Приложение № 1
к приказу МБОУ гимназии № 103
г. Минеральные Воды
от «14» февраля 2023 г. № 69

Регламент
определения уровня защищенности персональных данных, обрабатываемых в информационных системах персональных данных МБОУ гимназии № 103 г. Минеральные Воды

Настоящий Регламент определяет порядок определения уровня защищенности персональных данных, обрабатываемых в информационных системах персональных данных в МБОУ гимназии № 103 г. Минеральные Воды (далее-оператор).

Оператор обязан принимать меры, необходимые и достаточные для обеспечения выполнения обязанностей, предусмотренных № 152-ФЗ и принятыми в соответствии с ним нормативными правовыми актами.

Состав и перечень мер, необходимых и достаточных для обеспечения выполнения таких обязанностей, определяются оператором самостоятельно.

К таким мерам могут относиться (№152-ФЗ ст.18.1):

1. Назначение ответственного за организацию обработки ПДн;
2. Издание документов, определяющих политику оператора в отношении обработки ПДн, локальных актов по вопросам обработки персональных данных, а также локальных актов, устанавливающих процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений;
3. Применение правовых, организационных и технических мер по обеспечению безопасности ПДн (№152-ФЗ ст.19):

- определение угроз безопасности ПДн при их обработке в ИСПДн;
- применение организационных и технических мер по обеспечению безопасности ПДн при их обработке в ИСПДн, необходимых для выполнения требований к защите ПДн в соответствии с уровнем защищенности ИСПДн;
- применение прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;
- оценка эффективности принимаемых мер по обеспечению безопасности ПДн до ввода в эксплуатацию ИСПДн;
- учёт машинных носителей ПДн;
- обнаружение фактов НСД к ПДн и принятие мер;
- восстановление ПДн, модифицированных или уничтоженных вследствие НСД к ним;
- установление правил доступа к ПДн, а также обеспечение регистрации и учёта всех действий, совершаемых с ПДн;
- контроль за принимаемыми мерами по обеспечению безопасности ПДн и уровня защищенности ИСПДн;

4. Осуществление внутреннего контроля и (или) аудита соответствия обработки персональных данных №152-ФЗ, нормативным правовым актам, требованиям к защите ПДн, политике оператора в отношении обработки ПДн, локальным актам оператора;
5. Оценка вреда, который может быть причинен субъектам персональных данных в случае нарушения №152-ФЗ, соотнесение указанного вреда с принимаемыми мерами, направленными на обеспечение выполнения обязанностей, в соответствии с №152-ФЗ;
6. Ознакомление работников оператора, непосредственно осуществляющих обработку ПДн, с положениями законодательства РФ о персональных данных, в том числе требованиями к защите ПДн, документами, определяющими политику оператора в отношении обработки ПДн,

локальными актами по вопросам обработки персональных данных, и (или) обучение указанных работников;

7. Уведомление до начала обработки персональных данных уполномоченного органа по защите прав субъектов ПДн о намерении осуществлять обработку ПДн (№152-ФЗ, ст. 22).

До завершения эксплуатации ИСПДн система функционирует циклическим образом, периодически или на каком-либо ином основании осуществляется аудит. При завершении обработки ПДн происходит обезличивание данных, уничтожение данных, которые сопровождаются соответствующими актами о выводе ИСПДн из эксплуатации, об уничтожении данных, также необходимо подготовить уведомление уполномоченного органа по защите прав субъектов ПДн.

Таким образом, на основании анализа статей № 152-ФЗ набор шагов оператора по соблюдению № 152-ФЗ «О персональных данных» имеет вид:.

Шаг №1. «Инициация работ по защите персональных данных и назначение ответственных за организацию обработки и обеспечения безопасности персональных данных»:

Цели проведения работ:

1. Определение должностных лиц и структурных подразделений, ответственных за ИБ и соблюдение требований НПА РФ, регламентирующих порядок защиты ПДн;

2. Разработка и утверждение внутренних документов (положений, инструкций и т.п.), регламентирующих деятельность структурных подразделений, отвечающих за ИБ;

3. Разработка и утверждение документов, закрепляющих функциональные обязанности и права должностных лиц и структурных подразделений, отвечающих за ИБ.

Шаг №2. «Определение состава обрабатываемых ПДн, целей, сроков, условий и законных оснований обработки»:

Цели проведения работ:

1. Закрепление представления о составе, условиях и целях обработки ПДн, формирование основы для дальнейшего планирования работ по приведению процессов, в рамках которых происходит обработка ПДн, в соответствие требованиям НПА РФ, регламентирующих порядок обработки ПДн, документирование всех правил обработки и защиты ПДн, в том числе для повышения осведомленности конечных пользователей;

2. Документированным выражением данного представления для оператора ПДн являются Перечень персональных данных и Перечень лиц, допущенных к обработке персональных данных – подробные, четко структурированные документы, содержащие информацию обо всех категориях и видах ПДн, основаниях и условиях обработки, а также список лиц, имеющих к ним доступ.

Шаг №3. «Определение порядка взаимодействия с субъектами персональных данных»:

Цель проводимых работ: определение порядка реагирования на запросы субъектов ПДн и разработка описывающих его регламентов для сведения к минимуму вероятности нарушения прав субъектов при обработке их ПДн компанией-оператором.

Основной целью № 152-ФЗ является защита прав субъектов ПДн, поэтому в нем четко определены права субъектов ПДн и соответствующие обязанности оператора ПДн.

Невыполнение требований закона по предоставлению субъекту информации о содержании, условиях обработки его ПДн, другой информации, затрагивающей его законные права и интересы, может быть квалифицировано как нарушение установленного порядка обработки ПДн. Некорректная реакция (или ее отсутствие) на запрос субъекта персональных данных может быть поводом для обращения в Роскомнадзор с жалобой на действия оператора.

Шаг №4. «Определение порядка взаимодействия с другими организациями при обработке персональных данных»

Цели проводимых работ:

При анализе взаимодействия с другими организациями важно понимать роль организации в этом взаимодействии. В связи с этим организации-оператору требуется определить порядок таких взаимодействий.

Шаг №5. «Определение перечня информационных систем персональных данных (ИСПДн) и их характеристик»

Цели проводимых работ:

1. Выделение (идентификация) и определение состава ИСПДн, имеющихся в IT-инфраструктуре предприятия;
2. Определение характеристик ИСПДн в соответствии с НПА ФСТЭК России;
3. Документальная фиксация перечня всех идентифицированных ИСПДн и их характеристик.

Описание проводимых работ:

ИСПДн представляют собой совокупность содержащихся в базах данных ПДн и обеспечивающих их обработку информационных технологий и технических средств.

Выделение ИСПДн является обязательной процедурой, осуществляемой с учетом категорий и объема накапливаемых, обрабатываемых и распределяемых с их использованием ПДн.

Определение характеристик ИСПДн – основное условие корректного установления методов и средств защиты, необходимых для обеспечения безопасности ПДн.

Шаг №6. «Разработка модели угроз для ИСПДн»:

Цели проводимых работ:

1. Определение актуальных угроз и типов угроз безопасности ПДн при их обработке в ИСПДн;
2. Составление модели угроз для каждой ИСПДн, выделенной в информационной инфраструктуре организации-оператора;
3. Определив тип угроз безопасности ПДн, актуальных для информационной системы, необходимо установить уровень защищенности ПДн при обработке в ИСПДн.

Описание проводимых работ:

Оценка актуальности угроз безопасности ПДн является ключевым элементом в процессе построения и управления СЗПДн. Корректное определение совокупности объектов негативного воздействия, присущих им уязвимостей, способов реализации этих уязвимостей и, как следствие, источников данного негативного воздействия позволяет дать качественную характеристику меры риска осуществления той или иной угрозы безопасности ПДн. В свою очередь, наличие формализованного описания актуальных угроз безопасности ПДн дает возможность подразделениям организаций и лицам, ответственным за безопасность персональных данных:

– адекватно оценить необходимость реализации тех или иных мероприятий по обеспечению безопасности ПДн исходя из состояния защищенности ИСПДн на текущий момент;

– спрогнозировать развитие СЗПДн на краткосрочную и среднесрочную перспективу, провести оптимизацию бюджетов соответствующих подразделений, выставить приоритеты принимаемым мерам по обеспечению безопасности ПДн.

Шаг №7. «Проектирование и реализация системы защиты персональных данных»:

Цель проводимых работ: разработка и создание для каждой ИСПДн системы защиты ПДн, соответствующей законодательству РФ в области обеспечения ИБ и отвечающей требованиям, предъявляемым документами ФСТЭК России и ФСБ России к соответствующему классу ИСПДн.

Описание проводимых работ:

Создание системы защиты ПДн является неотъемлемой частью реализации всего спектра требований, предъявляемых к оператору ПДн 152-ФЗ и соответствующими подзаконными актами. Субъекты ПДн, передавая свои сведения оператору, вправе рассчитывать на то, что

безопасность этих сведений будет обеспечена всеми необходимыми мерами со стороны оператора. Это подразумевает под собой не только использование технических средств защиты, но и проведение определенных организационных мероприятий, направленных на обеспечение безопасности ПДн, обрабатываемых в каждой конкретной ИСПДн, эксплуатируемой оператором.

Шаг №8. «Определение необходимости уведомления уполномоченного органа на защите ПДн»:

Цели проводимых работ:

1. Определить необходимость подачи уведомления об обработке ПДн в уполномоченный орган по защите прав субъектов ПДн;
2. Подготовить правовое обоснование отсутствия необходимости подачи уведомления об обработке ПДн, если все обрабатываемые ПДн подпадают под исключения, предусмотренные частью 2 статьи 22 № 152-ФЗ;
3. В случае необходимости, подготовить уведомление об обработке ПДн в соответствии с требованиями регулятора и отправить в уполномоченный орган.

Описание проводимых работ:

Одним из условий обработки ПДн является необходимость уведомить уполномоченный орган по защите прав субъектов ПДн о своем намерении осуществлять обработку ПДн.

Невыполнение условия уведомления уполномоченного органа может быть квалифицировано как правонарушение, предусмотренное статьей 19.7 Кодекса РФ об административных правонарушениях от 30.12.2001 № 195-ФЗ и повлечь соответствующую ответственность.

Шаг №9. «Прекращение обработки ПДн»:

1. В случае выявления неправомерной обработки ПДн, осуществляемой оператором или лицом, действующим по поручению оператора, оператор в срок, не превышающий трех рабочих дней с даты этого выявления, обязан прекратить неправомерную обработку ПДн или обеспечить прекращение неправомерной обработки ПДн лицом, действующим по поручению оператора;
2. В случае если обеспечить правомерность обработки ПДн невозможно, оператор в срок, не превышающий десяти рабочих дней с даты выявления неправомерной обработки ПДн, обязан уничтожить такие ПДн или обеспечить их уничтожение;
3. Об устранении допущенных нарушений или об уничтожении ПДн оператор обязан уведомить субъекта ПДн или его представителя, а в случае, если обращение субъекта ПДн или его представителя либо запрос уполномоченного органа по защите прав субъектов ПДн были направлены уполномоченным органом по защите прав субъектов ПДн, также указанный орган;
4. В случае достижения цели обработки ПДн оператор обязан прекратить обработку ПДн или обеспечить ее прекращение и уничтожить ПДн или обеспечить их уничтожение в срок, не превышающий тридцати дней с даты достижения цели обработки ПДн, если иное не предусмотрено договором;
5. В случае отзыва субъектом ПДн согласия на обработку его ПДн оператор обязан прекратить их обработку или обеспечить прекращение такой обработки и в случае, если сохранение ПДн более не требуется для целей обработки ПДн, уничтожить ПДн или обеспечить их уничтожение в срок, не превышающий тридцати дней с даты поступления указанного отзыва, если иное не предусмотрено договором;
6. В случае отсутствия возможности уничтожения ПДн в течение срока, указанного в предыдущих пунктах, оператор осуществляет блокирование таких ПДн или обеспечивает их блокирование и обеспечивает уничтожение ПДн в срок не более чем шесть месяцев, если иной срок не установлен федеральными законами;
7. В случае прекращения обработки ПДн оператор обязан уведомить об этом уполномоченный орган по защите прав субъектов ПДн в течение десяти рабочих дней с даты возникновения таких изменений или с даты прекращения обработки ПДн.

Следующим шагом является составление алгоритма установления уровня защищённости с соблюдением требований законодательства. Основным документом является Постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

Уровень защищённости персональных данных – это комплексный показатель, который характеризует выполнение требований, нейтрализующих угрозы безопасности информационных систем персональных данных.

Установление уровня защищённости ПДн для каждой ИСПДн осуществляется в соответствии положениями пп. 9-12 Требований к защите персональных данных при их обработке в информационных системах персональных данных, утвержденных № 1119-ПП. Данными Требованиями установлены 4 уровня защищённости персональных данных, различающихся перечнем необходимых к выполнению требований по защите информационных систем. Ниже представлен пошаговый алгоритм определения уровня защищённости ПДн в ИСПДн.

Алгоритм определения уровня защищённости ПДн

1. Определить категорию обрабатываемых в ИСПДн ПДн.

Определяется, какого рода информация ПДн обрабатывается в информационной системе:

– общедоступная – ПДн субъектов ПДн, полученные только из общедоступных источников ПДн, созданных в соответствии со ст. 8 Закона о персональных данных;

– данные сотрудников;

– иная – ПДн, не относящиеся к специальным и биометрическим и не являющиеся общедоступными данными.

2. Определить тип субъектов ПДн.

На данном шаге необходимо определить тип субъектов ПДн, обрабатываемых в ИСПДн:

1) субъект ПДн, являющийся сотрудником организации;

2) субъект ПДн, не являющийся сотрудником организации.

3. Определить количество обрабатываемых субъектов ПДн.

В рамках данного шага необходимо проанализировать обрабатываемое количество субъектов ПДн в информационной системе и по результатам анализа получить контрольное значение:

1) менее 100 000 субъектов ПДн;

2) более 100 000 субъектов ПДн.

4. Определить, угрозы какого типа актуальны для ИС (ПП №1119, п. 6).

В зависимости от актуальности угроз получаем одно из следующих значений, представленных в таблице 1.1.

5. Определить тип угроз безопасности ПДн, актуальных для ИС с учётом оценки возможного вреда субъектам ПДн (№152-ФЗ, ст. 18.1, п. 5, ч. 1) и в соответствии с НПА, принятыми во исполнение №152-ФЗ, ст. 19, п. 5.

Таблица 1.1

Типы угроз

№ п/п	Тип угроз	Характеристика
1	угрозы 1-го типа	связаны с наличием недокументированных возможностей в системном программном обеспечении
2	угрозы 2-го типа	связаны с наличием недокументированных возможностей в прикладном программном обеспечении
3	угрозы 3-го типа	не связаны с наличием недокументированных возможностей в системном и прикладном программном обеспечении

6. Определить уровень защищенности ПДн (ПП №1119, п. 9-12).

По результатам, полученным в ходе предыдущих шагов, определяются уровни защищённости ПДн в ИСПДн, которые фиксируются Актом установления уровня защищённости ПДн в ИСПДн.

Чем выше определён уровень защищённости персональных данных, тем больше мер по обеспечению безопасности персональных данных требуется выполнить, тем более продуманной и многоаспектной должна быть система защиты, а это напрямую влияет на сумму, которую придётся потратить владельцам организации.

Если по ошибке определить более высокий уровень защищённости, то, соответственно, придётся строить более дорогую систему защиты персональных данных.

Для удобства определения уровней защищённости ПДн на рисунке 2.1 приведена таблица, которая сформирована на основании пп.9-12 Требований к защите персональных данных при их обработке в информационных системах персональных данных, утвержденных № 1119-ПП.

Категории ПДн		Специальные			Биомет-рические	Иные			Общедоступные		
Собственные работники		нет	нет	да		нет	нет	да	нет	нет	да
Количество субъектов		более 100 тыс.	менее 100 тыс.			более 100 тыс.	менее 100 тыс.		более 100 тыс.	менее 100 тыс.	
Тип актуальных угроз	1	1 УЗ	1 УЗ	1 УЗ	1 УЗ	1 УЗ	2 УЗ	2 УЗ	2 УЗ	2 УЗ	2 УЗ
	2	1 УЗ	2 УЗ	2 УЗ	2 УЗ	2 УЗ	3 УЗ	3 УЗ	2 УЗ	3 УЗ	3 УЗ
	3	2 УЗ	3 УЗ	3 УЗ	3 УЗ	3 УЗ	4 УЗ	4 УЗ	4 УЗ	4 УЗ	4 УЗ

Рисунок 2.1. Уровни защищённости ПДн в ИСПДн

Основываясь на данных об инфраструктуре модели созданной организации, необходимо составить акт определения уровня защищённости персональных данных информационной системы персональных данных.

Необходимыми исходными данными для составления акта являются:

1) название организации;
2) ФИО директора;
3) ФИО сотрудников, которых необходимо включить в комиссию;
4) категория обрабатываемых в ИСПДн ПДн;
5) тип субъектов ПДн, обрабатываемых в ИСПДн;
6) объем обрабатываемых субъектов ПДн;
7) типы угроз, актуальных для данной ИСПДн;
8) уровень защищённости ИСПДн.

Приложение 1 к Регламенту
определения уровня защищенности
персональных данных,
обрабатываемых в информационных
системах персональных данных
МБОУ гимназии № 103
г. Минеральные Воды

УТВЕРЖДАЮ
Директор МБОУ гимназии № 103
г. Минеральные Воды
_____ Р.Г. Агабекова
М.П.
« ___ » _____ 20____ г.

АКТ № 1
определения уровня защищённости персональных данных
информационной системы персональных данных
«Система обработки персональных данных сотрудников»

Комиссия по персональным данным, созданная в составе:
Председателя комиссии: директора _____

Членов комиссии: _____

_____

определила:

1. Информационная система обрабатывает **иные категории** персональных данных, так как в информационной системе не обрабатываются персональные данные, относящиеся к специальной категории ПДн (персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни субъектов ПДн), или к биометрическим персональным данным (ПДн, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность и которые используются оператором для установления личности субъекта ПДн), или к общедоступным персональным данным (ПДн, полученные только из общедоступных источников персональных данных, созданных в соответствии со статьей 8 Федерального закона «О персональных данных»);
2. Информационная система обрабатывает персональные данные **менее чем 100 000** субъектов персональных данных;
3. В связи с тем, что в информационной системе используется лицензионное, но не сертифицированное прикладное программное обеспечение, то для информационной системы **актуальны угрозы 2-го типа**, в том числе, актуальны угрозы, связанные с наличием недокументированных (недекларированных) возможностей в прикладном программном обеспечении.

По результатам проведенного анализа и исходя из того, что для информационной системы персональных данных «Система обработки персональных данных сотрудников» актуальны угрозы 2-го типа и в ней обрабатываются иные категории персональных данных субъектов в объеме менее чем 100 000 субъектов персональных данных, комиссия пришла к заключению, что для информационной системы персональных данных «Система обработки персональных данных сотрудников» необходимо обеспечить **3-й уровень защищенности** персональных данных при их обработке в информационной системе.

Комиссия устанавливает, что для обеспечения 3-го уровня защищенности персональных данных при их обработке в информационной системе персональных данных «Система обработки персональных данных сотрудников» необходимо выполнение следующих требований:

1. Организация режима обеспечения безопасности помещений, в которых размещена информационная система персональных данных «Система обработки персональных данных сотрудников», препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения;
2. Обеспечение сохранности носителей персональных данных;
3. Утверждение директором МБОУ гимназии № 103 г. Минеральные Воды документа, определяющего перечень лиц, доступ которых к персональным данным, обрабатываемым в информационной системе персональных данных «Система обработки персональных данных сотрудников», необходим для выполнения ими трудовых обязанностей;
4. Использование средств защиты информации, прошедших процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации, в случае, когда применение таких средств необходимо для нейтрализации актуальных угроз;
5. Приказом директора МБОУ гимназии № 103 г. Минеральные Воды должно быть назначено должностное лицо (работник), ответственный за обеспечение безопасности персональных данных, в том числе и в информационной системе персональных данных «Система обработки персональных данных сотрудников».

Председатель комиссии: _____ _____
(подпись)

Члены комиссии: _____ _____
(подпись)

_____ _____
(подпись)