляемую Неавтоматизированным способом.

4.3.3. Типовая форма должна быть составлена таким образом, чтобы каждый из субъектов персональных данных, содержащихся в документе, имел возможность ознакомиться со своими персональными данными, содержащимися в документе, не нарушая прав и законных интересов иных субъектов персональных данных.

4.3.4. Типовая форма должна исключать объединение полей, предназначенных для внесения персональных данных, цели обработки которых заведомо не совместимы.

4.4. При несовместимости целей обработки персональных данных, зафиксированных на одном Материальном носителе, если Материальный носитель не позволяет осуществлять обработку персональных данных отдельно от других зафиксированных на том же носителе персональных данных, должны быть приняты меры по обеспечению отдельной обработки персональных данных:

4.4.1. При необходимости использования или распространения определенных персональных данных отдельно от находящихся на том же Материальном носителе других персональных данных осуществляется копирование персональных данных, подлежащих распространению или использованию, способом, исключающим одновременное копирование персональных данных, не подлежащих распространению и использованию, и используется (распространяется) копия персональных данных.

4.4.2. При необходимости уничтожения или блокирования части персональных данных уничтожается или блокируется Материальный носитель с предварительным копированием сведений, не подлежащих уничтожению или блокированию, способом, исключающим одновременное копирование персональных данных, подлежащих уничтожению или блокированию.

4.5. Уничтожение или обезличивание части персональных данных, если это допускается Материальным носителем, может производиться способом, исключающим дальнейшую обработку этих персональных данных с сохранением возможности обработки иных данных, зафиксированных на материальном носителе (удаление, вымарывание).

4.6. Правила, предусмотренные пунктами 4.4 и 4.5 настоящего Положения, применяются также в случае, если необходимо обеспечить отдельную обработку зафиксированных на одном Материальном носителе персональных данных и информации, не являющейся персональными данными.

4.7. Уточнение персональных данных при осуществлении их обработки

Неавтоматизированным способом производится путем обновления или изменения данных на Материальном носителе, а если это не допускается техническими особенностями материального носителя, — путем фиксации на том же материальном носителе сведений о вносимых в них изменениях либо путем изготовления нового материального носителя с уточненными персональными данными.

4.8. Обработка персональных данных, осуществляемая Неавтоматизированным способом, должна производиться таким образом, чтобы в отношении каждой категории персональных данных можно было

определить места хранения персональных данных (Материальных носителей) и установить перечень лиц, осуществляющих обработку персональных данных либо имеющих к ним доступ.

4.9. Необходимо обеспечивать раздельное хранение персональных данных (Материальных носителей), обработка которых осуществляется в различных целях.

5. Обязанности лиц, имеющих доступ к персональным данным

5.1. Ответственность за обеспечение безопасности персональных данных и надлежащий режим работы Информационных систем Учреждения возлагается на руководителя Учреждения.

5.2. В своей работе сотрудники Учреждения, допущенные к обработке персональных данных в Информационных системах Учреждения, должны руководствоваться требованиями федеральных законов, нормативно-правовых документов Правительства Российской Федерации, Федеральной службы по техническому и экспортному контролю, Федеральной службы безопасности Российской Федерации, Министерства информационных технологий и связи Российской Федерации, а также настоящим Положением и инструкцией пользователя по защите персональных данных, обрабатываемых в Информационных системах.

5.3. В должностные инструкции сотрудников Учреждения, уполномоченных на обработку персональных данных в Информационных системах Учреждения, должны быть внесены обязанности о необходимости выполнения требований по обеспечению безопасности обрабатываемых ими персональных данных.

5.4. Ответственный за обеспечение безопасности персональных данных в Учреждении руководствуется в своей деятельности инструкцией ответственного за обеспечение безопасности персональных данных, обрабатываемых в Информационных системах Учреждения.

5.5. При обнаружении нарушений порядка предоставления персональных данных, обрабатываемых в Информационных системах Учреждения, оператор незамедлительно приостанавливает предоставление персональных данных пользователям Информационных систем Учреждения до выявления причин нарушений и устранения этих причин.

5.6. За нарушение норм настоящего Положения, а также федеральных законов, регламентирующих порядок обработки и обеспечения безопасности персональных данных, сотрудники Учреждения, допущенные к работе с персональными данными в Информационных системах Учреждения, несут гражданско-правовую, административную, уголовную и дисциплинарную ответственность в соответствии с действующим законодательством.

Федеральные документы

- Конституция Российской Федерации [Открыть](#)
- Федеральный закон об образовании в российской федерации [Открыть](#)

Профилактика и противодействие экстремизму

- Федеральный список экстремистских материалов (по состоянию на 2.11.2016) [Открыть](#)
- Федеральный закон №114 «О противодействии экстремистской деятельности» [Открыть](#)
- Федеральный закон от 05 июля 2002 года № 112-ФЗ «О внесении изменений и дополнений в законодательные акты Российской Федерации в связи с принятием Федерального закона „О противодействии экстремистской деятельности“» [Открыть](#)
- Указ Президента Российской Федерации от 23 марта 1995 года № 310 (в редакции от 03.11.2004) «О мерах по обеспечению согласованных действий органов государственной власти в борьбе с проявлениями фашизма и иных форм политического экстремизма в Российской Федерации» [Открыть](#)
- Федеральный закон от 24 июля 2007 года № 211-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в связи с совершенствованием государственного управления в области противодействия экстремизму» [Открыть](#)
- Постановление Правительства Российской Федерации от 18.01.2003 г. № 27 (в редакции от 24.03.2011) «Об утверждении Положения о порядке определения перечня организаций и физических лиц, в отношении которых имеются сведения об их участии в экстремистской деятельности, и доведения этого перечня до сведения организаций, осуществляющих операции с денежными средствами или иным имуществом» [Открыть](#)
- Федеральный закон от 6 октября 2003 года № 131-ФЗ «Об общих принципах организации местного самоуправления в Российской Федерации» [Открыть](#)

Нормативные, правовые и иные акты в сфере противодействия коррупции

- Федеральный закон от 17 июля 2009 № 172-ФЗ «Об антикоррупционной экспертизе нормативных правовых актов и проектов нормативных правовых актов» [Открыть](#)

- Федеральный закон от 7 мая 2013 № 79-ФЗ «О запрете отдельным категориям лиц открывать и иметь счета (вклады), хранить наличные денежные средства и ценности в иностранных банках, расположенных за пределами территории Российской Федерации, владеть и (или) пользоваться иностранными финансовыми инструментами» (ред. от 22.12.2014) Открыть

ФГОС и ГОС

- Федеральный государственный образовательный стандарт дошкольного образования Открыть
- Федеральный государственный образовательный стандарт начального общего образования Открыть
- Федеральный государственный образовательный стандарт среднего (полного) общего образования Открыть
- федеральный государственный образовательный стандарт основного общего образования Открыть
- Примерная основная образовательная программа начального общего образования Открыть

Прием в школу

- Приказ Минобрнауки России от 22.01.2014 N 32 «Об утверждении Порядка приема граждан на обучение по образовательным программам начального общего, основного общего и среднего общего образования» Открыть

- Федеральный государственный образовательный стандарт начального общего образования Открыть

Информационная безопасность детей

- Указ Президента РФ от 01.06.2012 г. № 761 «О Национальной стратегии действий в интересах детей на 2012-2017 годы» Открыть
- Федеральный закон от 27.07.2006 N 152-ФЗ (ред. от 21.07.2014) «О персональных данных» (27 июля 2006 г.) Открыть
- Федеральный закон от 13.03.2006 № 38-ФЗ «О рекламе» Открыть
- Федеральный закон от 29.12.2010 № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию» Открыть
- Федеральный закон от 24.07.1998 № 124-ФЗ «Об основных гарантиях прав ребенка в Российской Федерации» Открыть

Муниципальное бюджетное общеобразовательное учреждение
для обучающихся с ограниченными возможностями здоровья
основная общеобразовательная школа № 10
г. Чебаркуля

Российская Федерация, 456440, г. Чебаркуль Челябинской области, ул. Мира 21 Б.
Телефон: (8-35168) 2-46-08

Утверждаю
Директор МБОУ ООШ № 1
Е.А.Кривоносов
(приказ от 18.12.2020 № 169 -д)



Регламент резервного копирования персональных данных

ТЕРМИНЫ И СОКРАЩЕНИЯ

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

Оператор – государственный орган, муниципальный орган, юридическое или физическое лицо самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

Обработка персональных данных – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

Автоматизированная обработка персональных данных – обработка персональных данных помощью средств вычислительной техники.

Распространение персональных данных – действия, направленные на раскрытие персональных данных неопределенному кругу лиц.

Предоставление персональных данных - действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.

Блокирование персональных данных – временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных).

Уничтожение персональных данных – действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных.

Обезличивание персональных данных – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.

Информационная система персональных данных (ИСПДн) – совокупность содержащихся в базе данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

Трансграничная передача персональных данных - передача персональных данных на территории иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

Типовая информационная система – информационная система, в которой требуется обеспечени только конфиденциальности персональных данных.

Специальная информационная система – информационная система, в которой вне зависимости от необходимости обеспечения конфиденциальности персональных данных требуется обеспечить хотя бы одну из характеристик безопасности персональных данных, отличную от конфиденциальности (защищенность от уничтожения, изменения,

блокирования, а также иных несанкционированных действий).

2. ОБЩИЕ ПОЛОЖЕНИЯ

Настоящий Регламент определяет порядок резервирования персональных данных (далее – ПДн) в МБОУ ООШ № 10 для последующего восстановления работоспособности информационных систем персональных данных (далее – ИСПДн) при полной или частичной потере информации, определены порядок восстановления персональных данных.

Ответственными за выполнение требований данного Регламента и реализацию указанных в нем процедур являются Администратор безопасности информационных систем персональных данных (далее – Администратор безопасности ИСПДн).

3. ПОРЯДОК РЕЗЕРВНОГО КОПИРОВАНИЯ

3.1 МАССИВЫ ПЕРСОНАЛЬНЫХ ДАННЫХ, ПОДЛЕЖАЩИЕ РЕЗЕРВИРОВАНИЮ

Резервному копированию подлежит информация, хранящаяся на серверах:

- базы данных;
- каталоги данных на файловых серверах;
- общие каталоги отделов и подразделений.

3.2 МЕТОДЫ И СПОСОБЫ СОЗДАНИЯ РЕЗЕРВНЫХ КОПИЙ

Резервирование ПДн, хранящихся на серверах, осуществляется путем копирования резервируемой информации на магнитные ленты, RAID-массивы, магнитооптические накопители, съемные диски, дисковые накопители и облачные сервисы.

При резервировании ПДн, хранящихся на серверах, используются две стратегии резервирования:

- горячее резервирование (hotstandby)* – копирование данных основного сервера на резервный сервер при включенных сервисах автоматизированной системы, входящей в состав ИСПДн;
- холодное резервирование (standby backup)* – копирование данных основного сервера на резервный сервер при выключенных сервисах автоматизированной системы, входящей в состав ИСПДн.

Используются следующие методы резервного копирования:

- полное резервирование* – периодически создается полная копия массивов

данных;

- добавочное резервирование* – на первом этапе создается полная копия массивов данных, а на последующих этапах в данную копию вносятся изменения в соответствии с произошедшими изменениями.

Также используются следующие способы создания резервных копий:

- ручной* – резервные копии создаются простым копированием массивов данных ответственным работником;
- автоматизированный* – резервные копии создаются ответственным работником с использованием специализированного программного обеспечения;
- автоматический* – резервные копии создаются с использованием специализированного программного обеспечения в соответствии с предварительно настроенным расписанием.

Указанные методы могут использоваться как при создании резервных копий в соответствии с Планом резервного копирования ПДн, так и при создании резервных копий по запросу. Форма Плана приведена в Приложении 1 настоящего Регламента.

3.3. ПЛАН РЕЗЕРВНОГО КОПИРОВАНИЯ

В МБОУ Скоковской средней школе Даниловского района Ярославской области определены следующие режимы функционирования ИСПДн:

- штатный режим функционирования*, при котором клиентское, серверное программно-обеспечение, технические средства пользователей и администратора системы обеспечивают возможность круглосуточного и ежедневного функционирования;
- аварийный режим функционирования*, при котором произошло нарушение функционирования одного или нескольких компонент программного и (или) технического обеспечения.

Резервное копирование ПДн в штатном режиме производится в соответствии с Планом резервного копирования ПДн.

На протяжении периода времени, когда ИСПДн находится в аварийном состоянии, осуществляется ежедневное полное копирование, подлежащее резервированию, с использованием средств файловых систем серверов, располагающих необходимыми объемами дискового пространства для ее хранения.

4. УЧЕТ И ХРАНЕНИЕ РЕЗЕРВНЫХ КОПИЙ

Учету подлежат следующие типы носителей резервных копий:

- магнитные ленты;
- магнитооптические накопители;
- съемные диски;
- дисковые накопители.

4.1 ПОРЯДОК УЧЕТА РЕЗЕРВНЫХ КОПИЙ

Учет резервных копий, созданных автоматизированными средствами системы резервного копирования, производится в электронном журнале системы.

Резервные копии персональных данных маркируются следующим образом: <Название базы данных каталога>_<Дата и время резервной копии>.

Учет резервных копий, созданных вручную, осуществляется в Журнале восстановления, учета создания и использования резервных копий ПДн. с указанием даты, времени начала и окончания операций копирования или восстановления данных, а также с приведением комментариев в случае их необходимости. Также в Журнале резервного копирования учитывается:

- создание копии по запросу;
- полное копирование в случае возникновения аварийных ситуаций.

Форма Журнала представлена в Приложении 2 настоящего Регламента.

Ответственным за ведение Журнала является Администратор безопасности ИСПДн.

4.2 ПОРЯДОК ХРАНЕНИЯ РЕЗЕРВНЫХ КОПИЙ

Хранение носителей, содержащих ПДн, осуществляется в условиях, исключающих возможности хищения, изменения целостности или уничтожения содержащейся на них информации.

Носители резервных копий краткосрочного хранения хранятся в помещениях, доступ в которых ограничен.

Срок хранения резервных копий определяется согласно Плану резервного копирования. В случае необходимости долгосрочного хранения резервных копий по истечении 3 месяцев носители резервных копий перемещаются в сейфы, (металлические шкафы), запираемые на ключ или на отдельные сервера, для долгосрочного хранения, под ответственность Администратору безопасности ИСПДн.

Отметка о передаче носителей резервных копий для долгосрочного хранения резервных копий персональных данных проставляется в Журнале восстановления, учета создания и использования резервных копий персональных данных.

Допускается повторное использование носителей резервных копий по истечении срока хранения ПДн

5. КОНТРОЛЬ РЕЗЕРВНОГО КОПИРОВАНИЯ

Машинные носители, предназначенные для долгосрочного хранения информации, периодически проверяются на их пригодность и отсутствие сбойных секторов.

При появлении сбойных секторов на машинных носителях информация с этих носителей переносится на исправные. Неисправные носители уничтожаются согласно Регламента по учету, хранению и уничтожению носителей персональных данных.

Контроль результатов всех процедур резервного копирования осуществляется Администратором безопасности ИСПДн. В случае обнаружения ошибки в процессе резервного копирования выполняется повторное резервное копирование.

Администратором безопасности ИСПДн несет ответственность за корректное ведение Журнала восстановления, учета создания и использования резервных копий персональных данных.

6. ВОССТАНОВЛЕНИЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

Восстановление ПДн проводится в случае нарушения ее целостности вследствие несанкционированного доступа в систему, воздействия вирусов, программных ошибок, ошибок персонала, аппаратных сбоев и пр.

В случае необходимости восстановления ПДн из резервных копий Пользователь ИСПДн, который работает с этими данными, сообщает о случившемся своему руководителю.

Руководитель Пользователя ИСПДн оформляет запрос в форме служебной записки или электронной заявки и направляет ее Администратору безопасности ИСПДн. В заявке должны быть указаны:

- данные, которые необходимо восстановить;
- дата и время, по состоянию на которые должны быть восстановлены данные;
- желательный срок восстановления;
- описание причины, по которой произошла потеря персональных данных (ошибка пользователя, программный сбой и т.п.).

В зависимости от обстоятельств, по которым произошло нарушение целостности ПДн, Администрато

безопасности ИСПДн принимает решение о необходимости полного или частичного восстановления потерянных данных.

Кроме того, Администратор безопасности ИСПДн, получив запрос на восстановление данных принимает решение о реагировании на данный инцидент в соответствии с Регламентом по проведению контрольных мероприятий и реагированию на инциденты информационной безопасности.

Администратор безопасности ИСПДн несет ответственность за восстановление утерянных данных. Восстановление данных осуществляется в максимально сжатые сроки,

ограниченные техническими возможностями системы, но не более трех рабочих дней.

Факт восстановления ПДн регистрируется в Журнале восстановления, учета создания и использования резервных копий ПДн.

7. ПЕРЕСМОТР И ВНЕСЕНИЕ ИЗМЕНЕНИЙ

Пересмотр положений настоящего документа проводится в следующих случаях:

- на регулярной основе, но не реже одного раза в полгода;
- при появлении новых требований к обработке и обеспечению безопасности персональных данных со стороны российского законодательства и контролирующих органов исполнительной власти РФ;
- по результатам проверок контролирующих органов исполнительной власти Российской Федерации, выявивших несоответствия требованиям по обеспечению безопасности ПДн;
- по результатам внутреннего контроля (аудита) системы защиты ПДн в случае выявления существенных нарушений;
- по результатам расследования инцидентов информационной безопасности, связанных с обработкой и обеспечением безопасности ПДн и выявивших недостатки в правилах предоставления доступа ПДн.

Пересмотр и внесение изменений в настоящий документ регламентируется Регламентом по проведению контрольных мероприятий и реагированию на инциденты информационной безопасности.

Ответственным за пересмотр настоящего Регламента является Администратор безопасности ИСПДн. Внесение изменений производится на основании соответствующего приказа по школе.

Обязательство о неразглашении персональных данных

Я, _____,
паспорт серии _____, номер _____, выданный « _____ » _____ 20____ г.,
_____, являясь штатным работником
« _____ », в соответствии с трудовым договором,
должностной инструкцией понимаю, что получаю доступ к персональным данным физических
лиц, а именно: _____

Я также понимаю, что во время исполнения своих обязанностей мне приходится заниматься сбором, обработкой, накоплением, хранением и т.д. персональных данных физических лиц.

Я обязуюсь хранить в тайне известные мне конфиденциальные сведения, информировать руководителя образовательного учреждения о фактах нарушения порядка обращения с конфиденциальными сведениями, о ставших мне известным попытках несанкционированного доступа к информации.

Я обязуюсь соблюдать правила пользования документами, порядок их учета и хранения, обеспечивать в процессе работы сохранность информации, содержащейся в них, от посторонних лиц, знакомиться только с теми служебными документами, к которым получаю доступ в силу исполнения своих служебных обязанностей.

Я понимаю, что разглашение такого рода информации может нанести ущерб физическим лицам, как прямой, так и косвенный.

В связи с этим даю обязательство при работе (сборе, обработке, накоплении, хранении и т.д.) с персональными данными физических лиц соблюдать все описанные в Федеральном законе от 27.07.2006 г. № 152-ФЗ «О персональных данных», постановлении Правительства РФ от 15.09.2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» и других нормативных актах, требования.

Я предупрежден(а) о том, что в случае разглашения мной сведений, касающихся персональных данных физических лиц, или их утраты я несу ответственность в соответствии с действующим законодательством РФ.

« _____ » _____ 20____ г.

Подпись

Расшифровка подписи

Приложение к обязательству

Я _____ подтверждаю, что не имею права разглашать сведения:

- анкетные и биографические данные;
- сведения об образовании;
- сведения о трудовом и общем стаже;
- сведения о составе семьи;
- паспортные данные;
- сведения о воинском учете;
- сведения о заработной плате сотрудника;
- сведения о социальных льготах;
- специальность;
- занимаемая должность;
- наличие судимостей;
- адрес места жительства;
- домашний телефон;
- место работы или учебы членов семьи и родственников;
- характер взаимоотношений в семье;
- содержание трудового договора;
- состав декларируемых сведений о наличии материальных ценностей;
- содержание декларации, подаваемой в налоговую инспекцию;
- подлинники и копии приказов по личному составу;
- личные дела и трудовые книжки сотрудников;
- основания к приказам по личному составу;
- дела, содержащие материалы по повышению квалификации и переподготовке, их аттестации;
- копии отчетов, направляемые в органы статистики.

Подпись _____

Директор
МБОУ ООШ № 10

Е.А.Кривоносова
(ФИО)

« ____ » _____ 20 ____ г.

**Акт
об уничтожении персональных данных в МБОУ ООШ № 10**

Комиссия в составе:

	ФИО	Должность
Председатель		
Члены комиссии		

провела отбор всех носителей, содержащих персональные данные _____
_____ и установила, что в соответствии с требованиями
руководящих документов РФ по защите информации, персональные данные, записанные
на них в процессе эксплуатации _____
в период до « ____ » _____ 20 ____ г. включительно, подлежат уничтожению:

№ п/п	Тип носителя	Серийный номер носителя ПДн	Примечание
1.			
2.			
3.			
4.			
5.			

Всего подлежат уничтожению персональные данные на _____ (прописью)
носителях персональных данных _____

После утверждения Акта, перечисленные носители сверены с записями в Акте и на
указанных носителях, персональные данные _____

(Название учреждения)

уничтожены путем стирания персональных данных, встроенными механизмами
операционных систем и СУБД программно-технических
средств _____, а также _____

Председатель:

_____ (подпись)

_____ (ФИО)

Члены комиссии:

_____ (подпись)

_____ (ФИО)

Технический паспорт ИСПДн

Полное наименование оператора

«Утверждено»

Должность

личная подпись

расшифровка подписи

Технический паспорт информационной системы персональных данных

1. Общие сведения об ИСПДн _____

1.1. Наименование ИСПДн _____

1.2. Физическое расположение ИСПДн _____

1.3. Частная модель угроз безопасности ПДн в ИСПДн утверждена _____

дата подписи модели угроз ПДн в ИСПДн _____

1.4. Перечень ПДн, обрабатываемых в ИСПДн приводится в таблице

Перечень ПДн,
обрабатываемых в ИСПДн

№ п/п	Наименование персональных данных	Цель обработки ПДн в рамках ИСПДн

Перечень
технологических процессов обработки ПДн, используемых в ИСПДн

№ п/п	Наименование технологических процессов

1.5. Состав основных технических средств и систем (ОТСС)

Перечень
основных технических средств и систем, входящих в состав ИСПДн

№ п/п	Тип ОТСС	Программные и технические характеристики	Место установки	Кол-во, шт.

1.6. Состав вспомогательных технических средств и систем (ВТСС)

Перечень
вспомогательных технических средств, входящих в состав ИСПДн (средств вычислительной техники, не участвующих в обработке персональных данных)

№ п/п	Наименование и тип вспомогательных технических средств	Место установки	Кол-во, шт	Примечание

1.7. Состав средств защиты информации

Перечень
средств защиты информации, установленных в ИСПДн

№ п/п	Наименование и тип средств защиты информации	Сведения о сертификате	Место установки

Акт классификации информационной системы персональных данных

УТВЕРЖДАЮ

Директор МБОУ ООШ № 10

_____ Е.А.Кривоносова

(руководитель органа
исполнительной власти)

«__» _____ 20__ г.

Типовая форма акта
классификации информационной системы персональных данных

(наименование ИСПДн)

(организация)

(местоположение)

Комиссия в составе:

Председатель

Члены

комиссии

Рассмотрев исходные данные об информационной системе персональных данных:

- 1) категория персональных данных _____, $X_{пд} = _;$
- 2) объем обрабатываемых персональных данных _____, $X_{пд} = _;$
- 3) заданные характеристики безопасности персональных данных, обрабатываемых в информационной системе в соответствии с требованиями подпункта г) пункта 11 «Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденного постановлением Правительства Российской Федерации от 17 ноября 2007 г. № 781: **СПЕЦИАЛЬНАЯ**;
- 4) структура информационной системы: **АВТОНОМНАЯ** (локальная информационная система, распределенная информационная система);
- 5) наличие подключений информационной системы к сетям связи общего пользования и (или) сетям международного информационного обмена: **НЕТ (ДА)**;
- 6) режим обработки персональных данных:
МНОГОПОЛЬЗОВАТЕЛЬСКИЙ (ОДНОПОЛЬЗОВАТЕЛЬСКИЙ);

7) режим разграничения прав доступа пользователей информационной системы:

БЕЗ РАЗГРАНИЧЕНИЯ ПРАВ ДОСТУПА (С РАЗГРАНИЧЕНИЕМ ПРАВ ДОСТУПА);

8) местонахождение технических средств: **В ПРЕДЕЛАХ РОССИЙСКОЙ ФЕДЕРАЦИИ.**

В соответствии с пунктами 14 и 15 «Порядка проведения классификации информационных систем персональных данных», утвержденного совместным приказом ФСТЭК России, ФСБ России, Министерства информационных технологий и связи Российской Федерации от 13.02.2008 № 55/86/20 и на основании анализа исходных данных, РЕШИЛА:

информационной системе персональных данных _____
установить класс: _.

Председатель комиссии:

Члены комиссии:

«__» _____ 20__ г.

Алгоритм построения системы защиты персональных данных

Организационные меры защиты персональных данных включают в себя комплекс мероприятий по разработке организационно-распорядительных документов, регламентирующих весь процесс получения, обработки, хранения, передачи и защиты персональных данных.

Шаг 1. Создать специальную комиссию по защите персональных данных или назначить ответственного за обеспечение информационной безопасности.

В зависимости от величины организации целесообразно назначить либо одного человека, ответственного за обеспечение информационной безопасности, либо создать специальную комиссию по защите персональных данных. В качестве председателя комиссии целесообразно назначить кого – либо из первых заместителей руководителя организации, начальника службы безопасности организации или руководителя кадровой службы организации. В состав комиссии рекомендуется включить главного бухгалтера, руководителей подразделений организации обрабатывающих персональные данные, так как они знают структуру обрабатываемых персональных данных, задачи проводимой обработки, а также сотрудников организации, ведущих обработку персональных данных. В качестве лиц, обладающих специальным образованием в области защиты информации и необходимыми познаниями, в состав комиссии следует включить сотрудников организации, имеющей лицензию на техническую защиту конфиденциальной информации, если таковые имеются в штате организации.

Шаг 2. Произвести инвентаризацию информационной системы, обрабатывающей персональные данные.

Часто проведение этого этапа предпроектного обследования считают неразумным или нерациональным, но для построения сбалансированной системы защиты информации он необходим. На этом этапе составляется перечень всех информационных и аппаратных ресурсов организации. Данный перечень будет использоваться в дальнейшем для проведения категорирования, переконфигурирования локальной сети, выработки рекомендаций по построению системы защиты.

Выявляется топология локальной сети, ее архитектура и технологические связи внутренней сети, а также основные информационные потоки.

Также на данном этапе осуществляется определение физической и логической структуры будущей системы защиты информационной системы персональных данных. Устанавливается наличие средств защиты и существующей системы разграничения доступа к информационным ресурсам. Также изучаются имеющиеся сертификаты на средства защиты информации и выясняется необходимость сертификации уже установленных программных и программно-аппаратных комплексов защиты информации.

По итогам данного этапа составляется акт инвентаризации информационных ресурсов.

Шаг 3. Пересмотреть договоры с субъектами и контрагентами

Пересмотреть договоры с работниками и клиентами. Необходимо выяснить, содержатся ли в них пункты, касающиеся обработки и защиты персональных данных. В случае отсутствия подготовить дополнительные соглашения, ознакомить сотрудников и контрагентов. Подписать их.

Шаг 4. Сформировать перечень персональных данных.

В первую очередь, необходимо установить перечень персональных данных (далее ПДн) физических лиц, которые обрабатываются в учреждении. Если кадровый учет и бухгалтерия есть в любом учреждении, то другие направления деятельности, где используются персональные данные, требуется установить: это могут быть данные посетителей, партнеров, контрагентов и т.п.

Также нужно определить цели обработки персональных данных: трудовые отношения с работниками; договор оказания услуг и т.п.

Сроки обработки и хранения. Хранение ПДн должно быть не дольше, чем этого требуют цели их обработки, по достижению которых ПДн подлежат уничтожению. Установить перечень ПДн, по которым цели обработки достигнуты.

Шаг 5. Составить и направить в Управление Роскомнадзора "Уведомление об обработке персональных данных".

Начав деятельность, организация обязана подать уведомление о начале обработки персональных данных в Управление Роскомнадзора. На основании уведомления организация регистрируется в реестре операторов, осуществляющих обработку персональных данных.

Уведомление должно быть направлено в письменной форме и подписано руководителем или направлено в электронной форме и подписано электронной цифровой подписью.

Одной из самых распространенных ошибок операторов, не желающих выполнять требования Закона, является ссылка на начало п. 2 ст. 22 Закона:

Операторы ссылаются на оформление договорных отношений с субъектами и размышляют так: «Уведомление подавать не обязательно, значит, работы по созданию системы защиты персональных данных проводить излишне».

«Оператор вправе осуществлять без уведомления уполномоченного органа по защите прав субъектов персональных данных обработку персональных данных полученных оператором в связи с заключением договора, стороной которого является субъект персональных данных...»

Ссылаясь на этот пункт статьи, забывают о том, что персональные данные сами отправляют в Управление Федеральной налоговой службы, Управление Пенсионного фонда России, в страховые компании, в аутсорсинговые компании и т.д., то есть третьим лицам.

Завершается п. 2 ст. 22 Закона словами:

«... если персональные данные не распространяются, а также не предоставляются третьим лицам без согласия субъекта персональных данных и используются оператором исключительно для исполнения указанного договора и заключения договоров с субъектом персональных данных»

Таким образом, все юридические лица обязаны подавать уведомление в Управление Роскомнадзора субъекта Федерации и создавать систему защиты персональных данных.

Шаг 6. Получить согласие субъектов на обработку их персональных данных.

Необходимо разработать "Согласие субъекта на обработку персональных данных", в котором обязательными полями будут перечень персональных данных, цель их обработки, а также методы и способы обработки персональных данных и получить подписи каждого субъекта, персональные данные которого обрабатывает Ваша организация.

Шаг 7. Документально регламентировать работу с персональными данными.

Разработать документы, регламентирующие работу с персональными данными.

Шаг 8. Ограничить доступ своих сотрудников и пользователей информационных систем к персональным данным.

Лица, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения служебных (трудовых) обязанностей, допускаются к соответствующим персональным данным на основании «Перечня лиц, допущенных персональным данным».

Шаг 9. Сформировать модель угроз персональным данным.

Частная модель угроз организации – оператора составляется в соответствии с руководящим документом ФСТЭК России от 14.02.2008 «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных». Поскольку данный документ имеет гриф «для служебного пользования», то получить его можно, отправив запрос в территориальное Управление ФСТЭК с просьбой о предоставлении комплекта документов по защите персональных данных.

Квалифицированное составление частной модели угроз имеет важное значение для организации - оператора. Именно от этого зависит выбор необходимых и достаточных способов защиты информационной системы, подбор оборудования, а, следовательно, конечная стоимость всех работ по обеспечению безопасности персональных данных.

Шаг 10. Классифицировать ИСПДн согласно приказа ФСТЭК/ФСБ/Мининформсвязи от 13.02.2008 №55/86/20 «Об утверждении порядка проведения классификации ИСПДн».

На основании закона «О персональных данных» любая информационная система персональных данных должна быть классифицирована. Процесс классификации - это процесс отнесения информационной системы персональных данных к одному из четырех классов, определенных Приказом Мининформсвязи/ФСТЭК/ФСБ от 13.02.2008 № 55/86/20 «Об утверждении Порядка проведения классификации информационных систем персональных данных».

Класс присваивается в зависимости от количества субъектов, персональные данные которых обрабатываются в ИСПДн, а также с учетом категории обрабатываемых данных. Категории персональных данных установлены приказом Федеральной службы по техническому и экспортному контролю (ФСТЭК России) Федеральной службы безопасности Российской Федерации (ФСБ России) Министерства информационных технологий и связи Российской Федерации (Мининформсвязи России) от 13 февраля 2008 г. N 55/86/20 г. Москва "Об утверждении Порядка проведения классификации информационных систем персональных данных".

Шаг 11. Получить лицензию ФСТЭК на техническую защиту конфиденциальной информации (в случае самостоятельной установки программно-аппаратных средств защиты информации) или воспользоваться услугами сторонней организации, имеющей данную лицензию.

После изучения вопроса и понимания того, что выполнять работы необходимо, каждый руководитель задает себе следующий вопрос: можно ли самостоятельно выполнить требования законодательства или лучше воспользоваться услугами специализированной организации?

С учетом временных ограничений (срок завершения работ – 01.01.2011 года) проведение работ собственными силами может растянуться на длительный период, превышающий установленные законом сроки. Соответственно, возникают риски предъявления претензий со стороны регуляторов за неисполнение требований законодательства.

Шаг 12. Организовать эксплуатацию ИСПДн и контролировать безопасность обработки персональных данных путем проведения ежегодного аудита информационной безопасности.

Необходимо контролировать соблюдение условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией. Проводить разбирательство и составлять заключения по фактам несоблюдения условий хранения носителей ПДн, использования средств защиты информации, которые могут привести к нарушению конфиденциальности ПДн.

Шаг 13. Обучить лиц, использующих средства защиты информации, применяемые в информационных системах, правилам работы с ними.

Для того, чтобы организация могла выполнять требования законодательства по защите персональных данных, мало разработать организационно-распорядительные и эксплуатационные документы и купить технические средства защиты информации. Очень важно на постоянной основе проводить обучение сотрудников новым средствам защиты информации, которые они используют в силу выполнения своих должностных обязанностей, а также правилам работы с этими средствами.