Утверждаю:
Заведующий МБДОУ д/с № 8
Л.А. Семенякина
Приказ от 03.09.2014 г. за № 213

Регламент
по защите информации ограниченного доступа и при обработке
в МБДОУ д/с № 8

1. Общие положения

1.1. Настоящий Регламент по защите информации ограниченного доступа в муниципальном бюджетном дошкольном образовательном учреждении детском саду комбинированного вида № 8 (далее - Регламент) определяет комплекс организационных и технических мероприятий в части защиты информации ограниченного доступа, не составляющей государственной тайны (далее — информация), при ее обработке, обращении, хранении и передаче по Интернет.

1.2. Регламент разработан в соответствии с Трудовым кодексом РФ, Федеральным законом РФ от 27.07.2006г. №152-ФЗ «О персональных данных», постановлением Правительства Российской Федерации от 17.11.2007 г. №781 «Об утверждении положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных», Указом Президента Российской Федерации от 6 марта 1997 г. № 188 "Об утверждении Перечня сведений конфиденциального характера" (в ред. от 23.09.2005г. № 1111), Уставом МБДОУ д/с № 8, утвержденным Распоряжение администрации города Белгорода" от 10 ноября 2011 года " от 3697.

1.3. Ответственность за организацию работ по защите информации на объектах информатизации, размещенных в МБДОУ д/с № 8, возлагается на делопроизводителя (автоматизированные системы различного уровня и назначения, системы связи, отображения и размножения вместе с помещениями, в которых они установлены, предназначенные для обработки и передачи информации, подлежащей защите).

2. Обязанности должностных лиц по защите информации, обрабатываемой на объектах информатизации

2.1. Работники МБДОУ д/с № 8, допущенные для выполнения своих должностных обязанностей к работе с информацией на персональных электронно-вычислительных машинах, входящих в состав объекта информатизации (далее - пользователь), обязаны выполнять предусмотренные в МБДОУ д/с № 8 меры по защите информации.

2.2. Ответственные лица за обеспечение информационной безопасности обязаны:

· принимать решение об ограничении доступа к информации в порученной сфере ответственности;

· участвовать в подготовке Перечня сведений ограниченного доступа МБДОУ д/с № 8;

· определять перечень пользователей, которым для исполнения должностных обязанностей необходим допуск к информации;

· организовать учет и хранение бумажных и машинных носителей информации;

· принимать участие в уточнении обязанностей назначенных за обеспечение

необходимых для выполнения функций управления в установленной сфере деятельности;
· контролировать соблюдение пользователями требований настоящего Регламента при обработке информации на персональных электронно-вычислительных машинах;
· информировать руководителя учреждения при обнаружении фактов разглашения информации;
2.3. Работники, отвечающие за защиту информации на объектах информатизации, обязаны:
· иметь список пользователей объекта информатизации управления;
· разграничивать доступ пользователей и обслуживающего персонала к информационным ресурсам, программным средствам обработки (передачи) и защиты информации на объекте информатизации;
· принимать участие в разработке инструкции по обеспечению безопасности информации на объектах информатизации, создаваемых в МБДОУ д/с № 8;
· своевременно информировать руководителя учреждения о допущенных нарушениях установленного порядка защиты информации.
2.4. Пользователь обязан:
· перед началом работы на ПЭВМ проверить свои рабочие папки на жестком магнитном диске, съемные машинные носители информации (дискеты, компакт-диски и т. п.) на отсутствие вирусов с помощью штатных средств антивирусной защиты;
· при необходимости использования машинных носителей информации, поступивших из других учреждений, предприятий и организаций провести проверку этих носителей на отсутствие вирусов;
· при сообщениях тестовых программ о появлении вирусов немедленно прекратить работу, сообщить делопроизводителю по защите информации;
· при обработке информации использовать только машинные носители информации, состоящие на балансе МБДОУ д/с № 8;
· соблюдать правила работы со средствами защиты информации и установленный (в случае необходимости) режим разграничения доступа к техническим средствам, программам, файлам с информацией при ее обработке;
· при выходе в течение рабочего дня из помещения, в котором размещается объект информатизации, убирать машинные носители информации в запираемое хранилище;
· осуществлять ввод личного пароля в отсутствии посторонних лиц и не производить его запись на любые носители;
· при обнаружении различных неисправностей в работе компьютерной техники, программном обеспечении сообщить ведущему инженеру-программисту (администратору) по защите информации.

3. Мероприятия по защите информации на объектах информатизации

3.1. В целях реализации организационных и технических мероприятий по защите информации на объектах информатизации необходимо разрабатывать руководящие документы по защите информации в МБДОУ:
· модель угроз информационной безопасности;
· перечень защищаемых объектов информатизации;

· акты о категорировании защищаемых объектов информатизации;
· документа о вводе в эксплуатацию средств вычислительной техники, обрабатывающих информацию, приказ о назначении работника, ответственного за эксплуатацию средств защиты информации на объекте информатизации;
· инструкция по антивирусной защите.

3.2. В целях реализации технических мер защиты информации на объектах информатизации организуется их аттестация (комплекс организационно-технических мероприятий, в результате которых посредством специального документа (аттестата соответствия) подтверждается, что объект информатизации соответствует требованиям стандартов или иных нормативно-технических документов по безопасности информации и осуществляется антивирусная защита ПЭВМ.

Аттестация объектов информатизации проводится специализированной организацией, имеющей лицензию на право работы в области защиты информации.

Антивирусная защита информации на объектах информатизации осуществляется путем:
· внедрения и применения средств антивирусной защиты информации;
· обновления баз данных средств антивирусной защиты информации;
· своевременных действий при обнаружении заражения информации программными вирусами.