

Приложение 3  
УТВЕРЖДЕНО  
приказом ГБОУ НАО  
«Средняя школа №4  
г. Нарьян-Мара с  
углубленным изучением  
отдельных предметов»  
от 15.03.19 № 165

## ПОЛОЖЕНИЕ

### об обработке персональных данных с использованием средств автоматизации

#### 1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящее Положение об обработке персональных данных с использованием средств автоматизации (далее — Положение) ГБОУ НАО «Средняя школа №4 г. Нарьян-Мара с углубленным изучением отдельных предметов» разработано в соответствии с Федеральным законом «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ, Федеральным законом «О персональных данных» от 27.07.2006 № 152-ФЗ, Постановлением Правительства Российской Федерации «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» от 01.11.2012 г. № 1119, а также другими нормативно-правовыми актами, действующими на территории Российской Федерации.

1.2. Цели разработки Положения:

1.2.1. определение порядка обработки персональных данных субъектов персональных данных, персональные данные которых подлежат обработке на основании полномочий ГБОУ НАО «Средняя школа №4 г. Нарьян-Мара с углубленным изучением отдельных предметов»;

1.2.2. обеспечение защиты прав и свобод человека и гражданина при обработке их персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну;

1.2.3. установление ответственности должностных лиц, имеющих доступ к персональным данным, за невыполнение требований норм, регулирующих обработку и защиту персональных данных.

1.3. К любой информации, содержащей персональные данные субъекта, применяется режим конфиденциальности, за исключением:

1.3.1. обезличенных персональных данных;

1.3.2. общедоступных персональных данных.

1.4. Режим конфиденциальности персональных данных снимается в случаях их обезличивания и по истечении срока их хранения, или продлевается на основании заключения экспертной комиссии ГБОУ НАО «Средняя школа №4 г. Нарьян-Мара с углубленным изучением отдельных предметов», если иное не определено законом Российской Федерации.

## II. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

2.1. **Доступ к информации** – возможность получения информации и ее использования.

2.2. **Информационная система (ИС)** – система, предназначенная для хранения, поиска и обработки информации, и соответствующие организационные ресурсы (человеческие, технические, финансовые и т. д.), которые обеспечивают и распространяют информацию.

2.3. **Информация** – сведения (сообщения, данные) независимо от формы их представления.

2.4. **Контролируемая зона (КЗ)** - это пространство (территория, здание, часть здания, помещения), в котором исключено неконтролируемое пребывание лиц, не имеющих постоянного или разового допуска, и посторонних транспортных средств.

2.5. **Носитель информации** – любой материальный объект или среда, используемый для хранения или передачи информации.

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

2.7. **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.

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

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

2.10. **Средство защиты информации (СЗИ)** – техническое, программное средство, вещество и (или) материал, предназначенные или используемые для защиты информации.

2.11. **Субъект персональных данных** – физическое лицо, которое прямо или косвенно определено или определяемо с помощью персональных данных.

## III. ПОРЯДОК ИСПОЛЬЗОВАНИЯ ПЕРСОНАЛЬНЫХ ДАННЫХ

3.1. Обработка персональных данных может осуществляться исключительно в целях, указанных в Политике в отношении обработки и защиты персональных данных ГБОУ НАО «Средняя школа №4 г. Нарьян-Мара с углубленным изучением отдельных предметов».

3.2. При определении объема и содержания, обрабатываемых персональных данных работники ГБОУ НАО «Средняя школа №4 г. Нарьян-Мара с углубленным изучением отдельных предметов» должны руководствоваться Политикой в отношении

обработки и защиты персональных данных ГБОУ НАО «Средняя школа №4 г. Нарьян-Мара с углубленным изучением отдельных предметов» с учетом действующего законодательства Российской Федерации, а также настоящим Положением.

3.3. Обработка персональных данных с использованием средств автоматизации (автоматизированным способом) может осуществляться исключительно на автоматизированных рабочих местах ИСПДн утвержденных «Перечнем автоматизированных рабочих мест информационных систем персональных данных».

3.4. Перечень нормативно-правовых актов, определяющих основания обработки персональных данных в ГБОУ НАО «Средняя школа №4 г. Нарьян-Мара с углубленным изучением отдельных предметов» определяется Политикой в отношении обработки и защиты персональных данных.

#### **IV. ПОРЯДОК ХРАНЕНИЯ ПЕРСОНАЛЬНЫХ ДАННЫХ**

4.1. Хранение носителей (дискет, дисков и т.п.), содержащих персональные данные, должно осуществляться в специальных папках, закрытых шкафах или сейфах, в порядке, исключающем доступ к ним третьих лиц.

4.2. Безопасность персональных данных при их обработке с использованием технических и программных средств обеспечивается с помощью системы защиты персональных данных, включающей в себя организационные меры и средства защиты информации, удовлетворяющие устанавливаемым в соответствии с законодательством РФ требованиям, обеспечивающим защиту информации.

4.3. Обработка персональных данных в ГБОУ НАО «Средняя школа №4 г. Нарьян-Мара с углубленным изучением отдельных предметов» осуществляется до наступления одного из условий прекращения обработки персональных данных указанных в Политике в отношении обработки и защиты персональных данных ГБОУ НАО «Средняя школа №4 г. Нарьян-Мара с углубленным изучением отдельных предметов».

4.4. По истечении срока хранения (30 дней, если иное не прописано в нормативно-правовых актах) для машинных носителей допускается гарантированное удаление информации методом многократной перезаписи с помощью специализированных программ (например, «Safe Erase», «Eraser», «FDelete») без уничтожения материального носителя.

4.5. Обезличивания персональных данных в ГБОУ НАО «Средняя школа №4 г. Нарьян-Мара с углубленным изучением отдельных предметов» не предполагается.

#### **V. ПОРЯДОК ПЕРЕДАЧИ ПЕРСОНАЛЬНЫХ ДАННЫХ**

5.1. Передавать персональные данные субъектов допускается только тем работникам, которые имеют доступ к обработке персональных данных.

5.2. В целях соблюдения законодательства РФ, для достижения целей обработки, а также в интересах и с согласия субъектов персональных данных ГБОУ НАО «Средняя школа №4 г. Нарьян-Мара с углубленным изучением отдельных предметов» в ходе своей деятельности предоставляет персональные данные организациям, перечисленным в Политике в отношении обработки и защиты персональных данных ГБОУ НАО «Средняя школа №4 г. Нарьян-Мара с углубленным изучением отдельных предметов».

5.3. Допускается распространение персональных данных с согласия субъекта персональных данных.

## **VI. ОРГАНИЗАЦИЯ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ**

6.1. Защита персональных данных субъекта от неправомерного их использования или утраты обеспечивается ГБОУ НАО «Средняя школа №4 г. Нарьян-Мара с углубленным изучением отдельных предметов» за счет своих средств.

6.2. Защита персональных данных должна вестись по трём взаимодополняющим направлениям:

6.2.1. Проведение организационных мероприятий:

6.2.1.1. разработка и внедрение внутренних организационно-распорядительных документов, регламентирующих обработку и защиту персональных данных субъектов, в том числе порядок доступа в помещения и к персональным данным;

6.2.1.2. ознакомление работников с законодательством Российской Федерации и внутренними нормативными документами, получение обязательств, касающихся обработки персональных данных;

6.2.1.3. организация учёта носителей персональных данных;

6.2.1.4. разработка модели угроз безопасности персональным данным;

6.2.1.5. проведение обучения работников по вопросам защиты персональных данных.

6.2.2. Программно-аппаратная защита:

6.2.2.1. внедрение программно-аппаратных средств защиты информации, прошедших в соответствии с Федеральным законом №184 от 27.12.2002 г. «О техническом регулировании» оценку соответствия.

6.2.3. Инженерно-техническая защита:

6.2.3.1. установка сейфов или запирающихся шкафов для хранения носителей персональных данных;

6.2.3.2. установка усиленных дверей, сигнализации, режима охраны здания и помещений, в которых обрабатываются персональные данные.

6.3. Определение конкретных мер, общую организацию, планирование и контроль выполнения мероприятий по защите персональных данных осуществляет ответственный за организацию обработки персональных данных в соответствии с законодательством в области защиты персональных данных и локальными нормативно-правовыми актами ГБОУ НАО «Средняя школа №4 г. Нарьян-Мара с углубленным изучением отдельных предметов».

6.4. Организацию и контроль защиты персональных данных в структурных подразделениях ГБОУ НАО «Средняя школа №4 г. Нарьян-Мара с углубленным изучением отдельных предметов» осуществляют их непосредственные руководители.

## **VII. ПОРЯДОК ПРЕДОСТАВЛЕНИЯ ДОСТУПА К ПЕРСОНАЛЬНЫМ ДАННЫМ**

7.1. Допуск к персональным данным субъекта могут иметь только те работники ГБОУ НАО «Средняя школа №4 г. Нарьян-Мара с углубленным изучением отдельных предметов», которым персональные данные необходимы в связи с исполнением ими своих трудовых обязанностей. Перечень таких работников отражен в «Списке лиц, доступ которых к персональным данным необходим для выполнения служебных (трудовых) обязанностей».

7.2. Процедура оформления допуска к персональным данным представляет собой следующую строгую последовательность действий:

7.2.1. ознакомление работника с настоящим Положением, Политикой в отношении обработки и защиты персональных данных ГБОУ НАО «Средняя школа №4 г. Нарьян-Мара с углубленным изучением отдельных предметов» и другими локальными нормативно-правовыми актами ГБОУ НАО «Средняя школа №4 г. Нарьян-Мара с углубленным изучением отдельных предметов», касающимися обработки персональных данных;

7.2.2. истребование с работника «Обязательства о неразглашении информации ограниченного доступа».

7.3. Каждый работник должен иметь доступ к минимально необходимому набору персональных данных субъектов, необходимых ему для выполнения служебных (трудовых) обязанностей.

7.4. Работникам, не имеющим надлежащим образом оформленного допуска, доступ к персональным данным субъектов запрещается.

## **VIII. ТРЕБОВАНИЯ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ**

8.1. Состав информационных систем ГБОУ НАО «Средняя школа №4 г. Нарьян-Мара с углубленным изучением отдельных предметов» определяется «Перечнем информационных систем».

8.2. 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, программные средства, средства защиты информации, применяемые в информационных системах.

8.3. 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.

8.4. Средства защиты информации, применяемые в информационных системах, в обязательном порядке проходят процедуру оценки соответствия в установленном законодательством РФ порядке.

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

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

8.7. Безопасность персональных данных при их обработке в информационной системе обеспечивает специалист, ответственный за обеспечение безопасности персональных данных в информационных системах.

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

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

8.8.2. своевременное обнаружение фактов несанкционированного доступа к персональным данным;

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

8.8.4. возможность незамедлительного восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

8.8.5. постоянный контроль над обеспечением уровня защищенности персональных данных.

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

8.9.1. определение угроз безопасности персональных данных при их обработке, формирование на их основе модели угроз;

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

8.9.3. проверку готовности средств защиты информации к использованию с составлением заключений о возможности их эксплуатации;

8.9.4. установку и ввод в эксплуатацию средств защиты информации в соответствии с эксплуатационной и технической документацией;

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

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

8.9.7. учет лиц, допущенных к работе с персональными данными в информационной системе;

8.9.8. контроль по соблюдению условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией;

8.9.9. 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;

8.9.10. описание системы защиты персональных данных.

8.10. Иные требования по обеспечению безопасности информации и средств защиты информации в ГБОУ НАО «Средняя школа №4 г. Нарьян-Мара с углубленным изучением отдельных предметов» выполняются в соответствии с требованиями

федеральных органов исполнительной власти и органов исполнительной власти субъекта РФ, в котором находится Оператор.

## IX. ОТВЕТСТВЕННОСТЬ

9.1. Ответственность за соблюдение требований по защите информации ограниченного доступа и надлежащего порядка проводимых работ возлагается на пользователей ИС, ответственного за обеспечение безопасности персональных данных в информационных системах и ответственного за организацию обработки персональных данных ГБОУ НАО «Средняя школа №4 г. Нарьян-Мара с углубленным изучением отдельных предметов».

9.2. Работники ГБОУ НАО «Средняя школа №4 г. Нарьян-Мара с углубленным изучением отдельных предметов», виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных субъекта, несут дисциплинарную, административную, гражданско-правовую и уголовную ответственность в соответствии с законодательством Российской Федерации.

9.2.1. Разглашение персональных данных субъекта (передача их посторонним лицам, в том числе другим работникам, не имеющим к ним доступ), их публичное раскрытие, утрата документов и иных носителей, содержащих персональные данные субъекта, а также иные нарушения обязанностей по их защите и обработке, установленных настоящим Положением, локальными нормативно-правовыми актами ГБОУ НАО «Средняя школа №4 г. Нарьян-Мара с углубленным изучением отдельных предметов», влечет наложение на работника, имеющего доступ к персональным данным, дисциплинарных взысканий в виде: замечания, выговора, увольнения. Работник ГБОУ НАО «Средняя школа №4 г. Нарьян-Мара с углубленным изучением отдельных предметов», имеющий доступ к персональным данным субъекта и совершивший указанный дисциплинарный проступок, несет полную материальную ответственность в случае причинения его действиями ущерба ГБОУ НАО «Средняя школа №4 г. Нарьян-Мара с углубленным изучением отдельных предметов» (в соответствии с п.7 ст. 243 Трудового кодекса РФ).

9.2.2. В отдельных случаях, при разглашении персональных данных, работник, совершивший указанный проступок, несет ответственность в соответствии со статьей 13.14 Кодекса об административных правонарушениях РФ.

9.2.3. В случае незаконного сбора или публичного распространения информации о частной жизни лица (нарушения неприкосновенности частной жизни), предусмотрена ответственность в соответствии со ст. 137 Уголовного кодекса РФ.

9.3. Директор ГБОУ НАО «Средняя школа №4 г. Нарьян-Мара с углубленным изучением отдельных предметов» за нарушение норм, регулирующих получение, обработку и защиту персональных данных субъектов, несет административную ответственность согласно ст. 5.27 и 5.39 Кодекса об административных правонарушениях Российской Федерации, а также возмещает субъекту ущерб, причиненный неправомерным использованием информации, содержащей персональные данные этого субъекта.

Приложение 4  
УТВЕРЖДЕНЫ  
приказом ГБОУ НАО  
«Средняя школа №4  
г. Нарьян-Мара с  
углубленным изучением  
отдельных предметов»  
от 25.03.19 № 165

## Правила обработки персональных данных

### I. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Данные Правила разработаны с целью защиты интересов ГБОУ НАО «Средняя школа №4 г. Нарьян-Мара с углубленным изучением отдельных предметов» и субъектов персональных данных, в целях предотвращения раскрытия (передачи), а также соблюдения надлежащих правил обращения с персональными данными.

1.2. Данные Правила предназначены для использования всеми работниками ГБОУ НАО «Средняя школа №4 г. Нарьян-Мара с углубленным изучением отдельных предметов», допущенными к работе с персональными данными.

1.3. Работники ГБОУ НАО «Средняя школа №4 г. Нарьян-Мара с углубленным изучением отдельных предметов», доступ которых к персональным данным необходим для выполнения ими своих служебных (трудовых) обязанностей, должны быть ознакомлены с положениями законодательства Российской Федерации о персональных данных, в том числе требованиями к защите персональных данных, документами, определяющими политику оператора в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных

### II. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

2.1. **Информация** - сведения (сообщения, данные) независимо от формы их представления (ст. 2 ФЗ РФ от 27.07.2006 г. N 149-ФЗ «Об информации, информационных технологиях и защите информации»).

2.2. **Доступ к информации** – возможность получения информации и её использования (ст. 2 ФЗ РФ от 27.07.2006 г. N 149-ФЗ «Об информации, информационных технологиях и защите информации»).

2.3. **Носитель информации** - любой материальный объект или среда, используемый для хранения или передачи информации.

2.4. **Несанкционированный доступ (НСД)** – доступ к информации, хранящейся на различных типах носителей (бумажных, магнитных, оптических и т. д.) в компьютерных базах данных, файловых хранилищах, архивах, секретных частях и т. д. различных организаций путём изменения (повышения, фальсификации) своих прав доступа.

**2.5. Контролируемая зона (КЗ)** - это пространство (территория, здание, часть здания, кабинеты), в котором исключено неконтролируемое пребывание лиц, не имеющих постоянного или разового допуска, и посторонних транспортных средств.

**2.6. Информационная система (ИС)** – система, предназначенная для хранения, поиска и обработки информации, и соответствующие организационные ресурсы (человеческие, технические, финансовые и т. д.), которые обеспечивают и распространяют информацию.

**2.7. 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 (ст. 3 ФЗ РФ от 27.07.2006 г. N 152-ФЗ «О персональных данных»).

**2.8. Пароль** – секретная комбинация цифр, знаков, слов, или осмысленное предложение, служащие для защиты информации от несанкционированного доступа к информационным ресурсам.

**2.9. Персональные данные** - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных) (ст. 3 ФЗ РФ от 27.07.2006 г. N 152-ФЗ «О персональных данных»).

**2.10. Распространение персональных данных** - действия, направленные на раскрытие персональных данных неопределенному кругу лиц (ст. 3 ФЗ РФ от 27.07.2006 г. N 152-ФЗ «О персональных данных»).

**2.11. Субъект персональных данных** — физическое лицо, которое прямо или косвенно определено или определяется с помощью персональных данных

**2.12. 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 (ст. 3 ФЗ РФ от 27.07.2006 г. N 152-ФЗ «О персональных данных»).

### **III. ПОРЯДОК РАБОТЫ СО СВЕДЕНИЯМИ, СОДЕРЖАЩИМИ ПЕРСОНАЛЬНЫЕ ДАННЫЕ**

3.1. При обработке персональных данных на бумажных носителях, съёмных машинных носителях (флеш-носителях, дисках, и т.п.), компьютерах и других технических средствах, работники ГБОУ НАО «Средняя школа №4 г. Нарьян-Мара с углубленным изучением отдельных предметов» обязаны следить как за сохранностью самих бумажных документов, съёмных машинных носителей и компьютеров и других технических средств, так и за сохранностью содержащейся в них информации, а именно не допускать неправомерного ознакомления с ней лиц, не имеющих допуска к работе с персональными данными.

3.2. Запрещается хранение или оставление бумажных документов и съёмных машинных носителей, содержащих персональные данные, в виде, позволяющем осуществить визуальный просмотр содержащихся в них персональных данных, их фотографирование или несанкционированное создание копий. Напечатанные документы,

содержащие персональные данные, должны изыматься из принтеров немедленно. Хранение бумажных документов и съёмных машинных носителей, содержащих персональные данные, допускается только в специальных закрытых шкафах, сейфах и помещениях, к которым исключён доступ лиц, не допущенных к обработке соответствующих персональных данных.

3.3. Запрещается без прямой служебной необходимости делать выписки персональных данных, распечатывать документы с персональными данными или записывать персональные данные на съёмные машинные носители.

3.4. Запрещается использовать для передачи персональных данных съёмные машинные носители, не учтённые в «Журнале учета съёмных носителей информации».

3.5. Запрещается выносить документы, съёмные машинные носители или переносные компьютеры, содержащие персональные данные, за пределы помещений контролируемой зоны ГБОУ НАО «Средняя школа №4 г. Нарьян-Мара с углубленным изучением отдельных предметов», если это не требуется для выполнения служебных (трудовых) обязанностей и если на это не дано разрешение директора ГБОУ НАО «Средняя школа №4 г. Нарьян-Мара с углубленным изучением отдельных предметов» или ответственного за организацию обработки персональных данных.

3.6. Бумажные документы с персональными данными, у которых истёк срок хранения, лишние или испорченные копии документов с персональными данными, должны быть уничтожены без возможности их восстановления (например, в shredders).

3.7. Большие объёмы бумажных документов с персональными данными, съёмные машинные носители с персональными данными, а также встроенные в компьютеры носители с персональными данными должны уничтожаться под контролем ответственного за организацию обработки персональных данных, способом, исключающим дальнейшее восстановление информации.

3.8. Мониторы компьютеров, использующихся для обработки персональных данных, должны быть ориентированы таким образом, чтобы исключить визуальный просмотр информации с них лицами, не имеющими допуск к обработке персональных данных.

3.9. Запрещается установка и использование при работе в АРМ вредоносных программ, ведущих к блокированию работы сети, самовольное изменение сетевых адресов, самовольное вскрытие блоков АРМ, модернизация или модификация АРМ и программного обеспечения. Несанкционированная передача АРМ с прописанными сетевыми настройками. Передача АРМ из одного подразделения в другое производится только ответственным за обеспечение безопасности информации с предварительно удалёнными сетевыми настройками. Использование технологии беспроводного доступа без разрешения ответственного за обеспечение безопасности в информационных системах.

3.10. Для работы с персональными данными разрешается использовать только автоматизированные рабочие места, указанные в «Перечне автоматизированных рабочих мест информационных систем», при этом для обработки персональных данных можно использовать только программное обеспечение, указанное в «Перечне программного обеспечения, обрабатывающего персональные данные».

3.11. Запрещается упоминать в разговоре с третьими лицами сведения, содержащие персональные данные.

3.12. Запрещается в нерабочее время или за пределами помещений ГБОУ НАО «Средняя школа №4 г. Нарьян-Мара с углубленным изучением отдельных предметов» упоминать в разговоре с кем-либо, включая любых работников ГБОУ НАО «Средняя школа №4 г. Нарьян-Мара с углубленным изучением отдельных предметов», сведения, содержащие персональные данные.

3.13. Запрещается обсуждать порядок доступа, места хранения, средства и методы защиты персональных данных с кем-либо, кроме ответственного за организацию обработки персональных данных, ответственного за обеспечение безопасности персональных данных в информационных системах, руководства, или лица, уполномоченного руководством на обсуждение данных вопросов.

#### **IV. ПОРЯДОК ДОСТУПА ЛИЦ В ПОМЕЩЕНИЯ**

4.1. При обеспечении доступа лиц соблюдаются требования законодательства РФ по защите персональных данных.

4.2. Обеспечение доступа лиц в помещения предусматривает комплекс специальных мер, направленных на поддержание и обеспечение установленного порядка деятельности структурных подразделений и определяет порядок пропуска работников ГБОУ НАО «Средняя школа №4 г. Нарьян-Мара с углубленным изучением отдельных предметов» и иных третьих лиц в помещения.

4.3. Контроль за порядком обеспечения доступа лиц в помещения возлагается на руководителя структурного подразделения.

4.4. Не допускается нахождение работников ГБОУ НАО «Средняя школа №4 г. Нарьян-Мара с углубленным изучением отдельных предметов» в помещениях контролируемой зоны в нерабочее для них время без согласования с руководством и без служебной записки. В нерабочее время, в случае служебной необходимости могут задержаться на рабочих местах только при наличии служебной записки, подписанной руководителем структурного подразделения. В служебной записке указывается (Ф.И.О. работника, № кабинета и время окончания работы, при работе нескольких человек указывается ответственное лицо). Служебная записка предоставляется ответственному за организацию обработки персональных данных. В случае неотложных заданий, поступивших после окончания рабочего дня, порядок допуска в помещения контролируемой зоны ГБОУ НАО «Средняя школа №4 г. Нарьян-Мара с углубленным изучением отдельных предметов» осуществляется аналогичным образом, по личному разрешению ответственного за организацию обработки персональных данных до начала неотложных работ.

4.5. В случаях, не терпящих отлагательства (пожар, авария систем тепло-, водоснабжения и т.п.), когда находящимся в помещении оборудованию, материальным ценностям и документации грозит опасность уничтожения или вывода из строя, работник оповещает пожарную охрану (аварийную службу), вызывает руководителя подразделения или работника, ответственного за помещение. Помещение вскрывается до прибытия указанных лиц, и принимаются меры к тушению пожара (ликвидации аварии), эвакуации ценностей, имущества и документации. Около эвакуируемых ценностей, имущества и документации выставляется временный пост охраны. Акт о вскрытии помещения составляется после окончания работ, связанных с ликвидацией происшествия.

4.6. Нахождение посетителей допускается только в рабочее время в присутствии работников, имеющих допуск к персональным данным.

4.7. В помещения ИС пропускаются:

4.7.1. беспрепятственно - Директор ГБОУ НАО «Средняя школа №4 г. Нарьян-Мара с углубленным изучением отдельных предметов» и работники, имеющие допуск к работе с персональными данными и с целью выполнения должностных обязанностей;

4.7.2. при наличии служебного удостоверения, с разрешения директора ГБОУ НАО «Средняя школа №4 г. Нарьян-Мара с углубленным изучением отдельных предметов» или руководителя структурного подразделения, в сопровождении ответственного за организацию обработки персональных данных или руководителя структурного подразделения - работники контролирующих органов, работники пожарных и аварийных служб, работники полиции;

4.7.3. ограниченно - работники, не имеющие допуска к работе с персональными данными или не имеющие функциональных обязанностей в помещении, работники сторонних организаций и учреждений для выполнения договорных отношений.

4.8. Посетители пропускаются в помещения ИС ГБОУ НАО «Средняя школа №4 г. Нарьян-Мара с углубленным изучением отдельных предметов» в рабочее время в сопровождении работников, допущенных к обработке персональных данных.

4.9. В помещениях, в которых происходит обработка персональных данных, запрещено использование не предусмотренных служебными обязанностями технических устройств, фотографирование, видеозапись, звукозапись, в том числе с использованием мобильных телефонов.

4.10. Рабочие и специалисты ремонтно-строительных организаций пропускаются в помещение для проведения ремонтно-строительных работ на основании заявок, подписанных директором или руководителями структурных подразделений ГБОУ НАО «Средняя школа №4 г. Нарьян-Мара с углубленным изучением отдельных предметов».

4.11. В целях предотвращения несанкционированного доступа к сведениям, содержащим персональные данные, работы проводятся только под контролем ответственного за организацию обработки персональных данных или руководителя структурного подразделения.

4.12. Контроль за допуском в помещения контролируемой зоны в рабочее время возлагается на руководителей подразделений, за которыми закреплены данные помещения. В нерабочее время, выходные и нерабочие праздничные дни охрана помещений контролируемой зоны обеспечивается средствами охранной сигнализации, а в случае их неисправности выставлением поста охраны.

4.13. Для исключения возможности бесконтрольного проникновения в помещения и к установленному в них оборудованию посторонних лиц, двери в отсутствие штатных работников запираются на ключ.

4.14. Помещения, где хранятся персональные данные, защищаемые криптографическими средствами защиты информации, должны быть оснащены входными дверьми с замками для обеспечения постоянного закрытия дверей помещений на замок и их открытия только для санкционированного прохода. Помещения должны опечатываться по окончании рабочего дня или быть оборудованы соответствующими техническими устройствами, сигнализирующими о несанкционированном вскрытии помещений.

4.15. Руководители структурных подразделений, либо работники, уполномоченные хранить ключи от сейфов и помещений должны вести «Журнал учета ключей от сейфов и помещений».

4.16. Контроль за допуском в помещения контролируемой зоны в рабочее время возлагается на руководителей подразделений, за которыми закреплены данные помещения. В нерабочее время, выходные и нерабочие праздничные дни охрана помещений контролируемой зоны обеспечивается средствами охранной сигнализации, а в случае их неисправности выставлением поста охраны.

4.17. Оборудование в помещении должно размещаться таким образом, чтобы исключить возможность бесконтрольного доступа к нему посторонних лиц.

4.18. Окна помещений, в которых ведётся обработка персональных данных, должны быть оборудованы шторами или жалюзи.

4.19. Режим работы охраны устанавливается штатным расписанием и должностными инструкциями.

4.20. Уборка помещений ИС должна производиться под контролем работника, допущенного к обработке персональных данных в этом помещении.

4.21. Во время уборки в помещении должна быть приостановлена работа с персональными данными, должны быть выключены или заблокированы все АРМ, на которых обрабатываются персональные данные. Носители, содержащие персональные данные, должны быть убраны в закрытые шкафы или сейфы.

## **V. ДЕЙСТВИЯ ПРИ ОБНАРУЖЕНИИ ПОПЫТОК НЕСАНКЦИОНИРОВАННОГО ДОСТУПА**

5.1. К попыткам несанкционированного доступа относятся:

5.1.1. сеансы работы с персональными данными незарегистрированных пользователей, или пользователей, нарушивших установленную периодичность доступа, или срок действия полномочий которых истёк, или превышающих свои полномочия по доступу к данным;

5.1.2. действия третьего лица, пытающегося получить доступ (или уже получившего доступ) к ИС, при использовании учётной записи администратора или другого пользователя ИС, методом подбора пароля, использования личного пароля, разглашённого владельцем учётной записи или любым другим методом.

5.2. При выявлении факта несанкционированного доступа пользователь ИСПДн обязан:

5.2.1. прекратить несанкционированный доступ к персональным данным;

5.2.2. доложить директору ГБОУ НАО «Средняя школа №4 г. Нарьян-Мара с углубленным изучением отдельных предметов» служебной запиской о факте несанкционированного доступа, его результате (успешный, неуспешный) и предпринятых действиях;

5.2.3. известить руководителя структурного подразделения, в котором работает пользователь, от имени учетной записи которого была осуществлена попытка несанкционированного доступа, о факте несанкционированного доступа;

5.2.4. известить ответственного за обеспечение безопасности персональных данных в информационных системах и ответственного за организацию обработки ПДн о факте несанкционированного доступа.

## **VI. ТРЕБОВАНИЯ ПО ТЕХНИЧЕСКОМУ УКРЕПЛЕНИЮ**

6.1. Руководители структурных подразделений обеспечивают обязательное выполнение мероприятий по техническому укреплению и оборудованию специальными техническими средствами охраны, системами пожарной безопасности и должны руководствоваться следующими основными требованиями:

6.1.1. Двери и окна должны иметь прочные и надежные петли, шпингалеты, крючки или задвижки и быть плотно подогнаны к рамам и дверным коробам. Допускается применение электромеханических, электромагнитных замков и задвижек.

6.1.2. Оконные проемы первых этажей зданий должны быть укреплены металлическими решетками, запираемыми с внутренней стороны, если это не противоречит требованиям пожарной безопасности.

6.1.3. Конструкция оконных рам должна исключать возможность демонтажа с наружной стороны оконного проема стекол.

6.1.4. Стекла в рамах должны быть надежно закреплены в пазах.

6.1.5. Рамы указанных оконных проемов должны оборудоваться запорными устройствами.

## **VII. ОТВЕТСТВЕННОСТЬ**

7.1. Работники ГБОУ НАО «Средняя школа №4 г. Нарьян-Мара с углубленным изучением отдельных предметов», виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных субъектов, несут дисциплинарную, административную, гражданско-правовую и уголовную ответственность в соответствии с законодательством Российской Федерации.

7.2. Разглашение персональных данных субъекта (передача их посторонним лицам, в том числе другим работникам, не имеющим к ним допуск), их публичное раскрытие, утрата документов и иных носителей, содержащих персональные данные субъекта, а также иные нарушения обязанностей по их защите и обработке, установленных локальными нормативно-правовыми актами (приказами, распоряжениями) ГБОУ НАО «Средняя школа №4 г. Нарьян-Мара с углубленным изучением отдельных предметов», влечет наложение на работника, имеющего доступ к персональным данным, дисциплинарных взысканий в виде: замечания, выговора, увольнения. Работник ГБОУ НАО «Средняя школа №4 г. Нарьян-Мара с углубленным изучением отдельных предметов», имеющий доступ к персональным данным субъекта и совершивший указанный дисциплинарный проступок, несет полную материальную ответственность в случае причинения его действиями ущерба ГБОУ НАО «Средняя школа №4 г. Нарьян-Мара с углубленным изучением отдельных предметов» (в соответствии с п.7 ст. 243 Трудового кодекса РФ).

7.2.1. В отдельных случаях, при разглашении персональных данных, работник, совершивший указанный проступок, несет ответственность в соответствии со статьей 13.14 Кодекса об административных правонарушениях РФ.

7.3. В случае незаконного сбора или публичного распространения информации о частной жизни лица (нарушения неприкосновенности частной жизни), предусмотрена ответственность в соответствии со ст. 137 Уголовного кодекса РФ.

7.4. Директор ГБОУ НАО «Средняя школа №4 г. Нарьян-Мара с углубленным изучением отдельных предметов» за нарушение норм, регулирующих получение, обработку и защиту персональных данных субъектов, несет административную ответственность согласно ст. 5.27 и 5.39 Кодекса об административных правонарушениях Российской Федерации, а также возмещает субъекту ущерб, причиненный неправомерным использованием информации, содержащей персональные данные этого субъекта