



**УПРАВЛЕНИЕ ДОШКОЛЬНОГО ОБРАЗОВАНИЯ АДМИНИСТРАЦИИ
МУНИЦИПАЛЬНОГО ОБРАЗОВАНИЯ ГОРОДСКОГО ОКРУГА «СЫКТЫВКАР»**

Муниципальное автономное общеобразовательное учреждение
«Прогимназия № 81» г. Сыктывкара
(МАОУ «Прогимназия № 81»)

167016 Республика Коми г. Сыктывкар ул. Карьерная д.18 progimnazia81@yandex.ru
8 (8212 31-22-33, 31 – 26 – 61 (тел), 8 (8212) 32 – 20 – 27 (факс))

УТВЕРЖДАЮ:

Директор МАОУ «Прогимназия № 81»

Т.В. Чернавина

Приказ № 178 от 18.04.2017 года

(Приложение № 3)



ПОЛОЖЕНИЕ

**об ответственном лице, осуществляющем функции по организации защиты
персональных данных в МАОУ «Прогимназия № 81»**

1. Положение об ответственном лице, осуществляющем функции по организации защиты персональных данных (далее – ПД), обеспечению безопасности ПД при их обработке в информационных системах персональных данных в МАОУ «Прогимназия № 81» (далее – Положение) разработано на основании требований нормативно-методических документов Российской Федерации в области защиты персональных данных.

2. Настоящее Положение устанавливает требования к полномочиям и обязанностям ответственного за обеспечение защиты ПД должностного лица МАОУ «Прогимназия № 81» (далее – ответственное лицо) при их обработке в информационных системах персональных данных (далее ИСПД) в МАОУ «Прогимназия № 81». При этом, обрабатываемые ПД представляют собой совокупность ПД, содержащихся в базах данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких ПД с использованием средств автоматизации (далее информационные системы) или без использования таковых.

3. Под техническими средствами, позволяющими осуществлять обработку ПД, понимаются средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки ПД (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.

4. Ответственное лицо назначается приказом директора МАОУ «Прогимназия № 81» и обеспечивает безопасность ПД путем исключения несанкционированного, в том числе случайного, доступа к ПД, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение ПД, а также иные несанкционированные действия.

5. Ответственное лицо обеспечивает безопасность ПД при их обработке в информационных системах с помощью системы защиты ПД, 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 ПД), а также используемые в информационной системе информационные технологии. Технические и программные средства должны удовлетворять установленным в соответствии с законодательством Российской Федерации требованиям, обеспечивающим защиту информации.

6. Для обеспечения безопасности ПД, при их обработке в информационных системах, ответственное лицо обеспечивает защиту 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.

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

8. Ответственное лицо обеспечивает достаточность принятых мер по организации безопасной обработки ПД в информационных системах, оцениваемой при проведении государственного контроля и надзора.

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

9. Ответственное лицо обеспечивает применение средств защиты информации в информационных системах, прошедших в установленном порядке процедуру оценки соответствия.

10. Ответственное лицо обеспечивает и организует разработку организационной, технической документации на ИСПД и подготовку информационной системы к проведению оценки соответствия (аттестации).

11. При проведении классификации ИСПД ответственное лицо руководствуется порядком проведения классификации ИСПД устанавливаемым совместно Федеральной службой по техническому и экспортному контролю Российской Федерации.

12. Ответственное лицо обеспечивает обмен персональными данными при их обработке в информационных системах по каналам связи, защита которых обеспечивается путем реализации соответствующих организационных мер и (или) путем применения технических средств.

13. Ответственное лицо обеспечивает размещение информационных систем, специального оборудования и охрану помещений, в которых ведется работа с ПД, организацию режима безопасности в этих помещениях при котором обеспечивается сохранность носителей ПД и средств защиты информации, а также исключается возможность неконтролируемого проникновения или пребывания в этих помещениях посторонних лиц.

14. Возможные каналы утечки информации при обработке ПД в информационных системах определяются Федеральной службой по техническому и экспортному контролю Российской Федерации и Федеральной службой безопасности Российской Федерации в пределах их полномочий.

15. Пользователями ИСПД являются сотрудники, обрабатывающие ПД в информационной системе, отвечающие за обеспечение конфиденциальности ПД и безопасности ПД в информационной системе на своем рабочем месте.

16. При обработке ПД в информационной системе

- ответственное лицо обеспечивает и требует от пользователей ИСПД в рамках их компетенции:

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

б) своевременное обнаружение фактов несанкционированного доступа к ПД;

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

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

д) постоянный контроль за обеспечением уровня защищенности ПД.

17. Мероприятия по обеспечению безопасности ПД при их обработке в информационных системах организуются и проводятся ответственным лицом и включают в себя:

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

б) разработку на основе модели угроз системы защиты ПД, обеспечивающей нейтрализацию предполагаемых угроз с использованием методов и способов защиты ПД, 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 Пользователей ИСПД, использующих средства защиты информации, применяемые в информационных системах, правилам работы с ними;

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

ж) учет Пользователей ИСПД, допущенных к работе с ПД 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 ПД, использования средств защиты информации, которые могут привести к нарушению конфиденциальности ПД или другим нарушениям, приводящим к снижению уровня защищенности ПД, разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений;

к) описание системы защиты ПД.

18. Сотрудники, доступ которых к ПД, обрабатываемым в информационной системе, необходим для выполнения служебных (трудовых) обязанностей, допускаются к соответствующим ПД на основании списка, утвержденного ответственным лицом и согласованного с администратором информационной безопасности ИСПД.

19. Ответственное лицо обеспечивает регистрацию запросов Пользователей информационной системы на получение ПД, а также факты предоставления ПД по этим запросам в электронном журнале обращений. Содержание электронного журнала обращений периодически проверяется ответственным лицом и администратором информационной безопасности ИСПД.

20. При обнаружении нарушений порядка предоставления ПД администратор информационной безопасности ИСПД по распоряжению ответственного лица незамедлительно приостанавливает предоставление ПД пользователям информационной системы до выявления причин нарушений и устранения этих причин.

21. Положение вступает в силу с момента утверждения приказом директора МАОУ «Прогимназия № 81».

22. Настоящее Положение действует до принятия иных нормативных документов, которые являются основанием для признания локального нормативного акта утратившим силу.

23. Изменения и дополнения в настоящее Положение вносятся приказом директора МАОУ «Прогимназия № 81».

24. Настоящее Положение размещается на официальном сайте МАОУ «Прогимназия № 81» ***прогимназия81.рф***

25. Положение на бумажном носителе доступно для ознакомления в кабинете должностного лица, являющегося ответственным за обеспечение безопасности персональных данных в МАОУ «Прогимназия № 81».

ЛИСТ ОЗНАКОМЛЕНИЯ

с Положением об ответственном лице, осуществляющем функции по организации защиты персональных данных в Муниципальном автономном общеобразовательном учреждении «Прогимназия №81» г. Сыктывкара

№ п/п	ФИО работника	Должность	Дата ознакомления	Подпись
1.				
2.				
3.				
4.				
5.				
6.				
7.				
8.				
9.				
10.				
11.				
12.				
13.				
14.				
15.				
16.				
17.				
18.				