УТВЕРЖДЕНО
приказом директора МБОУ «НОШ № 5»
Ким Н.А.
от 14.03.2014 № 17/1

ПОЛОЖЕНИЕ
о работе с персональными данными автоматизированных информационных систем общеобразовательного учреждения МБОУ «НОШ № 5»

1. Общие положения

1.1. Настоящее Положение разработано в соответствии с нормативными правовыми актами и методическими документами в области обеспечения безопасности информации конфиденциального характера:

– Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

– Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»;

– Федеральный закон от 21.12.2012 3 № 273 –ФЗ «Об образовании в Российской Федерации»;

– Постановление Правительства Российской Федерации от 31.08.2013 № 735 «О федеральной информационной системе обеспечения проведения государственной итоговой аттестации обучающихся, освоивших основные образовательные программы осинового общего и среднего общего образования, и приема граждан в образовательные организации для получения среднего профессионального и высшего образования и региональных информационных системах обеспечения проведения государственной итоговой аттестации обучающихся, освоивших основные образовательные программы основного общего и среднего образования», и определяет порядок работы с информацией, содержащей персональные данные, с использованием автоматизированной информационной системы МБОУ «НОШ № 5» (в дальнейшем Учреждение).

1.2. Настоящее Положение устанавливает требования к обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, представляющих собой совокупность персональных данных, содержащихся в базах данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации (далее - информационные системы).

Под техническими средствами, позволяющими осуществлять обработку персональных данных, понимаются средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки персональных данных (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации, применяемые в информационных системах.

1.3. Безопасность персональных данных достигается путем исключения несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий.

Безопасность персональных данных при их обработке в информационных системах обеспечивается с помощью системы защиты персональных данных, включающей организационные меры и средства защиты информации (в том числе шифровальные

(криптографические) средства, средства предотвращения несанкционированного доступа, утечки информации по техническим каналам, программно-технических воздействий на технические средства обработки персональных данных), а также используемые в информационной системе информационные технологии. Технические и программные средства должны удовлетворять устанавливаемым в соответствии с законодательством Российской Федерации требованиям, обеспечивающим защиту информации.

Для обеспечения безопасности персональных данных при их обработке в информационных системах осуществляется защита речевой информации и информации, обрабатываемой техническими средствами, а также информации, представленной в виде информативных электрических сигналов, физических полей, носителей на бумажной, магнитной, магнитно-оптической и иной основе.

1.4. Методы и способы защиты информации в информационных системах устанавливаются Федеральной службой по техническому и экспортному контролю и Федеральной службой безопасности Российской Федерации в пределах их полномочий.

Достаточность принятых мер по обеспечению безопасности персональных данных при их обработке в информационных системах оценивается при проведении государственного контроля и надзора.

1.5. Работы по обеспечению безопасности персональных данных при их обработке в информационных системах являются неотъемлемой частью работ по созданию информационных систем.

2. Основные понятия и определения, используемые в Положении

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

2.2. «Оператор» – государственный орган, муниципальный орган, юридическое или физическое лицо, организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели и содержание обработки персональных данных;

2.3. «Обработка персональных данных» – действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных;

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

2.5. «Использование персональных данных» – действия (операции) с персональными данными, совершаемые оператором в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта персональных данных или других лиц либо, иным образом затрагивающих права и свободы субъекта персональных данных или других лиц;

2.6. «Уничтожение персональных данных» – действия, в результате которых невозможно восстановить содержание персональных данных в автоматизированной информационной системе или в результате которых уничтожаются материальные носители персональных данных;

2.7. «Обезличивание персональных данных» – действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных;

2.8. «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 использования таких средств;

2.9. «Конфиденциальность персональных данных» – обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространения без согласия субъекта персональных данных или наличия иного законного основания;

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

2.11. «Доступ к информации» – возможность получения информации и ее использования. Персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

2.12. «Системный администратор» – сотрудник Учреждения, ответственный за функционирование информационной инфраструктуры Учреждения в установленном штатном режиме работы.

2.13. «Несанкционированный доступ» – доступ к информации или действия с информацией, осуществляемые с нарушением установленных прав и (или) правил доступа к информации или действий с ней с применением штатных средств информационной системы или средств, аналогичных им по своему функциональному предназначению и техническим характеристикам.

2.14. «Угроза безопасности» – совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к конфиденциальной информации, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение конфиденциальной информации, а также иных несанкционированных действий при ее обработке в информационной системе.

3. Цели и задачи обработки персональных данных

3.1. Оператором, организующим и осуществляющим обработку персональных данных, является Учреждение.

3.2. Обработка персональных данных с использованием автоматизированных информационных систем Учреждение осуществляется с целью содействия субъектам персональных данных в осуществлении учебной, научной, трудовой деятельности, обеспечения личной безопасности, учета результатов исполнения договорных обязательств, а также наиболее полного исполнения Учреждением обязательств и компетенций в соответствии с законодательством.

3.3. Обработка персональных данных с использованием автоматизированных информационных систем Учреждения осуществляется для решения следующих задач:

1) учет кадрового состава Учреждения, научной, учебной, методической деятельности работников, мониторинг качества учебного процесса;

2) учет информации об учащихся Учреждения, информации об обучении и посещаемости;

4) комплексный мониторинг деятельности Учреждения;

5) иные задачи, необходимые для деятельности Учреждения.

4. Права субъектов персональных данных

4.1. В соответствии с разделом 2 настоящего Положения к субъектам персональных данных автоматизированных информационных систем Учреждения относятся следующие категории лиц:

- Администрация Учреждения;
- Педагогический коллектив Учреждения;
- Учащиеся Учреждения;
- Иные лица.

4.2. Субъект персональных данных самостоятельно принимает решение о предоставлении своих персональных данных и дает согласие на их обработку.

4.3. Согласие на обработку персональных данных оформляется в письменном виде.

4.4. Согласие на обработку персональных данных может быть отозвано субъектом персональных данных по письменному запросу на имя директора Учреждения с указанием причин отзыва.

4.5. Субъект персональных данных имеет право на получение сведений об операторе, о месте его нахождения, о наличие у оператора персональных данных, относящихся к соответствующему субъекту персональных данных, а также на ознакомление с такими персональными данными.

4.6. Субъект персональных данных вправе требовать от оператора уточнения своих персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки.

4.6. Сведения о персональных данных должны быть предоставлены субъекту персональных данных оператором в доступной форме, и в них не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных.

4.7. Доступ к своим персональным данным предоставляется субъекту персональных данных или его законному представителю оператором при получении письменного запроса субъекта персональных данных или его законного представителя.

Письменный запрос должен быть адресован на имя директора Учреждения, содержать номер основного документа, удостоверяющего личность субъекта персональных данных или его законного представителя, сведения о дате выдачи указанного документа и выдавшем его органе и собственноручную подпись субъекта персональных данных или его законного представителя.

5. Состав персональных данных

5.1. Состав персональных данных, обрабатываемых с использованием автоматизированных информационных систем Учреждения определяется настоящим Положением и соответствует целям и задачам сбора, обработки и использования персональных данных в соответствии с разделом 3 настоящего Положения.

5.2. Перечень сведений, представляемых в качестве персональных данных автоматизированных информационных систем Учреждения зависит от категории субъекта персональных данных и утверждается директором Учреждения (Приложение 1).

5.3. При добавлении новых информационных полей, содержащих персональные данные, в базу данных автоматизированных информационных систем Учреждения проводится дополнительное анкетирование субъектов персональных данных. Если субъект ранее дал согласие на обработку своих персональных данных с использованием автоматизированной

информационной системы, то, заполняя дополнительную анкету, он даёт согласие на обработку дополнительной информации персонального характера, перечень которой указан в анкете.

6. Порядок сбора, хранения и использования персональных данных

6.1. Информация персонального характера может быть получена непосредственно от субъекта персональных данных и только с его письменного согласия.

6.2. Субъекты персональных данных при получении от них согласия на обработку персональных данных в автоматизированной информационной системе должны быть ознакомлены с перечнем собираемых и используемых сведений, с целями и задачами сбора, хранения и использования персональных данных.

6.3. Анкеты, содержащие информацию персонального характера, а также согласие на обработку персональных данных с использованием автоматизированной информационной системы ОУ должны храниться в личном деле.

6.5. Ввод персональных данных в автоматизированную информационную систему ОУ осуществляется сотрудником в соответствии с его должностными обязанностями. На бумажном носителе информации, содержащей персональные данные (анкеты, личные листки и др.) работник, осуществляющий ввод данных, оставляет отметку с информацией о должности, фамилии, имени, отчестве лица, осуществившего ввод данных, а также дату ввода информации.

6.6. Сотрудники, осуществляющие ввод и обработку данных с использованием автоматизированных информационных систем Учреждения, несут ответственность за достоверность и полноту введенной информации.

6.7. Сотрудники, осуществляющие ввод и обработку данных с использованием автоматизированных информационных систем Учреждения, в соответствии с должностными обязанностями и установленными регламентами должны проверять хранящиеся персональные данные на актуальность и не должны вносить изменения, противоречащие информации, полученной непосредственно от субъекта персональных данных.

6.8. При работе с программными средствами автоматизированных информационных систем ОУ, реализующими функции просмотра и редактирования персональных данных, запрещается демонстрация экранных форм, содержащих такие данные, лицам, не имеющим соответствующих должностных обязанностей.

6.9. Порядок работы с документами и отчетами, подготовленными с использованием автоматизированных информационных систем Учреждения и содержащими персональные данные, регламентируется настоящим Положением. Назначение документа или отчета, содержащего персональные данные, и его содержание должны соответствовать должностным обязанностям лица, подготовившего отчет, а также лица, для которого данный отчет подготовлен.

6.10. Хранение персональных данных автоматизированных информационных систем ОУ осуществляется на сервере(ах) Учреждения с использованием специализированного программного обеспечения, отвечающего требованиям информационной безопасности.

6.11. Хранение резервных и технологических копий баз данных автоматизированных информационных систем, содержащих информацию персонального характера, осуществляется на сервере(ах) Учреждения и оптических, магнитооптических и прочих носителях, доступ к которым ограничен.

6.12. Вынос резервных и технологических копий баз данных автоматизированных информационных систем, содержащих информацию персонального характера, из Учреждения запрещен. Передача и копирование резервных и технологических копий баз данных допустима только для прямого использования с целью технологической поддержки автоматизированных информационных систем.

6.13. В случае если для научных, прикладных исследований, для решения задач статистики необходимо сохранить персональные данные, которые больше не используются в тех целях, ради которых они были собраны, эти данные могут сохраняться преимущественно в обезличенной форме в виде анонимных сведений.

6.14. На сайт Учреждения могут быть размещены общедоступные персональные данные, перечень которых определяется по согласованию с субъектом таких данных на момент передачи в открытые источники.

6.15. Безопасность персональных данных при их обработке в информационной системе обеспечивает оператор или лицо, которому на основании договора оператор поручает обработку персональных данных (далее - пользователь) (приложение № 2).

6.15.1.Обеспечение безопасности информации при ее обработке в информационных системах инфраструктуры Учреждения достигается применением организационных и технических мер, направленных на обеспечение режима информационной безопасности. В обязательном порядке подлежат защите технические и программные средства, используемые в информационных системах инфраструктуры Учреждения.

6.15.2. Основными направлениями защиты информации являются:

- обеспечение защиты информации от хищения, утраты, утечки, уничтожения, искажения, подделки и блокирования доступа к ней за счет несанкционированного доступа и специальных воздействий;

- обеспечение защиты информации от утечки по техническим каналам при ее обработке, хранении и передаче по каналам связи.

6.15.3. Основными мерами защиты информации являются:

- ограничение доступа пользователей в помещения, где размещены технические средства, позволяющие осуществлять обработку информации;

- ограничение доступа пользователей в помещения, где хранятся носители информации;

- разграничение доступа пользователей к информационным ресурсам;

- использование средств защиты информации, прошедших в установленном порядке процедуру оценки соответствия требованиям безопасности информации;

- использование защищенных каналов связи;

- организация физической защиты помещений и технических средств, позволяющих осуществлять обработку информации;

- размещение дисплеев и других средств отображения информации, исключающее ее несанкционированный просмотр;

- предотвращение внедрения в информационные системы вредоносных программ (программ-вирусов) и программных закладок.

6.16. При обработке персональных данных в информационной системе должно быть обеспечено:

а) проведение мероприятий, направленных на предотвращение несанкционированного доступа к персональным данным и (или) передачи их лицам, не имеющим права доступа к такой информации;

б) своевременное обнаружение фактов несанкционированного доступа к персональным данным;

в) недопущение воздействия на технические средства автоматизированной обработки персональных данных, в результате которого может быть нарушено их функционирование;

г) возможность незамедлительного восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

д) постоянный контроль за обеспечением уровня защищенности персональных данных.

6.17. Мероприятия по обеспечению безопасности персональных данных при их обработке в информационных системах включают в себя:

а) определение угроз безопасности персональных данных при их обработке, формирование на их основе модели угроз;

б) разработку на основе модели угроз системы защиты персональных данных, обеспечивающей нейтрализацию предполагаемых угроз с использованием методов и способов защиты персональных данных, предусмотренных для соответствующего класса информационных систем;

в) проверку готовности средств защиты информации к использованию с составлением заключений о возможности их эксплуатации;

г) установку и ввод в эксплуатацию средств защиты информации в соответствии с эксплуатационной и технической документацией;

д) обучение лиц, использующих средства защиты информации, применяемые в информационных системах, правилам работы с ними;

е) учет применяемых средств защиты информации, эксплуатационной и технической документации к ним, носителей персональных данных;

ж) учет лиц, допущенных к работе с персональными данными в информационной системе;

з) контроль за соблюдением условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией;

и) разбирательство и составление 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;

к) описание системы защиты персональных данных.

6.18. Требования информационной безопасности при работе в сети «Интернет»

При работе с ресурсами сети «Интернет» запрещается:

а) разглашение конфиденциальной информации, ставшей известной работнику Учреждения по служебной необходимости либо иным путем;

б) публикация, загрузка и распространение материалов, содержащих вирусы или другие компьютерные коды, файлы или программы, предназначенные для нарушения, уничтожения либо ограничения функциональности любого компьютерного или телекоммуникационного оборудования или программ, для осуществления несанкционированного доступа, а также серийные номера к коммерческим программным продуктам и программы для их генерации, логины, пароли и прочие средства для получения несанкционированного доступа к платным ресурсам в сети «Интернет», а также размещение ссылок на вышеуказанную информацию;

в) загрузка и запуск «исполняемых» либо иных файлов без предварительной проверки на наличие вирусов установленным антивирусным пакетом.

Вся информация о ресурсах сети «Интернет», посещаемых работникам Учреждения, сохраняется в журнале посещений (ведется в электронном виде).

Системный администратор обязан проводить анализ использования ресурсов сети «Интернет» и в случае необходимости представлять отчет об использовании интернет-ресурсов работниками Учреждения (приложение № 3).

7. Особенности предоставления доступа к персональным данным

7.1. Доступ работников к персональным данным автоматизированной информационной системы Учреждения осуществляется с письменного согласия директора Учреждения.

Работник, которому требуется доступ к персональным данным, подает представление на имя руководителя, в котором указывает цель получения сведений персонального характера и период использования прав доступа.

7.2. Сотрудник, получивший согласие директора Учреждения на доступ к персональным данным, должен быть ознакомлен с настоящим Положением.

7.3. Каждый пользователь имеет индивидуальную учетную запись, которая определяет его права и полномочия в автоматизированных информационных систем. Информация об учетной записи не может быть передана другим лицам. Пользователь несет персональную ответственность за конфиденциальность сведений собственной учетной записи.

7.4. Созданием, удалением и изменением учетных записей пользователей автоматизированных информационных систем занимаются уполномоченные лица в соответствии со своими должностными обязанностями.

7.5. Запрещается использование для доступа к автоматизированных информационных систем Учреждения учетных записей других пользователей.

8. Порядок передачи информации, содержащей персональные данные

8.1. Порядок передачи информации, содержащей персональные данные автоматизированных информационных систем Учреждения, внутри Учреждения определяется должностными обязанностями работников или приказами по Учреждению.

8.2. В соответствии с законодательством Российской Федерации персональные данные автоматизированных информационных систем Учреждения могут быть переданы правоохранительным, судебным органам и другим учреждениям в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства.

8.3. Решение о передаче информации, содержащей персональные данные автоматизированных информационных систем Учреждения третьим лицам, принимается директором Учреждения.

8.4. Вопросами взаимодействия с уполномоченным органом по защите прав субъектов персональных данных в части, касающейся персональных данных автоматизированных информационных систем Учреждения, занимается ответственное лицо за хранение персональных данных в автоматизированных информационных систем Учреждения.

9. Ответственность за нарушение требования настоящего Положения

9.1. Лица, виновные в нарушении требований настоящего Федерального закона, несут гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность.