УТВЕРЖДЕНО:
Заведующим МБДОУ д/с №14
_____ Е.И. Чепелевой
Приказ № 144/2
от «08» 08 20 21 г

ИНСТРУКЦИЯ
ответственного за обеспечение безопасности информации
в муниципальном бюджетном дошкольном образовательном учреждении
детский сад №14 «Центр развития ребенка
«Золотой ключик» г. Белгорода

СОДЕРЖАНИЕ

Обозначения и сокращения 3
1. Общие положения 4
2. Обязанности ответственного 5

ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

В настоящем документе применяются следующие обозначения и сокращения:

АРМ	– автоматизированное рабочее место
ИСПДн	– информационная система персональных данных
ЛВС	– локальная вычислительная сеть
МЭ	– межсетевой экран
НСД	– несанкционированный доступ
ОС	– операционная система
ПДн	– персональные данные
ПК	– персональный компьютер
ПО	– программное обеспечение
РД	– руководящие документы
СЗИ	– средство защиты информации
СЗПДн	– система защиты персональных данных

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1 Ответственный за обеспечение безопасности информации назначается приказом руководителя муниципального бюджетного дошкольного образовательного учреждения детский сад №14 «Центр развития ребенка «Золотой ключик» г. Белгорода (далее – Учреждение).

1.2 Ответственный за обеспечение безопасности информации подчиняется непосредственно руководителю или лицу, замещающему руководителя.

1.3 Ответственный за обеспечение безопасности информации в своей работе руководствуется настоящей инструкцией, Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных», законодательством РФ, руководящими и нормативными документами ФСТЭК России, ФСБ России, Роскомнадзора, а также регламентирующими документами Учреждения в области защиты персональных данных.

1.4 Ответственный за обеспечение безопасности информации является должностным лицом Учреждения, уполномоченным на внутренний контроль за соблюдением требований законодательства Российской Федерации при обработке персональных данных, в том числе требований к защите персональных данных, проведение работ по защите информации, содержащей персональные данные и поддержанию достигнутого уровня защиты персональных данных, обрабатываемых с использованием средств автоматизации и без использования таковых.

1.5 Ответственный за обеспечение безопасности информации должен иметь специальное рабочее место, размещенное в здании Учреждения так, чтобы исключить несанкционированный доступ к нему посторонних лиц и других пользователей.

1.6 На рабочем месте ответственного за обеспечение безопасности информации должны присутствовать средства физической защиты внешних электронных и бумажных носителей информации (личный сейф, железный шкаф).

1.7 Ответственный за обеспечение безопасности информации осуществляет методическое руководство сотрудников, допущенных к обработке ПДн, к техническим средствам информационной системы персональных данных персональных данных персональных данных и информационной системы персональных данных персональных данных персональных данных (ИСПДн) и иной конфиденциальной информации, в вопросах обеспечения безопасности информации.

1.8 Требования ответственного за обеспечение безопасности информации, связанные с выполнением им своих должностных обязанностей, обязательны для исполнения всеми работниками Учреждения, имеющими доступ к конфиденциальной информации.

1.9 Ответственный за обеспечение безопасности информации несет персональную ответственность за качество проводимых им работ по контролю действий пользователей при работе в ИСПДн, состояние и поддержание установленного уровня защиты ИСПДн.

1.10 Ответственный за обеспечение безопасности информации по согласованию с руководителем Учреждения для консультаций по выбору и реализации методов и способов защиты информации в информационной системе может привлекать организацию, имеющую оформленную в установленном порядке лицензию на осуществление деятельности по технической защите конфиденциальной информации.

2. ОБЯЗАННОСТИ ОТВЕТСТВЕННОГО

2.1 В рамках поставленных перед ответственным за обеспечение безопасности информации задач, на него возлагаются следующие функции:

организовать предоставление субъекту персональных данных либо его представителю по запросу информацию об обработке его персональных данных;

осуществлять внутренний контроль за соблюдением требований законодательства Российской Федерации при обработке конфиденциальной информации, в том числе требований к защите персональных данных;

доводить до сведения лиц, допущенных к обработке персональных данных, положения законодательства РФ о персональных данных, нормативных правовых актов по вопросам обработки персональных данных, требований к защите персональных данных;

организовать прием и обработку обращений и запросов субъектов персональных данных или их представителей и (или) осуществлять контроль за приемом и обработкой таких обращений и запросов;

организовать получение обязательства о прекращении обработки персональных данных у лиц, непосредственно осуществляющих обработку персональных данных, в случае расторжения с ним договора (контракта);

проводить систематический анализ состояния защиты информации по вопросам, входящим в его компетенцию;

соблюдать правила использования конфиденциальной информации и персональных данных, порядок учета и хранения, исключать доступ к информации посторонних лиц.

2.2 Ответственный за обеспечение безопасности информации обязан:

знать и выполнять требования действующих нормативных и руководящих документов, а также внутренних инструкций, распоряжений, регламентирующих порядок действий по защите персональных данных;

уточнять в установленном порядке обязанности пользователей и администраторов ИСПДн;

контролировать неизменность состояния защищенности информационных системах персональных данных персональных данных обработки персональных данных;

контролировать обработку ПДн без использования средств автоматизации согласно принятому в учреждении порядку обработки персональных данных без использования средств автоматизации и Положению об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации, утвержденному Постановлением правительства РФ № 687 от 15 сентября 2008г;

ответственный за обеспечение безопасности информации выполняет свои обязанности индивидуально или в составе рабочих групп, формируемых распоряжениями руководства Учреждения;

при доступе или обработке персональных данных ответственному за обеспечение безопасности информации запрещается: использовать сведения, содержащие персональные данные, в неслужебных целях; передавать персональные данные по незащищенным каналам связи без использования сертифицированных средств криптографической защиты информации; снимать

копии с документов и других носителей информации, содержащих персональные данные, или производить выписки из них, а равно использовать различные технические средства (видео- и звукозаписывающую аппаратуру) для фиксации сведений, содержащих персональные данные.

ответственный за обеспечение безопасности информации, виновный в нарушении требований законодательства о защите персональных данных, в том числе допустившие разглашение персональных данных, несет персональную гражданскую, уголовную, административную, дисциплинарную и иную, предусмотренную законодательством ответственность.