**Принято:**
решением Совета школы
от «20» февраля 2023 г.
протокол № 3

**Утверждаю:**
Директор МБОУ СОШ №17 г. Твери
_____ И.С.Орлова
Приказ № 35/3-ОД от 05.04.2023 года

# ПОЛОЖЕНИЕ
## о работе с персональными данными в МБОУ СОШ №17

### 1. Назначение и область действия Положения

Настоящее положение о персональных данных (далее - Положение) содержит общие положения, 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 Муниципальном бюджетном общеобразовательном учреждении средней общеобразовательной школе с углубленным изучением математики №17 г. Твери (далее - МБОУ СОШ №17), описание состава документов правового обеспечения обработки персональных данных в МБОУ СОШ №17, 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.

1.1. Под персональными данными работника понимается информация, касающаяся конкретного работника, необходимая оператору (руководителю образовательного учреждения и (или) уполномоченному им лицу) в связи с трудовыми отношениями, возникающими между работником и работодателем (руководителем образовательного учреждения).

1.2. Под персональными данными обучающегося понимается информация, касающаяся конкретного обучающегося, необходимая оператору (руководителю образовательного учреждения и (или) уполномоченному им лицу) в связи с отношениями, возникающими между родителями (законными представителями) обучающегося и образовательным учреждением (руководителем образовательного учреждения).

1.3. Положение устанавливает требования к обработке персональных данных

**Принято:**
решением Совета школы
от «20» февраля 2023 г.
протокол № 3

**Утверждаю:**
Директор МБОУ СОШ №17 г. Твери
_____И.С.Орлова
Приказ № 35/3-ОД от 05.04.2023 года

# ПОЛОЖЕНИЕ
# о работе с персональными данными в МБОУ СОШ №17

## 1. Назначение и область действия Положения

Настоящее положение о персональных данных (далее - Положение) содержит общие положения, 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 Муниципальном бюджетном общеобразовательном учреждении средней общеобразовательной школе с углубленным изучением математики №17 г. Твери (далее - МБОУ СОШ №17), описание состава документов правового обеспечения обработки персональных данных в МБОУ СОШ №17, 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.

1.1. Под персональными данными работника понимается информация, касающаяся конкретного работника, необходимая оператору (руководителю образовательного учреждения и (или) уполномоченному им лицу) в связи с трудовыми отношениями, возникающими между работником и работодателем (руководителем образовательного учреждения).

1.2. Под персональными данными обучающегося понимается информация, касающаяся конкретного обучающегося, необходимая оператору (руководителю образовательного учреждения и (или) уполномоченному им лицу) в связи с отношениями, возникающими между родителями (законными представителями) обучающегося и образовательным учреждением (руководителем образовательного учреждения).

1.3. Положение устанавливает требования к обработке персональных данных

в МБОУ СОШ №17 в соответствии с видами деятельности, указанными в уставе ОУ, и политикой информационной безопасности ОУ.

Все работники МБОУ СОШ №17 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.

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

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

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

***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.

***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.

Оператор (руководитель образовательного учреждения и (или) уполномоченное им лицо) обрабатывает персональные данные работников, учащихся, их родителей (законных представителей) и иных лиц (субъектов персональных данных) в соответствии с определенными в уставе целями. При достижении целей персональные данные удаляются либо передаются на архивное хранение в виде документированной информации в течение сроков, определенных требованиями номенклатуры дел.

При обработке персональных данных обеспечиваются точность персональных данных, их достаточность и актуальность. Неполные и неточные данные уточняются или удаляются.

Оператор (руководитель образовательного учреждения и (или) уполномоченное им лицо) обрабатывает персональные данные:

− без использования средств автоматизации и в ИСПДн;

− в статистических или иных исследовательских целях при условии обезличивания.

Оператор (руководитель образовательного учреждения и (или) уполномоченное им лицо) не передает персональные данные иностранным государствам, иностранным физическим лицам и иностранным юридическим лицам и не обрабатывает биометрические персональные данные в целях установления личности.

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. Документы, содержащие сведения, составляющие персональные данные

Документы, содержащие сведения, необходимые для заключения, изменения или прекращения трудового договора с работником (оформления трудовых отношений с работником):

- паспорт;
- документы об образовании, квалификации;
- медицинское заключение об отсутствии противопоказаний для занятия конкретным видом деятельности в образовательном учреждении;
- страховое свидетельство государственного пенсионного страхования;
- ИНН;
- приговор суда о запрете заниматься педагогической деятельностью или занимать руководящие должности;
- справка об отсутствии судимости;
- документ воинского учета.

Документы, содержащие сведения, необходимые для предоставления работнику гарантий и компенсаций, установленных действующим законодательством:

- документы о составе семьи;
- документы о состоянии здоровья (сведения об инвалидности и т.п.);
- документы о состоянии здоровья детей и других близких родственников (например, справки об инвалидности, о наличии хронических заболеваний);
- документы, подтверждающие право на дополнительные гарантии и компенсации по определенным основаниям, предусмотренным законодательством (донорстве, нахождении в зоне воздействия радиации в связи с аварией на Чернобыльской АЭС и т.п.);
- документы о беременности работницы;
- документы о возрасте малолетних детей;
- документы о месте обучения детей.

Документы, содержащие сведения, необходимые для реализации конституционного права на получение образования (заключения договора с родителями (законными представителями) обучающегося):

- документ, удостоверяющий личность обучающегося (свидетельство о рождении или паспорт);

- документ о получении образования, необходимого для поступления в соответствующий класс (личное дело, справка с предыдущего места учебы и т.п.);
- медицинское заключение об отсутствии противопоказаний для обучения в образовательном учреждении конкретного вида и типа;
- медицинское заключениео возможности изучения предметов, представляющих повышенную опасность для здоровья (физкультура, информатика и т.п.);
- документ о месте проживания;
- паспорт одного из родителей (законных представителей) обучающегося;
- полис обязательного медицинского страхования.

Документы, содержащие сведения, необходимые для предоставления обучающемуся гарантий и компенсаций, установленных действующим законодательством:

- документы о составе семьи;
- документы о состоянии здоровья (сведения об инвалидности, наличии хронических заболеваний);

документы, подтверждающие право на дополнительные гарантии и компенсации по определенным основаниям, предусмотренным законодательством (родители-инвалиды, неполная семья, ребенок-сирота, опекаемый и т.п.).

## 4. Порядок получения и обработки персональных данных

4.1 Обработка персональных данных работника.

4.1.1. Обработка (получение, сбор, использование, передача, хранение и защита) персональных данных работника может осуществляться исключительно в целях:

- обеспечения соблюдения законов и иных нормативных правовых актов;
- содействия работникам в трудоустройстве, обучении и продвижении по службе;
- обеспечения личной безопасности работников;
- контроля количества и качества выполняемой работы;
- обеспечения сохранности имущества в минимально необходимом для этих целей объеме.

4.1.2. Все персональные данные работника можно получать только у него самого, за исключением случаев, предусмотренных федеральным законом. Если персональные данные работника возможно получить только у третьей стороны, то работник должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие. Работник должен быть проинформирован о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа дать письменное согласие на их получение.

4.1.3. В соответствии со ст. 24 Конституции РФ оператор (руководитель образовательного учреждения и (или) уполномоченное им лицо) вправе осуществлять сбор, передачу, уничтожение, хранение, использование информации о политических, религиозных, других убеждениях и частной жизни, а также информации, нарушающей тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений работника только с его письменного согласия или на основании судебного решения.

4.2. Обработка персональных данных обучающегося.

4.2.1. Обработка (получение, сбор, использование, передача, хранение и защита) персональных данных обучающегося может осуществляться исключительно в целях:

- обеспечения соблюдения законов и иных нормативных правовых актов;
- содействия обучающимся в обучении, трудоустройстве;
- обеспечения их личной безопасности;
- контроля количества и качества обучения;
- обеспечения сохранности имущества в минимально необходимом для этих целей объеме.

4.2.2. Все персональные данные несовершеннолетнего обучающегося до получения им основного общего образования можно получать только у его родителей (законных представителей). Если персональные данные обучающегося возможно получить только у третьей стороны, то родители (законные представители) обучающегося должны быть уведомлены об этом заранее и от них должно быть получено письменное согласие. Родители (законные представители) обучающегося должны быть проинформированы о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа дать письменное согласие на их получение.

4.2.3. Все персональные данные несовершеннолетнего обучающегося после получения им основного общего образования или совершеннолетнего обучающегося можно получать только у него самого. Если персональные данные такого обучающегося возможно получить только у третьей стороны, то он должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие. Такой обучающийся должен быть проинформирован о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа дать письменное согласие на их получение.

4.2.4. В соответствии со ст. 24 Конституции РФ, оператор (руководитель образовательного учреждения и (или) уполномоченное им лицо) вправе осуществлять сбор, передачу, уничтожение, хранение, использование информации о политических, религиозных, других убеждениях и частной жизни, а также информации, нарушающей тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений обучающегося только с его письменного согласия (согласия родителей (законных представителей) несовершеннолетнего обучающегося до получения им основного общегообразования), форма которого определяется ч.4 ст.9 Федерального закона «О защите персональных данных», или на основании судебного решения.

4.2.5. Оператор (руководитель образовательного учреждения и (или) уполномоченное им лицо) не обрабатывает и не передает третьим лицам без согласия субъекта персональных данных, его законного представителя информацию о национальности, расовой принадлежности, политических, религиозных, философских убеждениях, состоянии здоровья, интимной жизни субъекта персональных данных, за исключением случаев, когда такая информация необходима:

- для защиты жизни, здоровья или других жизненно важных интересов субъекта персональных данных, а получить согласие невозможно;
- в медико-профилактических целях;
- для выполнения требований законодательства о безопасности.

4.2.6. В случае прекращения трудового договора, расторжения и/или исполнения гражданско-правового договора, прекращения образовательных отношений с субъектом персональных данных оператор (руководитель образовательного учреждения и (или) уполномоченное им лицо) незамедлительно прекращает обработку персональных данных соответствующих субъектов и уничтожает их персональные данные в срок, не превышающий тридцати рабочих дней с даты достижения цели обработки персональных данных. Уничтожение по достижении цели обработки не распространяется на документированную информацию, переданную на архивное хранение.

4.2.7. При использовании оператором (руководителем образовательного учреждения и (или) уполномоченным им лицом) типовых форм документов, характер информации в которых предполагает или допускает включение в них персональных данных, соблюдаются следующие условия:

− типовая форма содержит: сведения о цели обработки персональных данных без использования средств автоматизации; наименование и адрес школы; 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 способов обработки персональных данных;

− при необходимости получения письменного согласия на обработку персональных данных типовая форма предусматривает поле, в котором субъект персональных данных может поставить отметку о своем согласии на обработку персональных данных без использования средств автоматизации;

− типовая форма составляется таким образом, чтобы каждый из субъектов персональных данных, содержащихся в документе, мог ознакомиться со своими персональными данными, не нарушая прав и законных интересов иных субъектов персональных данных.

## 5. 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.

## 6. Хранение, доступ и использование персональных данных

6.1. Комплекс мер по обеспечению безопасности персональных данных в МБОУ СОШ №17 направлен на защиту персональных данных от неправомерного или случайного уничтожения, изменения, блокирования, копирования, распространения и иных неправомерных действий.

6.2. Безопасность персональных данных при их обработке в ИСПДн обеспечивается с помощью системы защиты персональных данных, нейтрализующей актуальные угрозы.

6.3. Порядок действий по защите персональных данных с использованием средств автоматизации и без таких средств определяет план мероприятий, утвержденный приказом руководителя ОУ.

6.4. При обработке персональных данных места хранения материальных носителей определяются в отношении каждой категории персональных данных.

6.4.1. Персональные данные работника размещаются в личной карточке работника формы Т-2, которая заполняется после издания приказа о его приеме на работу. Личные карточки работников хранятся в специально оборудованных несгораемых шкафах в алфавитном порядке.

6.4.2. Персональные данные обучающегося размещаются в его личном деле, которое заполняется после издания приказа о зачислении в школу. Личные дела обучающихся формируются в папках классов, которые хранятся в специально оборудованных несгораемых шкафах.

6.4.3. Право доступа к личным данным работников и обучающихся имеют только оператор (руководитель образовательного учреждения и (или) уполномоченное им лицо) и лица, уполномоченные действующим законодательством.

6.4.4. Личные карточки уволенных работников хранятся в архиве образовательного учреждения в алфавитном порядке в течение 75 лет (ст. 339 «Перечня типовых управленческих документов, образующихся в деятельности организаций, с указанием сроков хранения», утвержденного Руководителем Федеральной архивной службы России 6 октября 2000 года).

6.5. В целях обеспечения безопасности персональных данных в качестве организационных и технических мер руководитель ОУ:

- назначает лицо, ответственное за организацию обработки персональных данных;

− определяет список лиц, допущенных к обработке персональных данных, в т. ч. при работе с документированной информацией, содержащей персональные данные;

− определяет места хранения материальных носителей персональных данных;

− устанавливает правила доступа к персональным данным, обрабатываемым в ИСПДн, а также обеспечивает регистрацию и учет всех действий, совершаемых с персональными данными в ИСПДн;

− контролирует эффективность мер, направленных на защиту персональных данных и ИСПДн согласно плану мероприятий по контролю в сфере информационной безопасности. Персональные данные работников и обучающихся хранятся на электронных носителях на сервере образовательного учреждения, а также на бумажных и электронных носителях у оператора (руководителя образовательного учреждения и (или) уполномоченного им лица).

6.6. При работе с персональными данными в целях обеспечения информационной безопасности необходимо, чтобы:

- оператор, осуществляющий работу с персональными данными, не оставлял в свое отсутствие компьютер незаблокированным;
- оператор имел свой персональный идентификатор и пароль, не оставлял его на рабочем месте и не передавал другим лицам.

6.7. Доступ к персональным данным работников без получения специального разрешения имеют:

- руководитель образовательного учреждения;
- заместитель директора, ответственный за работу с персональными данными;
- секретарь учебной части;
- специалист по кадрам (ответственный за ведение кадрового делопроизводства).

6.8. Доступ к персональным данным обучающегося без получения специального разрешения имеют:

- руководитель образовательного учреждения;
- заместители руководителя образовательного учреждения;
- секретарь учебной части;
- классные руководители (только к персональным данным обучающихся своего класса).

6.9. По письменному запросу, на основании приказа руководителя образовательного учреждения, к персональным данным работников и обучающихся могут быть допущены иные лица, в пределах своей компетенции.

6.10. Оператор (руководитель образовательного учреждения и (или) уполномоченное им лицо) при обработке персональных данных должен руководствоваться настоящим Положением и обязан использовать персональные данные работников и обучающихся лишь в целях, для которых они были предоставлены.

## 7. 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».

### *7.1 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".

***7.2 Уровни защищенности 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 данных, 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.

В соответствии с законодательством Российской Федерации, защита персональных данных МБОУ СОШ №17 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 №17;

• Ввести журнал учета обращений субъектов персональных данных (Приложение №2);

• Доработать План внутренних проверок состояния защиты персональных данных (См. Приложение №3);

• Ввести 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.

## 8. Передача персональных данных

8.1. Персональные данные работника (обучающегося) не могут быть сообщены третьей стороне без письменного согласия работника, обучающегося (родителей (законных представителей) несовершеннолетнего обучающегося до получения им основного общего образования), за исключением случаев, когда это необходимо для предупреждения угрозы жизни и здоровью работника (обучающегося), а также в случаях, установленных федеральным законом.

8.2. Передача персональных данных работника (обучающегося) его представителям может быть осуществлена в установленном действующим законодательством порядке только в том объеме, который необходим для выполнения указанными представителями их функций.

## 9. Угроза утраты персональных данных

- Под угрозой или опасностью утраты персональных данных понимается единичное или комплексное, реальное или потенциальное, активное или пассивное проявление возможностей внешних или внутренних источников угрозы создавать неблагоприятные события, оказывать дестабилизирующее воздействие на защищаемую информацию.
- Риск угрозы любым информационным ресурсам создают стихийные бедствия, экстремальные ситуации, террористические действия, аварии технических средств и линий связи, другие объективные обстоятельства, а также заинтересованные и незаинтересованные в возникновении угрозы лица.
- Защита персональных данных представляет собой предупреждение нарушения доступности, целостности, достоверности и конфиденциальности персональных данных и обеспечение безопасности информации в процессе управленческой и производственной деятельности организации.
- Защита ПД от неправомерного их использования или утраты должна быть обеспечена Учреждением за счет его средств в порядке, установленном федеральным законом.

«Внутренняя защита»:

- регламентация доступа персонала к конфиденциальным сведениям, документам и базам данных входит в число основных направлений

организационной защиты информации и предназначена для разграничения полномочий между руководителями и специалистами организации;

- для обеспечении внутренней защиты ПД необходимо соблюдать ряд мер: ограничение и регламентация состава работников, функциональные обязанности которых требуют конфиденциальных знаний; избирательное и обоснованное распределение документов и информации между работниками; рациональное размещение рабочих мест работников, при котором исключалось бы бесконтрольное использование защищаемой информации; знание работником требований нормативно — методических документов по защите информации и сохранении тайны; наличие необходимых условий в помещении для работы с конфиденциальными документами и базами данных; организация порядка уничтожения информации; своевременное выявление нарушения требований разрешительной системы доступа работниками подразделения; воспитательная и разъяснительная работа с сотрудниками подразделения по предупреждению утраты ценных сведений при работе с конфиденциальными документами.
- защита персональных данных на электронных носителях. Все папки, содержащие персональные данные учащихся и их родителей (законных представителей), должны быть защищены паролем.
- учреждение обязано в порядке, определенном федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, обеспечивать взаимодействие с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, включая информирование его о компьютерных инцидентах, повлекших неправомерную передачу (предоставление, распространения, доступ) персональных данных.
- учреждение в случае установления факта неправомерной или случайной передачи (предоставления, распространения, доступа) персональных данных, повлекшей нарушение прав субъектов персональных данных, учреждение обязано с момента выявления такого инцидента учреждением, уполномоченным органом по защите прав субъектов персональных данных или иным заинтересованным лицом уведомить уполномоченный орган по защите прав субъектов персональных данных

1) в течение двадцати четырех часов о произошедшем инциденте, о

предполагаемых причинах, повлекших нарушение прав субъектов персональных данных, и предполагаемом вреде, нанесенном правам субъектов персональных данных, о принятие мерах по устранению последствий соответствующего инцидента, а также предоставить сведения о лице, уполномоченном оператором на взаимодействие с уполномоченным органом по защите прав субъектов персональных данных, по вопросам, связанным с выявленным инцидентом;

2) в течении семидесяти двух часов о результатах внутреннего расследования выявленного инцидента, а также предоставить сведения о лицах, действия которых стали причиной выявленного инцидента (при наличии).

«Внешняя защита»:

- для защиты конфиденциальной информации создаются целенаправленные неблагоприятные условия и труднопреодолимые препятствия для лица, пытающегося совершить несанкционированный доступ и овладение информацией. Целью и результатом несанкционированного доступа к информационным ресурсам может быть не только овладение ценными сведениями и их использование, но и их видоизменение, уничтожение, и др;
- под посторонним лицом понимается любое лицо, не имеющее непосредственного отношения к организации, посетители, работники других организационных структур. Посторонние лица не должны знать распределение функций, рабочие процессы, технологию составления, оформления, ведения и хранения документов, дел и рабочих материалов;
- для обеспечения внешней защиты ПД необходимо соблюдать ряд мер: порядок приема, учета и контроля деятельности посетителей; пропускной режим организации; технические средства охраны, сигнализации; требования к защите информации при интервьюировании и собеседованиях.
- Все лица, связанные с получением, обработкой и защитой персональных данных, обязаны подписать обязательство о неразглашении персональных данных учащихся и их родителей (законных представителей).
- По возможности персональные данные обезличиваются.
-

## 10. Права, обязанности и ответственность субъекта персональных данных

• Закрепление прав субъектов персональных данных, регламентирующих защиту его персональных данных, обеспечивает сохранность полной и точной информации о нем.

• Субъект персональных данных принимает решение о предоставлении его персональных данных и дает согласие на их обработку свободно, своей волей и в своем интересе. Согласие на обработку персональных данных должно быть конкретным, предметным, информированным, сознательным и однозначных. Согласие на обработку персональных данных может быть дано субъектом персональных данных или его представителем в любой форме, позволяющей подтвердить факт его получения форме, если иное не установлено федеральным законом. В случае получения согласия на обработку персональных данных от представителя субъекта персональных данных полномочия данного представителя на дачу согласия от имени субъекта персональных данных проверяются Учреждением.

• Родители (законные представители) детей должны быть ознакомлены под расписку с документами организации, устанавливающими порядок обработки персональных данных воспитанников, очередников, учащихся и их родителей (законных представителей), а также об их правах и обязанностях в этой области.

• В целях защиты персональных данных, хранящихся в Учреждении, родители (законные представители) имеют право:

• требовать исключения или исправления неверных, или неполных персональных данных,

• на свободный бесплатный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей персональные данные;

• определять своих представителей для защиты своих персональных данных;

• на сохранение и защиту своей личной и семейной тайны.

• Родители (законные представители) детей обязаны передавать Учреждению комплекс достоверных, документированных персональных данных, состав которых установлен нормативными и распорядительными документами Минобрнауки России, Рособразования и Рособрнадзора, Уставом школы, своевременно сообщать об изменении своих персональных

данных.

• Родители (законные представители) детей ставят Учреждение в известность об изменении фамилии, имени, отчества, адреса проживания, контактные телефонов.

• В целях защиты частной жизни, личной и семейной тайны родители (законные представители) детей не должны отказываться от своего права на обработку персональных данных только с их согласия, поскольку это может повлечь причинение морального, материального вреда.

## 11. Права, обязанности и ответственность оператора персональных данных

• Персональная ответственность — одно из главных требований к организации функционирования системы защиты персональной информации и обязательное условие обеспечения эффективности этой системы.

• Юридические и физические лица, в соответствии со своими полномочиями владеющие информацией о гражданах, получающие и использующие ее, несут ответственность в соответствии с законодательством Российской Федерации за нарушение режима защиты, обработки и порядка использования этой информации.

• Руководитель, разрешающий доступ сотрудника к документу, содержащему персональные сведения учащихся и их родителей (законных представителей), несет персональную ответственность за данное разрешение.

• Каждый сотрудник организации, получающий для работы документ, содержащий персональные данные, несет единоличную ответственность за сохранность носителя и конфиденциальность информации.

• Сотрудник Учреждения, имеющий доступ к ПД в связи с исполнением трудовых обязанностей: обеспечивает хранение информации, содержащей ПД, исключающее доступ к ним третьих лиц. В отсутствие сотрудника на его рабочем месте не должно быть документов, содержащих ПД;

• при уходе в отпуск, служебной командировке и иных случаях длительного отсутствия работника на своем рабочем месте, обязан передать документы и иные носители, содержащие ПД лицу, на которое локальным актом Учреждения (приказом, распоряжением) будет возложено исполнение его трудовых обязанностей. В случае если такое лицо не назначено, то документы и иные носители, содержащие ПД, передаются другому

сотруднику, имеющему доступ к ПД по указанию директора Учреждения.

• при увольнении сотрудника, имеющего доступ к ПД, документы и иные носители, содержащие ПД, передаются другому сотруднику, имеющему доступ к персональным данным по указанию директора Учреждения.

• Доступ к персональных данным учащихся и их родителей (законных представителей) имеют сотрудники Учреждения, которым персональные данные необходимы в связи с исполнением ими трудовых обязанностей согласно перечню должностей.

• В целях выполнения порученного задания и на основании служебной записки с положительной резолюцией директора ОУ, доступ к ПД может быть предоставлен иному работнику, должность которого не включена в Перечень должностей сотрудников, имеющих доступ к персональным данным, и которым они необходимы в связи с исполнением трудовых обязанностей.

• В случае если работодателю оказывают услуги юридические и физические лица на основании заключенных договоров (либо иных оснований) и в силу данных договоров они должны иметь доступ к персональным данным, то соответствующие данные предоставляются работодателем только после подписания с ними соглашения о неразглашении конфиденциальной информации. В исключительных случаях, исходя из договорных отношений с контрагентом, допускается наличие в договорах пунктов о неразглашении конфиденциальной информации, в том числе предусматривающих защиту персональных данных учащихся и их родителей (законных представителей).

• Процедура оформления доступа к ПД включает в себя:

• ознакомление работника под роспись с настоящим Положением. При наличии иных нормативных актов (приказы, распоряжения, инструкции и т.п.), регулирующих обработку и защиту ПД, с данными актами также производится ознакомление работника под роспись.

• истребование с сотрудника (за исключением директора ОУ) письменного обязательства о соблюдении конфиденциальности персональных данных и соблюдении правил их обработки, подготовленного по установленной форме.

• Допуск к персональным данным учащихся и их родителей (законных представителей) других сотрудников работодателя, не имеющих надлежащим образом оформленного доступа, запрещается.

• Передача (обмен и т.д.) персональных данных между подразделениями

ОУ осуществляется только между сотрудниками, имеющими доступ к персональным данным учащихся и их родителей (законных представителей).

• Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту ПД, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с федеральными законами:

• за неисполнение или ненадлежащее исполнение работником по его вине возложенных на него обязанностей по соблюдению установленного порядка работы со сведениями конфиденциального характера работодатель вправе применять предусмотренные Трудовым Кодексом РФ дисциплинарные взыскания;

• должностные лица, в обязанность которых входит ведение персональных данных учащихся и их родителей (законных представителей), обязаны обеспечить каждому возможность ознакомления с документами и материалами, непосредственно затрагивающими его права и свободы, если иное не предусмотрено законом. Неправомерный отказ в предоставлении собранных в установленном порядке документов, либо несвоевременное предоставление таких документов или иной информации в случаях, предусмотренных законом, либо предоставление неполной или заведомо ложной информации — влечет наложение на должностных лиц административного штрафа в размере, определяемом Кодексом об административных правонарушениях;

• в соответствии с Гражданским Кодексом РФ лица, незаконными методами получившие информацию, составляющую служебную тайну, обязаны возместить причиненные убытки;

• уголовная ответственность за нарушение неприкосновенности частной жизни (в том числе незаконное собирание или распространение сведений о частной жизни лица, составляющего его личную или семейную тайну, без его согласия), неправомерный доступ к охраняемой законом компьютерной информации, неправомерный отказ в предоставление собранных в установленном порядке документов и сведений (если эти деяния причинили вред правам и законным интересам граждан), совершенные лицом с использованием своего служебного положения наказывается штрафом, либо лишением права занимать определенные должности или заниматься определенной деятельностью, либо арестом в соответствии с УК РФ.

• Неправомерность деятельности органов государственной власти и организаций по сбору и использованию персональных данных может быть

установлена в судебном порядке.

• Учреждение обязано сообщить родителям (законным представителям) детей о целях, способах и источниках получения персональных данных, а также о характере подлежащих получению персональных данных и возможных последствиях отказа родителей (законных представителей) дать письменное согласие на их получение.

• Учреждение обязано сообщить субъекту персональных данных или его представителю информацию о наличии персональных данных, относящихся к соответствующему субъекту персональных данных, а также предоставить возможность ознакомления с этими персональными данными при обращении субъекта персональных данных или его представителя либо в течении десяти рабочих дней с даты получения запроса субъекта персональных данных или его представителя. Указанный срок может быть продлен, но не более чем на пять рабочих дней в случае направления оператором в адрес субъекта персональных данных мотивированного уведомления с указанием причем с указанием причин продления срока предоставления запрашиваемой информации.

Разработка и осуществление мероприятий по обеспечению безопасности персональных данных при их обработке возлагается на лицо, ответственное за организацию обработки и защиты персональных данных, администратора 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 №17:**

- несет ответственность за нарушения порядка допуска работника к сведениям конфиденциального характера;
- проводит регулярно, не реже одного раза в квартал, инструктаж работников МБОУ СОШ №17 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 защиты персональных данных и использовании ресурсов ЛВС в соответствии с «Инструкцией администратора ЛВС».

**Пользователи ИСПДн** отвечают за соблюдение политики информационной безопасности, принятой в МБОУ СОШ №17, 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 №17, 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 №17;

- 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 №17, 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 №17 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 №17 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 №17 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 №17, разгласившие сведения конфиденциального характера, а также работники, по вине которых произошла утеря документов, несут ответственность, предусмотренную действующим законодательством Российской Федерации, внутренними документами МБОУ СОШ №17 и условиями трудового договора.

Приложение № 1
к Положению о персональных данных

## Лист ознакомления

С Положением о персональных данных в МБОУ СОШ №17, утвержденным приказом №___ от « »_____20__ г. ознакомлены:

| № п/п | Ф.И.О. | Должность | Дата | Подпись |
|---|---|---|---|---|
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

Приложение №2
к Положению о персональных данных

## Журнал учета обращений субъектов персональных данных о выполнении их законных прав при обработке персональных данных

| № п/п | ФИО субъекта ПДн | Дата обращения | Цель обращения |
|---|---|---|---|
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

Приложение №3
к Положению о персональных данных

## 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 | |

Приложение №4
к Положению о персональных данных

## Журнал учета ключей

| № ключа | Помещение | Ф.И.О. получателя | Дата выдачи | Подпись получателя | Примечание |
|---|---|---|---|---|---|
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |

Приложение №5
к Положению о персональных данных

**ПЕРЕЧЕНЬ**
**персональных данных, обрабатываемых в информационных системах персональных данных**
МБОУ СОШ №17

| № п/п | Наименование сведений | Субъекты ПДн | Наименование ИСПДн, где возможна обработка ПДн | Помещения, где может находится 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 | Кабинет директора, серверная, кабинет секретаря кабинет завуча, каб. №26 |
| 2 | ФИО, дата рождения | Обучающийся | информационная система «elljur.ru» | Кабинеты школы |
| 3 | ФИО, дата рождения, пол, домашний адрес, контактные телефоны, место работы, занимаемая должность | Родитель (Законный представитель) | Локальный документооборот | Кабинет директора, кабинет секретаря, кабинет завуча, |
| 4 | ФИО, занимаемая должность, контактные данные | Сотрудник | Локальный документооборот | Кабинет директора, кабинет секретаря, кабинет завуча, |

| | | | | |
|---|---|---|---|---|
| 5 | 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 бухгалтерского и кадрового учета | Бухгалтерия, кабинет директора, серверная |

Приложение №6
к Положению о персональных данных

**Журнал внутренних проверок мер обеспечения безопасности ПДн**

Журнал начат: « »_____20 __ г.

Должность_____

/Ф.И.О. должностного лица/

Журнал завершен: « »_____20 __ г.

Должность _____

/Ф.И.О. должностного лица/

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