

УТВЕРЖДАЮ
Директор МБОУ СОШ №3 г. Ка-
шин С.В. Галкина
М.П.
«02» 09 2014 г.



Приложение 1 к приказу
№ 109 от 02.09.14
об утверждении Положения
о персональных данных

ПОЛОЖЕНИЕ
о персональных данных
в МБОУ СОШ №3 г. Кашин

1. Назначение и область действия Положения

Настоящее положение о персональных данных (далее - Положение) содержит общеположения, требования законодательства к организации обработки персональных данных без использования средств автоматизации, к оператору информационных систем персональных данных, описание порядка проведения классификации информационных систем и персональных данных, основные мероприятия по защите персональных данных в МБОУ СОШ №3 г. Кашин, описание состава документов правового обеспечения обработки персональных данных в МБОУ СОШ №3 г. Кашин, состав персональных данных в разрезе информационных систем, характеристику типовых информационных систем персональных данных и основных угроз безопасности персональных данных, описана организационная сторона защиты персональных данных и ответственность должностных лиц по их защите.

Все работники МБОУ СОШ №3 г. Кашин должны быть ознакомлены с настоящим Положением под роспись, и сведения о факте ознакомления должны быть внесены в лист ознакомления (Приложение №1).

Необходимо опубликовать или иным образом предоставить неограниченный доступ к настоящему положению.

2. Общие положения

Законодательством Российской Федерации ответственность за надлежащую защиту персональных данных возлагается на организации, в которых персональные данные обрабатываются. Уполномоченным органом по контролю за соблюдением законодательства о персональных данных является Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор).

Роскомнадзор проводит плановые (целевые, комплексные) проверки, а также проверки по жалобам и обращениям физических и юридических лиц. Проверки систем защиты персональных данных могут также осуществляться ФСТЭК России или ФСБ России при проведении контроля систем защиты конфиденциальных данных или использования криптосредств.

Нарушение законодательства о персональных данных, в соответствии с Федеральным законом от 27.07.2006 г. № 152-ФЗ «О персональных данных» влечет за собой гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность, налагаемую в судебном порядке.

К персональным данным относится любая информация, относящаяся к прямо или косвенно определенному или определяемому лицу (субъекту персональных данных).

Оператор персональных данных - государственный орган, муниципальный орган, юридическое или физическое лицо, организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели и содержание такой обработки.

Информационная система персональных данных - информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без наличия таких средств

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.

В настоящее время законодательно-нормативная база по персональным данным включает:

- Федеральный закон от 19.12.2005 г. N 160-ФЗ «О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных».
- Федеральный закон Российской Федерации от 27.07.2006 г. N 152-ФЗ «О персональных данных».
- Постановление Правительства Российской Федерации от 01.11.2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»
- Постановление Правительства Российской Федерации от 15.09.2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».
- Постановление Правительства Российской Федерации от 6.07.2008 г. № 512 «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных».
- Постановление Правительства Российской Федерации от 15.08.2006 г. № 504 «О лицензировании деятельности по технической защите конфиденциальной информации».
- Приказ Россвязькомнадзора от 17.07.2008 г. № 08 «Об утверждении образца формы уведомления об обработке персональных данных».

Обеспечение безопасности персональных данных должно осуществляться в соответствии с методическими документами ФСТЭК России:

- Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных" от 15 февраля 2008 года.

Использование криптосредств для обеспечения безопасности персональных данных должно осуществляться в соответствии с:

- Приказом ФСБ России от 9.02.2005 г. № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации»);
- Постановлением Правительства Российской Федерации от 29.12.2007 г. № 957 «Об утверждении положений о лицензировании отдельных видов деятельности, связанных с шифровальными (криптографическими) средствами»;
- Методическими рекомендациями по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации (ФСБ России, от 21.02.2008 г. № 149/54-144)
- Типовыми требованиями по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных (ФСБ России, от 21.02.2008 г. № 149/6/6-622)

На основании указанных выше документов всеми организациями и физическими лицами на территории Российской Федерации должен обеспечиваться требуемый уровень безопасности персональных данных. Лица, виновные в нарушении требований несут предусмотренную законодательством Российской Федерации ответственность.

3. Обработка персональных данных без использования средств автоматизации

Обработка персональных данных без использования средств автоматизации осуществляется в соответствии с законодательством Российской Федерации и «Положением об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», утвержденным постановлением Правительства Российской Федерации от 15.09.2008 г №687.

Лица, осуществляющие обработку персональных данных без использования средств автоматизации (в том числе сотрудники организации-оператора или лица, осуществляющие такую обработку по договору с оператором), должны быть проинформированы о факте обработки ими персональных данных, обработка которых осуществляется оператором без использования средств автоматизации, категориях обрабатываемых персональных данных, а также об особенностях и правилах осуществления такой обработки, установленных нормативными правовыми актами федеральных органов исполнительной власти, органов исполнительной власти субъектов Российской Федерации, а также локальными правовыми актами организации (при их наличии).

Обработка персональных данных, осуществляемая без использования средств автоматизации, должна осуществляться таким образом, чтобы в отношении каждой категории

персональных данных были:

- определены места хранения персональных данных (материальных носителей) и установлен перечень лиц, осуществляющих обработку персональных данных либо имеющих к ним доступ.
- обеспечено раздельное хранение персональных данных (материальных носителей), обработка которых осуществляется в различных целях.
- соблюдены условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный к ним доступ.

Перечень мер, необходимых для обеспечения таких условий, порядок их принятия, а также перечень лиц, ответственных за реализацию указанных мер, устанавливается оператором (Более подробно см. документ «Положение об обработке ПДн без использования средств автоматизации»).

Учет и хранение в МБОУ СОШ №3 г. Кашин документов, содержащих персональные данные, следует осуществлять в соответствии с документом «Положение об обработке персональных данных без использования средств автоматизации».

4. Основные обязанности операторов информационных систем, обрабатывающих персональные данные

Безопасность персональных данных при их обработке в информационной системе обеспечивает оператор этой системы, который обрабатывает персональные данные, или лицо, осуществляющее обработку персональных данных по поручению оператора на основании заключаемого с этим лицом договора.

Выбор средств защиты информации для системы защиты персональных данных осуществляется оператором в соответствии с нормативно правовыми актами, принятыми Федеральной службой безопасности Российской Федерации и Федеральной службой по техническому и экспортному контролю во исполнение части 4 статьи 19 Федерального закона «О персональных данных».

5. Определение типа угроз безопасности и уровня защищенности персональных данных.

Постановление Правительства Российской Федерации от 01.11.2012 г № 1119 возлагает задачу обеспечения безопасности персональных данных при их обработке в информационной системе на оператора этой системы. Выбор средств защиты также определяется оператором.

Под актуальными угрозами безопасности персональных данных понимается совокупность условий и факторов, создающих актуальную опасность несанкционированного, в том

числе случайного, доступа к персональным данным при их обработке в информационной системе, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия.

Угрозы 1-го типа актуальны для информационной системы, если для нее в том числе актуальны угрозы, связанные с наличием недокументированных (недекларированных) возможностей в системном программном обеспечении, используемом в информационной системе.

Угрозы 2-го типа актуальны для информационной системы, если для нее в том числе актуальны угрозы, связанные с наличием недокументированных (недекларированных) возможностей в прикладном программном обеспечении, используемом в информационной системе.

Угрозы 3-го типа актуальны для информационной системы, если для нее актуальны угрозы, не связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении, используемом в информационной системе.

Определение типа угроз безопасности персональных данных, актуальных для информационной системы, производится оператором с учетом оценки возможного вреда, проведенной во исполнение пункта 5 части 1 статьи 18.1 Федерального закона "О персональных данных", и в соответствии с нормативными правовыми актами, принятыми во исполнение части 5 статьи 19 Федерального закона "О персональных данных".

Согласно требованиям к защите персональных данных при их обработке в информационных системах персональных данных, утвержденных постановлением Правительства РФ от 1 ноября 2012г. №1119 при обработке персональных данных в информационных системах устанавливаются 4 уровня защищенности персональных данных.

Необходимость обеспечения 1-го уровня защищенности персональных данных при их обработке в информационной системе устанавливается при наличии хотя бы одного из следующих условий:

а) для информационной системы актуальны угрозы 1-го типа и информационная система обрабатывает либо специальные категории персональных данных, либо биометрические персональные данные, либо иные категории персональных данных;

б) для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает специальные категории персональных данных более чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора.

Необходимость обеспечения 2-го уровня защищенности персональных данных при их обработке в информационной системе устанавливается при наличии хотя бы одного из следующих условий:

а) для информационной системы актуальны угрозы 1-го типа и информационная система обрабатывает общедоступные персональные данные;

б) для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает специальные категории персональных данных сотрудников оператора или специальные категории персональных данных менее чем 100000 субъектов персональных дан-

ных, не являющихся сотрудниками оператора;

в) для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает биометрические персональные данные;

г) для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает общедоступные персональные данные более чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора;

д) для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает иные категории персональных данных более чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора;

е) для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает специальные категории персональных данных более чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора.

Необходимость обеспечения 3-го уровня защищенности персональных данных при их обработке в информационной системе устанавливается при наличии хотя бы одного из следующих условий:

а) для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает общедоступные персональные данные сотрудников оператора или общедоступные персональные данные менее чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора;

б) для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает иные категории персональных данных сотрудников оператора или иные категории персональных данных менее чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора;

в) для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает специальные категории персональных данных сотрудников оператора или специальные категории персональных данных менее чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора;

г) для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает биометрические персональные данные;

д) для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает иные категории персональных данных более чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора.

Необходимость обеспечения 4-го уровня защищенности персональных данных при их обработке в информационной системе устанавливается при наличии хотя бы одного из следующих условий:

а) для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает общедоступные персональные данные;

б) для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает иные категории персональных данных сотрудников оператора или иные категории персональных данных менее чем 100000 субъектов персональных данных, не являющихся

При изменении состава ПДн, способов их обработки, добавления новых ИСПДн, необходимо заново определить необходимый уровень защищенности персональных данных.

Операторы обязаны при обработке персональных данных принимать требуемые организационные и технические меры, в том числе при необходимости использовать шифровальные (криптографические) средства для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных, а также от иных неправомерных действий.

6. Правовое обеспечение обработки персональных данных

Обработка персональных данных в МБОУ СОШ №3 г. Кашин производится в соответствии со следующими нормативными и организационно-распорядительными документами:

- Трудовым Кодексом Российской Федерации;
- ФЗ от 10.07.1992г. №3266-1 «Об образовании»;
- Законом Тверской области от 07.05.2008г. № 56-ЗО «Об образовании в Тверской области»;
- ФЗ №152 «О персональных данных» от 27.07.2006;
- Постановление Правительства РФ №687 от 15.09.2008;
- Постановление Правительства РФ №781 от 17.11.2007;
- Указ Президента РФ №609 от 30.05.2005;

7. Состав персональных данных, обрабатываемых в информационных системах. Цели и способы обработки персональных данных.

В состав информационной системы МБОУ СОШ №3 г. Кашин входит ряд ИСПДн, в которых в зависимости от выполняемых ИСПДн функций обрабатываются персональные данные учащихся МБОУ СОШ №3 г. Кашин, их родителей (законных представителей), а также работников МБОУ СОШ №3 г. Кашин. Список персональных данных указан в Перечне персональных данных, обрабатываемых в информационных системах персональных данных МБОУ СОШ №3 г. Кашин(Приложение №5)

Персональные данные обучающихся и их законных представителей обрабатываются с использованием средств автоматизации или без использования таких средств, с целью осуществления индивидуального учета результатов освоения обучающимся образовательных программ, обеспечения учебно-воспитательного процесса, предоставления мер социальной поддержки, обеспечения медицинского обслуживания, формирования баз данных, в том числе электронных, для обеспечения принятия управленческих решений, формирования информационных систем, имеющих федеральный статус, а также хранения в архивах данных об этих результатах.

Персональные данные работников МБОУ СОШ №3 г. Кашин обрабатываются с использованием средств автоматизации или без использования таких средств, с целью обеспече-

ния соблюдения законов и иных нормативных правовых актов, трудоустройства работников, обучения и продвижения по службе, обеспечения личной безопасности работников, контроля количества и качества выполняемой работы и обеспечения сохранности имущества.

Порядок работы с персональными данными работников определен в Положении о работе с персональными данными работников МБОУ СОШ №3 г. Кашин.

8. Учет и хранение документов, содержащих персональные данные

Учет и хранение в МБОУ СОШ №3 г. Кашин документов, содержащих персональные данные, следует осуществлять в соответствии с документом «Положение об обработке персональных данных без использования средств автоматизации».

9. Организация работ по защите персональных данных в информационной системе МБОУ СОШ №3 г. Кашин

В соответствии с законодательством Российской Федерации, защита персональных данных МБОУ СОШ №3 г. Кашин включает следующие организационные мероприятия:

- Определить (или уточнить) состав и категории обрабатываемых персональных данных;
- Определить порядок обработки персональных данных;
- Подготовить должностные инструкции сотрудников, обрабатывающих персональные данные;
- Назначить ответственных за работу с персональными данными;
- Обеспечить охрану персональных данных;
- Осуществить (или уточнить) классификацию действующих информационных систем, обрабатывающих персональные данные;
- Провести учет применяемых средств защиты информации, эксплуатационной и технической документации к ним, носителей персональных данных;
- Провести необходимые организационные и технические мероприятия для обеспечения защиты: персональных данных, обрабатываемых без использования средств автоматизации; информационных систем, обрабатывающих персональные данные;
- Провести учет лиц, допущенных к работе с персональными данными в информационной системе;
- Провести учет персональных данных, обрабатываемых в МБОУ СОШ №3 г. Кашин;
- Вести журнал учета обращений субъектов персональных данных (Приложение №2);
- Доработать План внутренних проверок состояния защиты персональных данных (См. Приложение №3);

- Вести журнал учета ключей от помещений (Приложение №4);
- Определить перечень ПДн, обрабатываемых в ИСПДн (Приложение №5);
- Вести журнал результатов внутренних проверок состояния защиты персональных данных (Приложение №6)
- Провести обучение лиц, использующих средства защиты информации, применяемые в информационных системах, правилам работы с ними в соответствии с документацией;
- Организовать контроль за соблюдением условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией;
- Организовать процедуру разбирательства и составления заключений по фактам несоблюдения условий хранения носителей персональных данных, использования средств защиты информации, которые могут привести к нарушению конфиденциальности персональных данных или другим нарушениям, приводящим к снижению уровня защищенности персональных данных, разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений.

10. Обязанности и ответственность должностных лиц

Разработка и осуществление мероприятий по обеспечению безопасности персональных данных при их обработке возлагается на лицо, ответственное за организацию обработки и защиты персональных данных, администратор локальной вычислительной сети (ЛВС). Кроме того, ответственность за выполнение требований настоящего Положения несут все пользователи ИСПДн.

Лицо, ответственное за организацию обработки и защиты персональных данных МБОУ СОШ №3 г. Кашин:

- несет ответственность за нарушения порядка допуска работника к сведениям конфиденциального характера;
- проводит регулярно, не реже одного раза в квартал, инструктаж работников МБОУ СОШ №3 г. Кашин по вопросу обеспечения защиты сведений конфиденциального характера;
- организует выполнение требований настоящего Положения и иных нормативных документов по обеспечению режима защиты информации сотрудниками на рабочих местах;
- определяет информационные ресурсы подразделения, подлежащие защите, уязвимые места, проводят анализ риска их использования и реализации рентабельных средств защиты;
- информирует отдел информационных технологий об изменениях в статусе любого сотрудника, использующего ресурсы информационных систем.

Администратор ЛВС осуществляет организацию и контроль мероприятий, связанных с защитой информации при работе в ЛВС, функционированием средств защи-

ты персональных данных и использовании ресурсов ЛВС в соответствии с «Инструкцией администратора ЛВС».

Пользователи ИСПДн отвечают за соблюдение политики информационной безопасности, принятой в МБОУ СОШ №3 г. Кашин, и докладывают лицу, ответственному за организацию обработки и защиты ПДн о любом подозрении при нарушении информационной защиты.

Пользователи ИСПДн обязаны:

- до получения доступа к конфиденциальным документам и сведениям изучить требования настоящего Положения, других нормативных документов по защите персональных данных, действующих в МБОУ СОШ №3 г. Кашин, в части их касающейся;
- хранить в тайне персональные данные, ставшие им известными по работе или иным путем, пресекать действия других лиц, которые могут привести к разглашению персональных данных, сообщать о фактах несанкционированного доступа и действий со стороны других исполнителей, случаях утечки и разрушения обрабатываемой информации;
- знакомиться с конфиденциальными документами и сведениями, к которым получили доступ в силу своих служебных обязанностей, правильно определять конфиденциальность документов, строго соблюдать правила их пользования, порядок учета и хранения;
- при составлении конфиденциальных документов, содержащих персональные данные, ограничиваться минимальными, действительно необходимыми конфиденциальными сведениями; определять количество экземпляров конфиденциальных документов, в строгом соответствии со служебной необходимостью и не допускать рассылки их адресатам, к которым они не имеют отношения;
- при работе с конфиденциальными документами, содержащими персональные данные, на рабочем месте держать только те конфиденциальные документы, с которыми осуществляется работа; все остальные хранить в сейфе (в металлическом шкафу);
- соблюдать правила работы со средствами защиты информации и установленный режим разграничения доступа к техническим средствам, программам, данным, файлам с персональными данными при ее обработке и другие требования установленные МБОУ СОШ №3 г. Кашин;
- при увольнении, уходе в отпуск, отъезде в длительную командировку сдавать или отчитываться перед подразделением которое отвечает за учет и хранение конфиденциальных сведений, содержащих персональные данные, за все числящиеся за ними конфиденциальные документы;
- знакомить представителей других организаций с конфиденциальными документами, содержащими персональные данные, только по согласованию и с письменного разрешения директора МБОУ СОШ №3 г. Кашин, при наличии документов у представителей других организаций, удостоверяющих их личность;

Пользователям ИСПДн запрещается:

- сообщать свои пароли кому бы то ни было, и разрешать входить в сеть под своим именем; подбирать или отгадывать чужие пароли;
- изменять конфигурационную настройку операционной системы; добавлять, изменять или удалять программное обеспечение, отдельные компоненты операционной системы;
- модифицировать чужие файлы, если по каким-то причинам у них есть доступ на запись;
- использовать персональные данные в открытых документах, на автоматизированных рабочих местах, не предназначенных для обработки (хранения) персональных данных;
- сообщать устно или письменно посторонним лицам персональные данные;
- выполнять работы, связанные с обработкой персональных данных, на дому;
- снимать копии с документов, содержащих персональные данные, или производить выписки из них без письменного разрешения руководителя подразделения;
- передавать и принимать без росписи документы, содержащие персональные данные;
- уничтожать самостоятельно (без согласования с руководителем подразделения) персональные данные;
- несанкционированно тиражировать, передавать и модифицировать программные средства защиты информации.

Детальные обязанности работников МБОУ СОШ №3 г. Кашин в части защите информации должны быть указаны в должностных инструкциях и положениях о соответствующих подразделениях. Допуск работников к работе с ПДн проводится в соответствии с Инструкцией по учету лиц, допущенных к обработке ПДн.

Отказ соблюдать настоящее Положение может подвергнуть защищаемую информацию МБОУ СОШ №3 г. Кашин недопустимому риску потери конфиденциальности, целостности или доступности при ее хранении, обработке или передаче.

При выявлении фактов нарушения прав доступа к сведениям конфиденциального характера руководителям структурных подразделений МБОУ СОШ №3 г. Кашин необходимо немедленно информировать об этом директора или его заместителя. По всем выявленным фактам проводятся служебные разбирательства с выяснением причин и обстоятельств произошедшего и с принятием дисциплинарных мер в отношении виновных нарушителей. При этом учитывается, что работники МБОУ СОШ №3 г. Кашин, разгласившие сведения конфиденциального характера, а также работники, по вине которых произошла утеря документов, несут ответственность, предусмотренную действующим законодательством Российской Федерации, внутренними документами МБОУ СОШ №3 г. Кашини условиями трудового договора.

**План внутренних проверок состояния защиты
персональных данных**

Мероприятие	Периодичность	Исполнитель
Контроль над соблюдением режима обработки ПДн	Ежемесячно	
Контроль над соблюдением режима защиты	Ежемесячно	
Контроль над выполнением антивирусной защиты	Ежемесячно	
Контроль над соблюдением режима защиты при подключении к сетям общего пользования и (или) международного обмена	Ежемесячно	
Проведение обследований на предмет выявления изменений в режиме обработки и защиты ПДн	Ежегодно	
Контроль за обновлениями программного обеспечения и единообразия применяемого ПО на всех элементах ИСПДн	Ежемесячно	
Контроль за обеспечением резервного копирования	Ежемесячно	
Организация анализа и пересмотра имеющихся угроз безопасности ПДн, а так же предсказание появления новых, еще неизвестных, угроз	Ежегодно	
Поддержание в актуальном состоянии нормативно-организационных документов	Ежемесячно	

ПЕРЕЧЕНЬ
персональных данных, обрабатываемых в информационных системах персональных данных
МБОУ СОШ №3 г. Кашин

№ п/п	Наименование сведений	Субъекты ПДн	Наименование ИСПДн, где возможна обработка ПДн	Помещения, где может находиться ИСПДн
1	ФИО, дата рождения, место рождения; адрес, образование, контакты, родственные связи, успеваемость и посещаемость в образовательном учреждении, данные о прибытии и выбытии в\из образовательного учреждения, сведения об обучении и специализации, продолжение обучения после получения основного общего образования	Обучающийся	Локальный документооборот	Кабинеты директора, секретаря и администрации
2	ФИО, дата рождения, контактный телефон, адрес прописки, адрес фактического проживания, паспортные данные, ФИО родителей, родственные связи	Обучающийся	АИС «Школа»	Кабинеты:
3	ФИО, дата рождения, пол, домашний адрес, контактные телефоны, место работы, занимаемая должность	Родитель (Законный представитель)	Локальный документооборот	Кабинеты директора, секретаря и администрации
4	ФИО, место работы, занимаемая должность, контактные телефоны, адрес фактического проживания	Родитель (Законный)	АИС «Школа»	Кабинеты:

		представитель)		
5	ФИО, занимаемая должность, контактные данные	Сотрудник	Локальный документооборот	Кабинеты директора, секретаря и администрации
6	ФИО, паспортные данные, финансовая информация, сведения о месте жительства, контактный телефон, социальный статус, сведения страхового свидетельства государственного пенсионного страхования, свидетельства о постановке на учет в налоговом органе физического лица по месту жительства, сведения о воинском учете, сведения о ближайших родственниках, данные о трудовом договоре, сведения о трудовом стаже, сведения о расчетах и начислениях, суммы взносов и доход	Сотрудник	ИСПДн кадрового учета	Кабинеты директора, секретаря и администрации
7	ФИО, ИНН, дата и место рождения, сведения о гражданстве, знание иностранных языков, информация об образовании, информация о трудовой деятельности, трудовой стаж, семейное положение, состав семьи, паспортные данные, адрес места жительства, контактные телефоны, сведения о воинском учете, данные об аттестации, повышении квалификации, наградах, медалях, поощрениях, почетных званиях.	Сотрудник	АИС «Школа»	Кабинеты:

Журнал внутренних проверок мер обеспечения безопасности ПДн

Журнал начат: « » _____ 20__ г.

Журнал завершен: « » _____ 20__ г.

Должность _____
/Ф.И.О. должностного лица/

Должность _____
/Ф.И.О. должностного лица/

№ п/п	Дата проверки	Результат проверки	Ф.И.О. проверяющего	Подпись	Примечания

