

УТВЕРЖДАЮ
Заведующий МАДОУ ДС №54
_____ Н.С. Стрелкина
Приказ от 06.03.2024г. №38

РЕГЛАМЕНТ
проведения внутреннего контроля соответствия обработки
персональных данных
в МАДОУ ДС №54 требованиям к защите персональных данных

1. Термины и определения

- 1.1. Информационная система персональных данных – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.
- 1.2. Инцидент информационной безопасности – любое непредвиденное или нежелательное событие, которое может нарушить деятельность или информационную безопасность. Инцидентами информационной безопасности являются:
 - утрата услуг, оборудования или устройств;
 - системные сбои или перегрузки;
 - ошибки пользователей;
 - несоблюдение политики или рекомендаций по информационной безопасности;
 - нарушение физических мер защиты;
 - неконтролируемые изменения систем;
 - сбои программного обеспечения и отказы технических средств;
 - нарушение правил доступа.
- 1.3. 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.
- 1.4. Персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).
- 1.5. Средство защиты информации – программное обеспечение, программно-аппаратное обеспечение, аппаратное обеспечение, вещество или материал, предназначенное или используемое для защиты информации.

2. Общие положения

- 2.1. Настоящий Регламент проведения внутреннего контроля соответствия обработки персональных данных в МАДОУ ДС №54 требованиям к защите персональных данных (далее – Регламент), разработан в соответствии с законодательством Российской Федерации о персональных данных (далее – ПДн) и нормативными правовыми актами (методическими документами) федеральных органов исполнительной власти по вопросам безопасности ПДн при их обработке в информационных системах персональных данных (далее – ИСПДн).
- 2.2. Настоящий Регламент определяет порядок проведения внутреннего контроля соответствия обработки ПДн (далее – Внутренний контроль), требованиям к защите ПДн.
- 2.3. Регламент обязателен для исполнения ответственным за организацию обработки ПДн, ответственным за обеспечение безопасности ПДн и администратором информационных систем персональных данных.

3. Порядок проведения внутреннего контроля

- 3.1. Для проведения внутреннего контроля в ИСПДн приказом Директора Учреждения создаётся комиссия, состоящая не менее чем из трех человек с обязательным включением в её состав:
 - ответственного за обеспечение безопасности ПДн в ИСПДн;
 - ответственного за организацию обработки ПДн.
- 3.2. В случае временного отсутствия (болезнь, отпуск, пр.) ответственных, в состав комиссии включаются лица их замещающие.
- 3.3. Допускается привлечение к проверкам сторонних экспертных организаций.
- 3.4. Председатель комиссии организует работу комиссии, решает вопросы взаимодействия комиссии с руководителями и работниками Учреждения, готовит и ведёт заседания комиссии, подписывает протоколы заседаний. По окончании работы комиссии готовится заключение по результатам внутреннего контроля, которое передается на рассмотрение Директору Учреждения.
- 3.5. Внутренний контроль проводится в соответствии с «Планом проведения внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных», утвержденным приказом Директора Учреждения, форма которого приведена в Приложении 1 к настоящему Регламенту.
- 3.6. В «Плане проведения внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных» указывается перечень проводимых мероприятий внутреннего контроля и периодичность их проведения.
- 3.7. Комиссия проводит внутренний контроль непосредственно на месте обработки ПДн, опрашивает работников Учреждения, осуществляющих обработку ПДн, осматривает рабочие места.

- 3.8. При проведении внутреннего контроля должен присутствовать руководитель проверяемого подразделения.
- 3.9. В ходе проведения внутреннего контроля осуществляется:
- контроль выполнения организационных и технических мер по обеспечению безопасности ПДн при их обработке в ИСПДн, необходимых для выполнения требований к защите ПДн;
 - анализ изменения угроз безопасности ПДн в ИСПДн, возникающих в ходе ее эксплуатации;
 - проверка параметров настройки и правильности функционирования программного обеспечения и средств защиты информации (далее – СЗИ);
 - контроль состава технических средств, программного обеспечения и СЗИ;
 - состояние учета СЗИ;
 - состояние учета средств шифровальной (криптографической) защиты информации;
 - состояние учета съемных машинных носителей ПДн;
 - соблюдение правил доступа к ПДн;
 - контроль наличия (отсутствия) фактов несанкционированного доступа к ПДн;
 - соблюдение пользователями ИСПДн парольной политики;
 - соблюдение пользователями ИСПДн антивирусной политики;
 - соблюдение пользователями ИСПДн правил работы со съемными машинными носителями ПДн;
 - контроль соблюдения работниками требований локальных нормативных актов, в т.ч. требований законодательства по вопросам обработки и защиты ПДн;
 - выявление уязвимостей в ИСПДн с использованием специализированных средств инструментального анализа защищенности.
- 3.10. Все работники обязаны по первому требованию членов комиссии предъявить для проверки все числящиеся за ними материалы и документы, дать устные или письменные объяснения по существу заданных им вопросов.
- 3.11. По завершении внутреннего контроля комиссией составляется «Акт о проведении контроля соответствия обработки персональных данных», форма которого приведена в Приложении 2 к настоящему Регламенту.
- 3.12. В «Акте о проведении контроля соответствия обработки персональных данных» указываются:
- перечень проведенных мероприятий;
 - выявленные нарушения;
 - мероприятия по устранению нарушений;
 - решения по результатам внутреннего контроля;
 - сроки устранения нарушений.

- 3.13. Периодичность проведения внутреннего контроля составляет не реже 1 раза в год.
- 3.14. Предложения о создании комиссии и о плановом/внеплановом проведении внутреннего контроля представляются Директору Учреждения ответственным за организацию обработки ПДн и ответственным за обеспечение безопасности ПДн в ИСПДн.
- 3.15. Внеплановый контроль проводится в следующих случаях:
 - наличие подозрений на нарушение требований по защите ПДн;
 - наличие подозрений на осуществление попыток несанкционированного доступа к ПДн;
 - наличие подозрений на сбой в работе технических средств ИСПДн, в т.ч. средств защиты информации;
 - предстоящая проверка надзорными органами.
- 3.16. Порядок проведения внепланового контроля совпадает с порядком проведения планового контроля.
- 3.17. При выявлении в ходе планового/внепланового контроля нарушений требований по обработке и защите ПДн осуществляется оперативное устранение выявленных нарушений.
- 3.18. Выявленные нарушения должны быть устранены в срок, не превышающий 30 дней с момента утверждения «Акта о проведении контроля соответствия обработки персональных данных».
- 3.19. По истечении срока, данного на устранение замечаний, комиссия проводит повторный контроль.

4. Ответственность

- 4.1. Ответственный за организацию обработки ПДн в МАДОУ ДС №54 несет ответственность за организацию проведения внутреннего контроля соответствия обработки ПДн в МАДОУ ДС №54 требованиям к защите ПДн.

5. Срок действия и порядок внесения изменений

- 5.1. Настоящий Регламент вступает в силу с момента его утверждения и действует бессрочно, до замены новым Регламентом.
- 5.2. Настоящий Регламент подлежит пересмотру не реже одного раза в три года.
- 5.3. Изменения и дополнения в настоящий Регламент вносятся приказом заведующего МАДОУ ДС №54.