Приложение №7
к приказу МБОУ СОШ №4
от 12.08.2016 года № 348

ПОЛИТИКА
В ОБЛАСТИ ОБРАБОТКИ И ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ МБОУ СОШ № 4

ВВЕДЕНИЕ

1. Настоящий документ «Политика в отношении обработки персональных данных» (далее - Политика) определяет высокоуровневую политику в отношении обработки МБОУ СОШ № 4 персональных данных субъектов и содержит сведения о реализуемых требованиях к защите персональных данных в МБОУ СОШ № 4.
2. Настоящая Политика разработана на основе действующих правовых и нормативных документов по защите конфиденциальной информации и персональных данных.
3. Под персональными данными в настоящем документе понимается любая информация, относящаяся к прямо или косвенно, определенному или определяемому физическому лицу (субъекту персональных данных).
4. Настоящая Политика утверждается приказом руководителя МБОУ СОШ № 4 и подлежит пересмотру по мере необходимости.

1.Общие положения

Согласно Статье Федерального закона от 25.07.2006 г. № 152-ФЗ МБОУ СОШ № 4 как оператор персональных данных обязан опубликовать, или иным образом обеспечить неограниченный доступ к документу, определяющему его политику в отношении обработки персональных данных, к сведениям о реализуемых требованиях к защите персональных данных.

МБОУ СОШ № 4 в рамках выполнения своей деятельности осуществляет обработку персональных данных и, в соответствии с действующим законодательством Российской Федерации, является оператором персональных данных с соответствующими правами и обязанностями, определенными Федеральным законом № 152 от 27.07.2006 г. «О персональных данных» и иными нормативными правовыми актами Российской Федерации (далее - РФ). Состав обрабатываемых данных, категории субъектов, чьи персональные данные обрабатываются МБОУ СОШ № 4, цели и правовые основания их обработки закреплены для каждой информационной системы МБОУ СОШ № 4 «Перечнем персональных данных, обрабатываемых в ИСПДН».

С целью поддержания деловой репутации и обеспечения выполнения законодательных требований МБОУ СОШ № 4 считает для себя обязательным обеспечение соответствия обработки персональных данных требованиям законодательства РФ в области защиты информации и персональных данных, и требует аналогичных мер от третьих лиц, которым передаются и (или) могут передаваться персональные данные на основании п.3 Постановления Правительства Российской Федерации от 01 ноября 2012 г. №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

1. Принципы, правила и цели обработки персональных данных

Обработка персональных данных осуществляется МБОУ СОШ № 4 с соблюдением принципов и правил, предусмотренных Федеральным законом от 27.07.2006 г. № 152-ФЗ «О персональных данных»:

- обработка персональных данных осуществляется на законной и справедливой основе;

- обработка персональных данных ограничивается достижением конкретных, заранее определенных и законных целей;
- не допускается обработка персональных данных, несовместимая с целями сбора персональных данных;
- не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой;
- обработке подлежат только персональные данные, которые отвечают целям их обработки;
- содержание и объем обрабатываемых персональных данных соответствуют заявленным целям обработки;
- обрабатываемые персональные данные не избыточны по отношению к заявленным целям их обработки;
- при обработке персональных данных обеспечивает точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных;
- МБОУ СОШ № 4 принимает необходимые меры по удалению или уточнению неполных или неточных данных;
- хранение персональных данных в МБОУ СОШ № 4 осуществляется в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом, к примеру Федеральный Закон от 22.10.2004 г. №125-ФЗ «Об архивном деле в Российской Федерации» или договором, стороной которого является субъект персональных данных;
- обрабатываемые персональные данные уничтожаются или обезличиваются по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено законодательством РФ;

Обработка персональных данных осуществляется МБОУ СОШ № 4 только в случаях:

- наличия согласия субъекта персональных данных на обработку его персональных данных, если иное не предусмотрено законодательством РФ;
- наличия заключенного договора, по которому МБОУ СОШ № 4 обязуется осуществлять обработку персональных данных субъектов по поручению оператора;
- необходимости достижения целей, предусмотренных нормативно-правовыми актами Российской Федерации и трудовым законодательством, для осуществления и выполнения возложенных законодательством РФ на МБОУ СОШ № 4 функций, полномочий и обязанностей;
- необходимости осуществления прав и законных интересов МБОУ СОШ № 4 или третьих лиц либо для достижения общественно значимых целей при условии, что при этом не нарушаются права и свободы субъекта персональных данных;
- когда персональные данные открыты для неограниченного круга лиц, доступ к которым предоставлен субъектом персональных данных либо по его просьбе;
- обязательного раскрытия и подлежащих к опубликованию персональных данных в соответствии с законодательством РФ;
- организации пропускного режима на территории МБОУ СОШ № 4.

Согласно требованиям Федерального закона № 152 от 27.07.2006 г. «О персональных данных», МБОУ СОШ № 4 в установленном порядке прошел регистрацию как оператор персональных данных. В открытом и общедоступном реестре операторов персональных данных, размещенном на официальном сайте Роскомнадзора как уполномоченного лица по защите прав и свобод субъектов персональных данных, содержится следующая актуальная информация:
- адрес МБОУ СОШ № 4;
- цели обработки персональных данных;
- категории персональных данных;
- категории субъектов, персональные данные которых обрабатываются;

- правовое основание обработки персональных данных;
- перечень действий с персональными данными, общее описание используемых МБОУ СОШ № 4 способов обработки персональных данных;
- фамилия, имя, отчество физического лица, ответственного в МБОУ СОШ № 4 за организацию обработки персональных данных, и номера его контактных телефонов, почтовые адреса и адреса электронной почты;
- описание мер, которые МБОУ СОШ № 4 обязуется осуществлять при обработке персональных данных, по обеспечению безопасности персональных данных при их обработке
- дата начала обработки персональных данных;
- срок или условие прекращения обработки персональных данных;
- сведения о наличии трансграничной передачи персональных данных в процессе их обработки.

МБОУ СОШ № 4 обязуется не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено законодательством РФ и договором с субъектом.

МБОУ СОШ № 4 не обрабатывает специальные и биометричесике категории персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни, сведения, характеризующие биологические и физические особенности человека. (данный абзац необходимо рассматривать субъективно для каждой информационной системы персональных данных оператора.)

МБОУ СОШ № 4 не осуществляет трансграничную передачу персональных данных субъектов персональных данных.

МБОУ СОШ № 4 не принимает решений, порождающих юридические последствия в отношении субъекта персональных данных или иным образом затрагивающее его права и законные интересы, на основании исключительно автоматизированной обработки его персональных данных.

2. Меры, направленные на обеспечение выполнения МБОУ СОШ № 4 обязанностей, предусмотренных законодательством РФ.

МБОУ СОШ № 4 осуществляет следующие организационно-технические меры для защиты персональных данных:
- назначение МБОУ СОШ № 4 лица, ответственного за организацию обработки персональных данных;
- издание документов, определяющих политику МБОУ СОШ № 4 в отношении обработки персональных данных, локальных актов по вопросам обработки персональных данных, а также локальных актов, устанавливающих процедуры, направленные на предотвращение и выявление нарушений законодательства РФ, устранение последствий таких нарушений;
- применение правовых, организационных и технических мер по обеспечению безопасности персональных данных в соответствии со статьей 19 Федерального закона № 152 «О персональных данных», включая:
- определение угроз безопасности персональных данных при их обработке в информационных системах персональных данных МБОУ СОШ № 4
- применение организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных МБОУ СОШ № 4, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные Правительством РФ уровни защищенности персональных данных;
- применение прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;

- оценка эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационных систем персональных данных МБОУ СОШ № 4 - учет машинных носителей персональных данных;
- обнаружение фактов несанкционированного доступа к персональным данным и принятие мер;
- восстановление персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- установление правил доступа к персональным данным, обрабатываемым в информационных системах персональных данных МБОУ СОШ № 4, а также обеспечение регистрации и учета всех действий, совершаемых с персональными данными в информационных системах персональных данных МБОУ СОШ № 4;
- контроль за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных МБОУ СОШ № 4
- осуществление внутреннего контроля соответствия обработки персональных данных законодательству РФ и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, политике МБОУ СОШ № 4 в отношении обработки персональных данных, локальным актам МБОУ СОШ № 4;
- оценка вреда, который может быть причинен субъектам персональных данных в случае нарушения законодательства РФ, соотношение указанного вреда и принимаемых МБОУ СОШ № 4 мер, направленных на обеспечение выполнения обязанностей, предусмотренных законодательством РФ;
- ознакомление работников МБОУ СОШ № 4, непосредственно осуществляющих обработку персональных данных, с положениями законодательства РФ о персональных данных, в том числе требованиями к защите персональных данных, документами, определяющими политику МБОУ СОШ № 4 в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных, и (или) обучение указанных работников.
- доступ к содержанию электронного журнала сообщений возможен исключительно для администратора безопасности, или лица, ответственного за обеспечение безопасности персональных дынных в информационных системах МБОУ СОШ № 4.

4. Право субъекта персональных данных на доступ к его персональным данным
4.1. Субъект персональных данных имеет право на получение сведений, указанных в части 6 настоящего раздела, за исключением случаев, предусмотренных законодательством РФ. Субъект персональных данных вправе требовать от законных представителей МБОУ СОШ № 4 уточнения его персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.
4.2. Сведения, указанные в части 6 настоящего раздела, предоставляются законными представителями МБОУ СОШ № 4 субъекту персональных данных в доступной форме.
4.3. Сведения, указанные в части 6 настоящего раздела, предоставляются субъекту персональных данных или его представителю законными представителями МБОУ СОШ № 4 при получении запроса субъекта персональных данных или его представителя в письменной форме.
4.4. В случае, если сведения, указанные в части 6 настоящего раздела, а также обрабатываемые персональные данные были предоставлены для ознакомления субъекту персональных данных по его запросу, субъект персональных данных вправе обратиться повторно к законным представителям МБОУ СОШ № 4 или направить МБОУ СОШ № 4 повторный запрос в письменной форме в целях получения сведений, указанных в части 6 настоящего раздела, и ознакомления с такими персональными данными не ранее чем через тридцать дней после первоначального обращения или направления первоначального запроса.

4.5. Субъект персональных данных вправе обратиться повторно к законному представителю МБОУ СОШ № 4 или направить повторный письменный запрос в МБОУ СОШ № 4 в целях получения сведений, указанных в части 6 настоящего раздела, а также в целях ознакомления с обрабатываемыми персональными данными до истечения срока, указанного в части 4 настоящего раздела, в случае, если такие сведения и (или) обрабатываемые персональные данные не были предоставлены ему для ознакомления в полном объеме по результатам рассмотрения первоначального обращения. Повторный запрос должен содержать обоснование направления повторного запроса.
4.6. Субъект персональных данных имеет право на получение информации, касающейся обработки его персональных данных, в том числе содержащей:
1) подтверждение факта обработки персональных данных МБОУ СОШ № 4;
2) правовые основания и цели обработки персональных данных;
3) цели и применяемые МБОУ СОШ № 4 способы обработки персональных данных;
4) наименование и место нахождения МБОУ СОШ № 4, сведения о лицах (за исключением работников образовательного учреждения), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с МБОУ СОШ № 4 или на основании законодательства РФ;
5) обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;
6) сроки обработки персональных данных, в том числе сроки их хранения;
7) порядок осуществления субъектом персональных данных прав, предусмотренных законодательством РФ;
8) информацию об осуществленной или о предполагаемой трансграничной передаче данных;
9) наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению МБОУ СОШ № 4, если обработка поручена или будет поручена такому лицу.

ПРАВИЛА РАБОТЫ С ОБЕЗЛИЧЕННЫМИ ПЕРСОНАЛЬНЫМИ ДАННЫМИ МБОУ СОШ № 4

ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящие Правила работы с обезличенными персональными данными МБОУ СОШ № 4 разработаны с учетом Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» и постановления Правительства РФ от 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных ФЗ «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами».
1.2. Настоящие Правила определяют порядок работы с обезличенными данными МБОУ СОШ № 4 Настоящие Правила утверждаются директором МБОУ СОШ № 4 и действует постоянно.

УСЛОВИЯ ОБЕЗЛИЧИВАНИЯ.

1.3. Обезличивание персональных данных может быть проведено с целью ведения статистических данных, снижения ущерба от разглашения защищаемых персональных данных, снижения класса информационных систем персональных данных МБОУ СОШ № 4 и по достижению целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.
1.4. Способы обезличивания при условии дальнейшей обработки персональных данных:
1.4.1. уменьшение перечня обрабатываемых сведений;
1.4.2. замена части сведений идентификаторами;
1.4.3. обобщение – понижение точности некоторых сведений;

1.4.4. понижение точности некоторых сведений (например, «Место жительства» может состоять из страны, индекса, города, улицы, дома и квартиры, а может быть указан только город);
1.4.5. деление сведений на части и обработка в разных информационных системах;
1.4.6. другие способы.
1.5. Способом обезличивания в случае достижения целей обработки или в случае утраты необходимости в достижении этих целей является сокращение перечня персональных данных.
1.6. Для обезличивания персональных данных годятся любые способы явно не запрещенные законодательно.
1.7. Перечень должностей работников МБОУ СОШ № 4 ответственных за проведение мероприятий по обезличиванию обрабатываемых персональных данных, приведен в п.4 настоящих Правил;
1.7.1. Руководитель МБОУ СОШ № 4 принимает решение о необходимости обезличивания персональных данных;
1.7.2. Лица, непосредственно осуществляющие обработку персональных данных, готовят предложения по обезличиванию персональных данных, обоснование такой необходимости и способ обезличивания, если это необходимо;
1.7.3. Лица, обслуживающие базы данных с персональными данными, совместно с ответственным за организацию обработки персональных данных, осуществляют непосредственное обезличивание выбранным способом.

ПОРЯДОК РАБОТЫ С ОБЕЗЛИЧЕННЫМИ ПЕРСОНАЛЬНЫМИ ДАННЫМИ

1.8. Обезличенные персональные данные не подлежат разглашению и нарушению конфиденциальности.
1.9. Обезличенные персональные данные могут обрабатываться с использования и без использования средств автоматизации.
1.10. При обработке обезличенных персональных данных с использованием средств автоматизации необходимо соблюдение:
1.10.1. парольной политики;
1.10.2. антивирусной политики;
1.10.3. правил работы со съемными носителями (если они используется);
1.10.4. правил резервного копирования;
1.10.5. правил доступа в помещения, где расположены элементы информационных систем;
1.10.6. иных предусмотренных законодательством РФ законов и правовых актов.
1.11. При обработке обезличенных персональных данных без использования средств автоматизации необходимо соблюдение:
1.11.1. правил хранения бумажных носителей;
1.11.2. правил доступа к ним и в помещения, где они хранятся;
1.11.3. иных предусмотренных законодательством РФ законов и правовых актов.

ПЕРЕЧЕНЬ ДОЛЖНОСТЕЙ МБОУ СОШ № 4 ОТВЕТСТВЕННЫХ ЗА ПРОВЕДЕНИЕ МЕРОПРИЯТИЙ ПО ОБЕЗЛИЧИВАНИЮ ОБРАБАТЫВАЕМЫХ ПЕРСОНАЛЬНЫХ ДАННЫХ

1. Директор
2. Заместители директора
3. Секретарь школы
4. Социальный педагог
5. Психологи
6. Педагоги
7. Классные руководители

Приложение №8
к приказу МБОУ СОШ №4
от 12.08.2016 года № 348

Регламент осуществления внутреннего контроля за обеспечением уровня защищенности персональных данных и соблюдений условий использования средств защиты информации, а также соблюдением требований законодательства Российской Федерации по обработке персональных данных в информационных системах персональных данных МБОУ СОШ № 4

1. Общие положения

Настоящий Регламент осуществления внутреннего контроля за обеспечением уровня защищенности персональных данных и соблюдений условий использования средств защиты информации, а также соблюдением требований законодательства Российской Федерации по обработке персональных данных в информационных системах персональных данных (далее – Регламент) устанавливает и определяет единый и обязательный порядок проведения контрольных мероприятий для каждой из подсистем, входящих в систему защиты персональных данных информационных систем персональных данных (далее -ИСПДн) МБОУ СОШ № 4.

Настоящий Регламент утверждается и вводится руководителем МБОУ СОШ № 4. и является обязательным для исполнения.

2. Порядок подготовки к проведению контрольных мероприятий

Контрольные мероприятия за обеспечением уровня защищенности персональных данных и соблюдений условий использования средств защиты информации, а также соблюдением требований законодательства Российской Федерации по обработке персональных данных в ИСПДн МБОУ СОШ № 4.

проводятся в следующих целях:

проверка выполнения требований организационно-распорядительной документации образовательного МБОУ СОШ № 4.

- действующего законодательства Российской Федерации в области обработки и защиты персональных данных;

оценка уровня осведомленности и знаний работников МБОУ СОШ № 4.

- в области обработки и защиты персональных данных (далее - ПДн);
- оценка обоснованности и эффективности применяемых мер и средств защиты.

Виды контрольных мероприятий

Контрольные мероприятия подразделяются на внутренние и внешние. Внутренние контрольные мероприятия осуществляются силами работников МБОУ СОШ № 4. Ответственных за обеспечение безопасности ПДн. При проведении внешних контрольных мероприятий привлекаются сторонние организации.

Кроме того, контрольные мероприятия подразделяются на плановые и внеплановые. Плановые контрольные мероприятия проводятся периодически в соответствии с утвержденным Планом проведения контрольных мероприятий (далее - План) и направлены на постоянное совершенствование системы защиты персональных данных МБОУ СОШ № 4. Внеплановые контрольные мероприятия проводятся на основании решения инженера по безопасности группы информационных технологий. Решение о проведении внеплановых контрольных мероприятий может быть принято в следующих случаях:

- по результатам расследования инцидента информационной безопасности;
- по результатам внешних контрольных мероприятий, проводимых регулирующими органами.

Кроме того любой работник МБОУ СОШ № 4 вправе подготавливать обоснованные предложения о необходимости проведения внеплановых контрольных мероприятий и предоставить их лицу, ответственному за обеспечение безопасности ПДн.

План проведения контрольных мероприятий

Для проведения плановых внутренних контрольных мероприятий лицо, ответственное за обеспечение безопасности персональных данных, разрабатывает План внутренних контрольных мероприятий на текущий год.

План проведения внутренних контрольных мероприятий (как плановых, так и внеплановых) включает следующие сведения по каждому из мероприятий:

- цели проведения контрольных мероприятий;
- задачи проведения контрольных мероприятий,
- объекты контроля (процессы, подразделения, информационные системы и т.п.);
- состав участников, привлекаемых для проведения контрольных мероприятий;
- сроки и этапы проведения контрольных мероприятий.

Общий срок контрольных мероприятий не должен превышать пяти рабочих дней. При необходимости срок проведения контрольных мероприятий может быть продлен, но не более чем на десять рабочих дней, соответствующие изменения отображаются в Отчете, выполняемом по результатам проведенных контрольных мероприятий (см. раздел 0).

Оформление результатов проведенных контрольных мероприятий

По итогам проведения внутренних контрольных мероприятий лицо, ответственное за обеспечение безопасности персональных данных, разрабатывает отчет, в котором указывается:

- описание проведенных мероприятий по каждому из этапов в соответствии с планом;
- отклонения от плана, в случае их наличия;
- перечень и описание выявленных нарушений;
- рекомендации по устранению выявленных нарушений.
- заключение по итогам проведения внутреннего контрольного мероприятия.

Отчет передается на рассмотрение руководству МБОУ СОШ № 4.

Общая информации о проведенном контрольном мероприятий фиксируется в Журнале учета мероприятий по обеспечению и контролю безопасности ПДн, обрабатываемых в ИСПДн МБОУ СОШ № 4. (см. Приложение 1 настоящего Регламента).

3. Общий порядок проведения контрольных мероприятий

Контрольные мероприятия проводятся при обязательном участии лица, ответственному за обеспечение безопасности ПДн, также по его ходатайству к проведению контрольных мероприятий могут привлекаться администраторы информационных систем, администраторы информационной безопасности.

Лицо, ответственное за обеспечение безопасности ПДн, не позднее чем за три рабочих дня до начала проведения контрольных мероприятий уведомляет всех работников, у которых планируется проведение контрольных мероприятий, и направляет им для ознакомления План проведения контрольных мероприятий. При проведении внеплановых контрольных мероприятий уведомление не требуется.

3.1.Контрольные мероприятия в подсистеме управления доступом

При проведении контрольных мероприятий могут выполняться следующие проверки:

- проверка соответствия установленных прав доступа (в прикладных системах, базах данных и т.п.) полномочиям в рамках трудовых обязанностей работника;
- проверка соответствия настроек и условий эксплуатации средств защиты информации требованиям, указанным в эксплуатационной документации;
- проверка процесса идентификации, аутентификации и авторизации при входе пользователя в систему (обращении к информационным ресурсам информационных систем);

- проверка механизмов блокирования доступа к средствам защиты от несанкционированного доступа1 (далее - НСД) при выполнении устанавливаемого числа неудачных попыток ввода пароля;
- проверка системы смены пароля принудительным образом (по истечению срока действия пароля);
- проверка выполнения требований по стойкости пароля.

3.2. Контрольные мероприятия в подсистеме регистрации и учета

При проведении контрольных мероприятий в подсистеме регистрации и учета, в зависимости от целей мероприятий, могут выполняться следующие проверки:

- проверка системных журналов на наличие зарегистрированных попыток несанкционированного доступа;
- проверка соответствия настроек и условий эксплуатации средств защиты информации требованиям, указанным в эксплуатационной документации и внутренних документах компании;
- имитация попытки несанкционированного доступа в систему, для проверки работы системы регистрации попытки НСД в системном журнале;
- проверка способов защиты системного журнала регистрации от уничтожения или модификации нарушителем2;
- проверка функционирующей системы автоматического непрерывного мониторинга событий в системе, которые могут являться причиной реализации угроз (создание, редактирование, запись, компиляция объектов).

Кроме того, при проведении проверок в части учета и хранения носителей персональных данных могут выполняться следующие проверки:

- проверка мест хранения носителей ПДн, сейфов и металлических шкафов, надежность их замков;
- проверка выполнения установленного порядка учета и хранения носителей ПДн;
- проверка фактического наличия всех носителей ПДн, в том числе учетные журналы, дела, документы (поступившие, изданные, переведенные на выделенное хранение);
- проверка фактического наличия всех носителей ПДн, переданных на архивное хранение;
- проверка фактического наличия всех не подшитых в дела и поступивших документов, содержащих ПДн, независимо от даты их регистрации;
- проверка номенклатуры дел с целью выделения документов, содержащих ПДн, для передачи в архив или на уничтожение;
- проверка правильности проставления регистрационных данных носителей, документов и дел, и учетных журналов;
- проверка правильности проставления в журнале отметок о движении носителей.

3.3. Контрольные мероприятия в подсистеме обеспечения целостности

При проведении контрольных мероприятий в подсистеме обеспечения целостности, в зависимости от целей мероприятий, могут выполняться следующие проверки:

- проверка механизмов контроля целостности пакетов обновлений средств защиты информации с использованием контрольных сумм;
- проверка соответствия настроек и условий эксплуатации средств защиты информации требованиям, указанным в эксплуатационной документации;
- проверка целостности используемого программного обеспечения, путем вычисления контрольных сумм;
- проверка фактического наличия экземпляров резервных копий;

---

[1] Несанкционированный доступ - доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых информационной системой

[2] Нарушитель (субъект атаки) – лицо (или инициируемый им процесс), проводящее (проводящий) атаку.

- проверка целостности сделанных резервных копий путем восстановления данных;
- имитация выполнения резервного копирования и восстановления данных при аварийном режиме функционирования системы.

3.4.Контрольные мероприятия в подсистеме антивирусной защиты

При проведении контрольных мероприятий в подсистеме антивирусной защиты, в зависимости от целей мероприятий, могут выполняться следующие проверки:

- проверка рабочих станций и серверов станций на наличие установленных программных средств антивирусной защиты;
- проверка соответствия настроек и условий эксплуатации средств защиты информации требованиям, указанным в эксплуатационной документации;
- проверка механизма своевременного обновления программных средств антивирусной защиты (в т.ч. баз данных вирусных сигнатур) на всех рабочих и серверных станциях;
- запуск полного сканирования системы в режиме реального времени антивирусным средством;
- проверка антивирусным средством используемых отчуждаемых носителей;
- проверка функционирования механизмов принудительной проверки используемых съемных носителей;
- имитация попыток заражения вредоносным программным обеспечением[3] серверных и рабочих станций;
- просмотр системных журналов и отчетов на наличие зафиксированных случаев заражения вредоносным ПО.

3.5.Контрольные мероприятия в подсистеме обеспечения безопасного межсетевого взаимодействия

При проведении контрольных мероприятий в подсистеме обеспечения безопасного межсетевого взаимодействия, в зависимости от целей мероприятий, могут выполняться следующие проверки:

- проверка соответствия установленных межсетевых экранов требуемому уровню защищенности;
- проверка соответствия настроек и условий эксплуатации средств защиты информации требованиям, указанным в эксплуатационной документации;
- имитация попыток проникновения в «закрытый» сегмент сети из открытого, в том числе с применением специального ПО;
- проверка системных журналов на наличие зафиксированных попыток обращения к «закрытым» ресурсам.

3.6. Контрольные мероприятия в подсистеме анализа защищенности

При проведении контрольных мероприятий в подсистеме анализа защищенности, в зависимости от целей мероприятий, могут выполняться следующие проверки:

- проверка выполнения своевременного обновления ПО, используемого для анализа защищенности, в т.ч. баз данных уязвимостей;
- проверка соответствия настроек и условий эксплуатации средств защиты информации требованиям, указанным в эксплуатационной документации;
- имитация попыток преодоления системы защиты, проверка системных журналов на наличие зафиксированных попыток НСД.

3.7. Контрольные мероприятия в подсистеме обнаружения и предотвращения вторжений

При проведении контрольных мероприятий в подсистеме обнаружения и предотвращения вторжений, в зависимости от целей мероприятий, могут выполняться следующие проверки:

---

[3] Вредоносное программное обеспечение - программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на персональные данные или ресурсы информационной системы персональных данных

- проверка соответствия настроек и условий эксплуатации средств защиты информации требованиям, указанным в эксплуатационной документации.

3.8. Контрольные мероприятия в подсистеме защиты от утечек по техническим каналам

При проведении контрольных мероприятий в подсистеме защиты от утечек по техническим каналам, в зависимости от целей мероприятий, могут выполняться следующие проверки:

- проверка в помещениях, где ведется обработка ПДн,;
- проверка размещения дисплеев рабочих станций, серверов и демонстрационного оборудования (проекторы, телевизоры и т.п.) таким образом, чтобы исключалась возможность просмотра посторонними лицами текстовой и графической информации, содержащей персональные данные.

3.9. Контрольные мероприятия в подсистеме физической защиты

При проведении контрольных мероприятий в подсистеме физической защиты, в зависимости от целей мероприятий, могут выполняться следующие проверки:

- проверка введения журналов учета посетителей, проходящих на территорию МБОУ СОШ № 4.
- проверка введения журналов посетителей, проходящих в защищаемые помещения;
- проверка электронных журналов СКУД на предмет попыток НСД в защищаемые помещения сотрудников, не имеющих права доступа в данные помещения;
- проверка наличия ключей (в том числе и электронных пропусков) от защищаемых помещений, а так же проверка сохранности вторых экземпляров ключей от защищаемых помещений;
- просмотр всех заявлений об утерянных ключах (в том числе и электронных пропусках) по которым можно получить доступ в защищаемые помещения, а так же проверка принятых мер (блокирование электронного пропуска, смена замка);
- проверка надежности замков, установленных в защищаемых помещениях;
- имитация попытки проникновения в защищаемые помещения для проверки срабатывания сигнализации и (или) системы контроля и управления доступом.

3.10. Контрольные мероприятия в подсистеме криптографической защиты

При проведении контрольных мероприятий в подсистеме криптографической защиты, в зависимости от целей мероприятий, могут выполняться следующие проверки:

- проверка соответствия настроек и условий эксплуатации средств защиты информации требованиям, указанным в эксплуатационной документации.
- проверка сохранности эксплуатационной и технической документации и ключевых документов на средства криптографической защиты;
- проверка журналов учета средств криптографической защиты и используемых криптоключей на правильность их ведения и хранения;
- проверка знаний работниками, использующими средства криптографической защиты, правил применения этих средств и правил обращения с криптоключами;
- проверка функционирования средств криптографической защиты путем имитации процессов, шифровании и дешифрования информации.

ПРИЛОЖЕНИЕ 1. ЖУРНАЛ УЧЕТА МЕРОПРИЯТИЙ ПО ОБЕСПЕЧЕНИЮ И КОНТРОЛЮ БЕЗОПАСНОСТИ ПДН, ОБРАБАТЫВАЕМЫХ В МБОУ СОШ № 4

УТВЕРЖДАЮ
_____
_____
«_____»_____2013г.

ЖУРНАЛ
УЧЕТА МЕРОПРИЯТИЙ ПО ОБЕСПЕЧЕНИЮ И КОНТРОЛЮ БЕЗОПАСНОСТИ ПДН, ОБРАБАТЫВАЕМЫХ В ИСПДН »НО»

Журнал начат «____» _____ 20___ г.
Должность
_____ / ФИО должностного лица /

Журнал завершен «____» _____ 20___ г.
Должность
_____ / ФИО должностного лица /

№ п/п	Наименование мероприятия, основание для проведения	Описание мероприятия	Сроки проведения контрольных мероприятий		Состав участников	Объекты контроля	Выявленные нарушения, выданные рекомендации		Отметка о контроле устранения выявленных нарушений
			Дата начала	Дата окончания					
1	2	3	4	5	6	7	8	9	10

Приложение №9
к приказу МБОУ СОШ №4
от 12.08.2016 года № 348

Положение
«О порядке уничтожения персональных данных»

1. Общие положения

1.1. Настоящий документ устанавливает порядок уничтожения информации, содержащей персональные данные, при достижении целей обработки или при наступлении иных законных оснований в МБОУСОШ №4 № 4 г. , в целях реализации: Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», Постановления Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», Постановления Правительства Российской Федерации от 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правыми актами.

2. Порядок уничтожения информации, содержащей персональные данные,
при достижении целей обработки или при наступлении иных законных оснований

2.1. Уничтожение документов, содержащих ПД, производится:

- по достижении целей их обработки согласно номенклатуре дел и документов;

- по достижении окончания срока хранения ПД, оговоренного в соответствующем соглашении заинтересованных сторон; в том числе, если они не подлежат архивному хранению.

2.2. Уничтожение документов, содержащих персональные данные, производится в случае выявления неправомерной обработки персональных данных в срок, не превышающий десяти рабочих дней с момента выявления неправомерной обработки персональных данных.

2.3. Уничтожение информации с ПД, хранящейся в электронном виде на материальных носителях, производиться путем выполнения процедуры специальной подготовки материальных носителей (многократное форматирование разделов, выделенных под хранение данных).

2.4. Уничтожение материальных носителей с ПД осуществляется механическим либо электромагнитным воздействием с помощью специализированных средств (шредер, уничтожитель оптических дисков и т.п.). Отобранные к уничтожению материалы измельчаются механическим способом до степени, исключающей возможность прочтения текста или сжигаются.

2.5. Уничтожение производится по мере необходимости, в зависимости от объемов накопленных для уничтожения документов.

2.6. Для уничтожения материальных носителей и информации на материальных носителях документально создается экспертная комиссия в составе не менее 2 человек. Уничтожение осуществляется по акту. Уничтожение документов производится в присутствии всех членов комиссии, которые несут персональную ответственность за правильность и полноту уничтожения перечисленных в акте документов (состав комиссии утверждается приказом). После уничтожения материальных носителей членами комиссии подписывается акт в трех экземплярах (Приложение 1) делается запись в журналах их учета и регистрации, а также в номенклатурах и описях дел проставляется отметка «Уничтожено. Акт №__(дата)».

2.7. Накапливаемые для уничтожения документы, копии документов, черновики, содержащие персональные данные, должны храниться отдельно.

Приложение №1

Акт № _____
об уничтожении носителей, содержащих персональные данные

Комиссия в составе:
Председатель – _____
Члены комиссии – _____

провела отбор бумажных, электронных, магнитных и оптических носителей персональных данных и другой конфиденциальной информации (далее носители) и установила, что в соответствии с требованиями руководящих документов по защите информации указанные носители и информация, записанная на них в процессе эксплуатации, в соответствии с действующим законодательством Российской Федерации, подлежит гарантированному уничтожению и составила настоящий акт о том, что произведено уничтожение носителей персональных данных в составе:

№ п/п	Дата	Тип носителя	Учетный номер носителя	Категория информации	Примечание

Всего носителей _____
(цифрами и прописью количество)

На указанных носителях персональные данные уничтожены путем
_____.
(стирания на устройстве гарантированного уничтожения информации и т.п.)

Перечисленные носители ПД уничтожены путем
_____.
(разрезания/сжигания/размагничивания/физического уничтожения/ механического уничтожения / иного способа)

Председатель комиссии: _____ /_____/
Члены комиссии: _____ /_____/
_____ /_____/

Приложение №2
к Порядку уничтожения персональных
данных при достижении целей их обработки

Типовая форма журнала уничтожения носителей персональных данных

Журнал уничтожения носителей персональных данных

Журнал начат ____ _____
Журнал завершен ____ _____
Ответственный _____ (Ф.И.О.)
На _____ листах

№ п/п	Наименование ИСПДн, в которой уничтожаются персональные данные	Ф.И.О. субъекта, персданные которого подлежащие уничтожению	Обоснование уничтожения	Наименование файла, и его месторасположение	Дата уничтожения	Ф.И.О. и подпись Исполнителя	Ф.И.О. и подпись ответственного за обработку персональных данных
1	2	3	4	5	6	7	8