

Утверждено:
приказом от 04.04.2019 г. №05
заведующий МБДОУ детский сад №12
«Рябинка» С.А. Степанова



Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных

Общие положения

Настоящие Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных (далее - Правила) в муниципальном бюджетном дошкольном образовательном учреждении детский сад №12 «Рябинка» (далее –ДОУ) относятся к основным организационно - распорядительным документам системы документов информационной безопасности и разработаны в соответствии с требованиями постановления Правительства Российской Федерации от 21 марта 2012 г. № 211 "Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом "О персональных данных" и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами".

В Правилах определен порядок организации и осуществления внутреннего контроля обработки персональных данных (ПДн) с целью своевременного выявления и предотвращения:

- хищения технических средств и носителей информации;
- утраты информации;
- преднамеренных программно-технических воздействий на информацию и (или) средства вычислительной техники, вызывающих нарушение целостности информации и нарушение работоспособности автоматизированной системы;
- несанкционированного доступа к ПДн с целью уничтожения, искажения, модификации (подделки), копирования и блокирования;
- утечки информации по техническим каналам.

Внутренний контроль состояния защиты информации включает в себя:

- контроль организации защиты информации;
- контроль эффективности защиты информации.

Порядок внутреннего контроля за соблюдением требований по обработке и обеспечению безопасности персональных данных

В целях осуществления внутреннего контроля соответствия обработки ПДн установленным требованиям организуется проведение периодических проверок условий обработки ПДн. Проверки осуществляются ответственным за организацию обработки ПДн ДОУ в составе комиссии и в соответствии с графиком, определенными приказом «Об утверждении плана внутренних проверок состояния защиты персональных данных».

При осуществлении внутреннего контроля соответствия обработки ПДн установленным требованиям производится проверка:

- соблюдения принципов обработки ПДн;
- соответствия локальных актов в области ПДн действующему законодательству Российской Федерации;
- выполнения работниками требований и правил обработки ПДн в информационных системах персональных данных (ИСПДн) ДОУ;

- актуальности содержащихся в Правилах обработки ПДн в каждой ИСПДн информации о законности целей обработки ПДн и оценке вреда, который может быть причинен субъектам персональных данных в случае нарушения требований по обработке и обеспечению безопасности ПДн;

- правильности осуществления сбора, систематизации, записи, накопления, хранения, уточнения (обновления, изменения), извлечения, использования, передачи (распространения, предоставления, доступа), обезличивания, блокирования, удаления, уничтожения ПДн в каждой ИСПДн;

- актуальности перечня должностей работников ДОУ уполномоченных на обработку ПДн, имеющих доступ к ПДн;

- соблюдения прав субъектов персональных данных, чьи ПДн обрабатываются в ИСПДн;

- соблюдения обязанностей как оператора ПДн, предусмотренных действующим законодательством в области ПДн;

- порядка взаимодействия с субъектами персональных данных, ПДн которых обрабатываются в ИСПДн», в том числе соблюдения сроков, предусмотренных действующим законодательством в области ПДн, соблюдения требований по уведомлению, порядка разъяснения субъектам персональных данных необходимой информации, порядка реагирования на обращения (запросы) субъектов персональных данных, порядка действий при достижении целей обработки ПДн и отзыве согласий субъектами персональных данных;

- наличия необходимых согласий субъектов персональных данных, чьи ПДн обрабатываются в ИСПДн;

- актуальности сведений, содержащихся в уведомлении об обработке (о намерении осуществлять обработку) персональных данных;

- актуальности перечня ИСПДн;

- знания и соблюдения работниками ДОУ положений действующего законодательства Российской Федерации в области ПДн;

- знания и соблюдения работниками положений локальных актов в области обработки и обеспечения безопасности ПДн;

- знания и соблюдения работниками инструкций, руководств и иных эксплуатационных документов на применяемые средства автоматизации, в том числе программное обеспечение, и средства защиты информации;

- соблюдения работниками конфиденциальности ПДн;

- актуальности локальных актов в области обеспечения безопасности ПДн, в том числе в Технических паспортах ИСПДн;

- соблюдения работниками требований по обеспечению безопасности ПДн;

- наличия локальных актов, технической и эксплуатационной документации технических и программных средств ИСПДн;

- по иным вопросам, связанным с защитой ПДн.

По результатам проведенной проверки ответственным за организацию обработки ПДн составляется акт и на основании его принимаются меры, необходимые для устранения выявленных нарушений.

Оценка соотношения вреда, который может быть причинен субъектам персональных данных в случае нарушения требований по обработке и обеспечению безопасности персональных данных

Во время осуществления внутреннего контроля соответствия обработки ПДн установленным требованиям производится оценка соотношения вреда, который может быть причинен субъектам персональных данных в случае нарушения требований по обработке и обеспечению безопасности ПДн и принимаемых мер по обработке и обеспечению безопасности ПДн.

При оценке соотношения вреда, который может быть причинен субъектам персональных данных в случае нарушения требований по обработке и обеспечению безопасности ПДн, для каждой ИСПДн производится экспертное сравнение заявленных в своих локальных актах оценки вреда, который может быть причинен субъектам персональных данных в случае нарушения требований по обработке и обеспечению безопасности ПДн и применяемых мер, направленных на обеспечение выполнения обязанностей, предусмотренных действующим законодательством в области ПДн и изложенных в настоящих Правилах осуществления внутреннего контроля соответствия обработки ПДн в ДОУ.

По итогам сравнений принимается решение о достаточности применяемых мер, направленных на обеспечение выполнения обязанностей, предусмотренных действующим законодательством в области ПДн и возможности или необходимости принятия дополнительных мер или изменения установленного в ДОУ порядка обработки и обеспечения безопасности ПДн.

Оценка соотношения вреда, который может быть причинен субъектам персональных данных в случае нарушения требований по обработке и обеспечению безопасности ПДн и принимаемых мер по обработке и обеспечению безопасности ПДн, в ДОУ оформляется в виде акта.

По результатам принятых решений ответственным за организацию обработки ПДн в ДОУ организуется работа по их реализации.

**Лист ознакомления работников с Правилами осуществления внутреннего
контроля соответствия обработки персональных данных требованиям к
защите персональных данных**

Фамилия, Имя, Отчество	Должность	Дата ознакомления, подпись
Степанова Светлана Анатольевна	Заведующий	
Кохановская Елена Викторовна	Старший воспитатель	
Иванюк Татьяна Григорьевна	Заведующий хозяйством	
Каленская Ирина Евгеньевна	Старшая медицинская сестра	