

**ПРИНЯТО:**

Общим собранием работников  
МДОБУ № 200  
протокол от 26.11.2018г.

**СОГЛАСОВАНО:**

Представительный орган  
работников МДОБУ № 200  
от 26.11.2018г.

Председатель  Л.В.Васильева

**УТВЕРЖДЕНО:**

Приказом МДОБУ № 200

от 26.11.2018г. № 106

Заведующий МДОБУ №200

И.П.Данилова



**ПОЛОЖЕНИЕ  
ОБ ОТВЕТСТВЕННОМ ЗА ИНФОРМАЦИОННУЮ  
БЕЗОПАСНОСТЬ**

**в муниципальном дошкольном образовательном бюджетном  
учреждении «Детский сад комбинированного вида №200»**

г. Оренбург

## **1. Общие положения**

1.1. Настоящее Положение об ответственном за информационную безопасность в муниципальном дошкольном образовательном бюджетном учреждении «Детский сад комбинированного вида №200» (далее- Положение) разработано в соответствии с Федеральным законом от 27.07.2006 № 149 «Об информации, информационных технологиях и о защите информации, Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

1.2. Ответственный за информационную безопасность назначается в МДОБУ №200 в целях выполнения требований действующего законодательства Российской Федерации, иных нормативно-правовых актов, регламентирующих обеспечение защиты информации, в том числе обеспечение безопасности при обработке персональных данных, а также обеспечение защиты и безопасности информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных.

## **2. Задачи**

Основными задачами ответственного за информационную безопасность в МДОБУ № 200 являются:

2.1. Разработка и реализация комплекса организационных и технических мер, направленных на выполнение установленных а к обеспечению безопасности и защите информации, в том числе персональных данных.

2.2. Обеспечение постоянного контроля в МДОБУ №200 за выполнением установленных требований к обеспечению безопасности и защите информации, в том числе персональных данных.

2.3. Разработка и внесение предложений администрации МДОБУ №200 по совершенствованию и развитию корпоративной системы обеспечения безопасности и защиты информации, в том числе персональных данных.

## **3. Функции**

Для выполнения поставленных задач ответственный за информационную безопасность в МДОБУ №200 осуществляет следующие функции:

3.1. Готовит и представляет на рассмотрение администрации ДОУ проекты локальных нормативных актов по вопросам обеспечения защиты информации, в том числе персональных данных.

3.2. Организует и проводит во взаимодействии с администрацией ДОУ классификацию информационных систем на этапе создания информационных систем или в ходе их эксплуатации (для ранее введенных в эксплуатацию и (или) модернизируемых информационных систем) с целью установления методов и способов защиты информации, необходимых для обеспечения безопасности персональных данных в соответствии с установленными требованиями.

3.3. Разрабатывает и реализует комплекс организационных мер по обеспечению защиты информации от:

- неправомерного доступа;
- уничтожения;
- модифицирования;
- блокирования;
- копирования;
- предоставления;
- распространения;
- иных неправомерных действий в отношении такой информации.

3.4. Для защиты информации, в том числе персональных данных от неправомерного доступа ответственный за информационную безопасность в МДОБУ №200 обеспечивает:

- контроль за строгим соблюдением принятого администрацией ДОУ Порядка доступа к конфиденциальной информации, в том числе к персональным данным;
- предотвращение несанкционированного доступа к информации и (или) передачи ее лицам, не имеющим права на доступ к информации;
- своевременное обнаружение фактов несанкционированного доступа к информации;
- предупреждение возможности неблагоприятных последствий нарушения порядка доступа к информации;
- возможность незамедлительного восстановления информации, модифицированной или уничтоженной вследствие несанкционированного доступа к ней.

3.5. Ответственный за информационную безопасность в МДОБУ №200 при создании и эксплуатации корпоративных информационных систем:

- самостоятельно разрабатывает и внедряет методы и способы защиты информации, соответствующие установленным требованиям;
- согласовывает исполнителю планируемые для использования в целях защиты информации методы и способы при условии их соответствия установленным требованиям.

3.6. Ответственный за информационную безопасность в МДОБУ №200:

- разрабатывает и реализует меры организационного и технического по недопущению воздействия на технические средства обработки информации, в результате которого нарушается их функционирование;
- организует и(или) проводит экспертизу технических средств, используемых при обработке информации на предмет соответствия возможностей защиты информации указанных средств установленным требованиям.

3.7. Ответственный за информационную безопасность в МДОБУ №200 разрабатывает и реализует меры по информированию и обучению персонала МДОБУ №200, в том

числе вновь принимаемых на работу лиц, по вопросам защиты информации и персональных данных.

3.8. Ответственный за информационную безопасность в МДОБУ №200 контролирует выполнение установленных требований по:

- осуществлению обмена 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;
- размещению информационных систем, специального оборудования и охране помещений, в которых ведется работа с персональными данными, организации режима обеспечения безопасности в этих помещениях в части обеспечения сохранности носителей персональных данных и средств защиты информации, а также исключения возможности неконтролируемого проникновения или пребывания в этих помещениях посторонних лиц;
- соблюдению парольной защиты;
- соблюдению установленного регламента работы с электронной почтой;
- соблюдению требований к программному обеспечению и его использованию.

3.9. В соответствии с установленными нормативно-правовыми актами требованиями ответственный за информационную безопасность в МДОБУ №200 обеспечивает:

- определение угроз безопасности персональных данных при их обработке, формирование на их основе модели угроз;
- разработку на основе модели угроз системы защиты персональных данных, обеспечивающей нейтрализацию предполагаемых угроз с использованием методов и способов защиты персональных данных, предусмотренных для соответствующего класса информационных систем;
- проверку готовности средств защиты информации к использованию с составлением заключений о возможности их эксплуатации;
- установку и ввод в эксплуатацию средств защиты информации в соответствии с эксплуатационной и технической документацией;
- обучение лиц, использующих средства защиты информации, применяемые в информационных системах, правилам работы с ними;
- учет применяемых средств защиты информации, эксплуатационной и технической документации к ним, носителей персональных данных;
- учет лиц, допущенных к работе с персональными данными в информационной системе;
- контроль за соблюдением условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией;
- разбор 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;

- описание системы защиты информации, в том числе персональных данных;
- ежегодное планирование работы по совершенствованию системы защиты информации, в том числе персональных данных;
- подготовку и предоставление отчетов заведующему, а также по требованию надзорных и иных уполномоченных органов об организационных и технических мероприятиях по защите информации, в том числе персональных данных;
- постоянный контроль за обеспечением уровня защищенности информации.

#### **4. Взаимодействие**

Для решения поставленных задач и осуществления предусмотренных настоящим Положением функций ответственный за информационную безопасность в МДОБУ №200 взаимодействует:

- с руководителем МДОБУ и его заместителями;
- с сотрудниками МДОБУ;
- с государственными, муниципальными органами, учреждениями и организациями, с надзорными органами, а также с иными органами, предприятиями и организациями.

В ходе взаимодействия руководитель и ответственный за информационную безопасность в ДОУ:

- в установленном порядке, получают необходимую для осуществления деятельности ответственного за информационную безопасность в ДОУ информацию, разъяснения, уточнения, нормативные и иные документы;
- готовит и в установленном порядке вносят заведующему предложения по проведению организационных и технических мероприятий, изданию локальных нормативных актов, принятию иных мер по установленным направлениям деятельности в сфере защиты информации, в том числе персональных данных;
- готовят и в установленном порядке предоставляют информацию по находящимся в их компетенции вопросам в сфере защиты информации, в том числе персональных данных, по запросам сотрудников ДОУ, государственных, муниципальных органов, учреждений и организаций, надзорных органов, а также иных органов, предприятий и организаций.

#### **5. Ответственность**

5.1. Ответственный за информационную безопасность в ДОУ несет ответственность перед руководством ДОУ согласно действующему законодательству, нормативно-правовым и локальным нормативным правовым актам за обеспечение:

- выполнения поставленных задач и функций,
- работы с документами и их сохранности, своевременного и качественного исполнения поручений и обращений,

- выполнения требований правил внутреннего трудового распорядка ДОУ.

5.2. Ответственность за оперативную работу с поступающими документами и контроль за их исполнением в МДОБУ №200, несет ответственный за информационную безопасность в ДОУ.

5.3. Ответственный за информационную безопасность в МДОБУ №200 несет ответственность за своевременное и качественное выполнение:

- требований выполнения действующего законодательства Российской Федерации, иных нормативно-правовых документов, регламентирующих обеспечение защиты информации, в том числе обеспечение безопасности при обработке персональных данных;

- обязанностей, предусмотренных Трудовым кодексом РФ, правилами внутреннего трудового распорядка, коллективным договором, настоящим Положением, трудовыми договорами и должностными инструкциями.