Белоярский район
Ханты-Мансийский автономный округ – Югра

Муниципальное автономное дошкольное образовательное учреждение
Белоярского района «Центр развития ребенка -детский сад «Сказка» г. Белоярский»
(МАДОУ «Детский сад «Сказка» г. Белоярский»)

ПРИКАЗ

15.09.2020г. **№ 460**

Белоярский

Об утверждении инструкций в области информационной безопасности в МАДОУ «Центр развития ребенка – детский сад «Сказка» г. Белоярский»

Во исполнение положений Постановления Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»

ПРИКАЗЫВАЮ:

1. Утвердить:

1.1. Инструкцию пользователей информационных систем персональных данных (Приложение 1 к настоящему приказу);

1.2. Инструкцию персонала на случай возникновения внештатных ситуаций (Приложение 2 к настоящему приказу);

1.3. Инструкцию о порядке учета и хранения съемных носителей информации (Положение 3 к настоящему приказу);

1.4. Инструкцию, определяющую порядок охраны, внутри объектовый режим и порядок допуска лиц в помещения, в которых ведется обработка персональных данных (Приложение 4 к настоящему приказу);

1.5. Инструкцию о порядке резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации информационных систем персональных данных (Приложение 5 к настоящему приказу).

2. Ответственному за обеспечение безопасности персональных данных обеспечить контроль предварительного ознакомления всех пользователей, допущенных к информационным системам персональных данных, с действующими редакциями прилагаемых инструкций.

3. Контроль исполнения настоящего приказа оставляю за собой.

Заведующий **Курбачева О.В.**

Приложение 1
к приказу № 460 от 15.09.2020г.

Инструкция пользователей информационных систем персональных данных МАДОУ «Центр развития ребенка – детский сад «Сказка» г. Белоярский»

1. Каждый сотрудник, участвующий в рамках своих функциональных обязанностей в автоматизированной обработке персональных данных и имеющий доступ к соответствующим данным (далее – «Пользователь»), несет персональную ответственность за свои действия.

2. В процессе использования информационных систем персональных данных (далее – «ИСПДн») все Пользователи обязаны выполнять следующие требования:

2.1. знать и соблюдать нормативные требования в области защиты персональных данных, а также обязательные правила, установленные локальными нормативными актами МАДОУ «Центр развития ребенка – детский сад «Сказка» г. Белоярский» (далее – МАДОУ), доведенные до сведения Пользователя;

2.2. выполнять только те операции, которые соответствуют должностным (служебным) обязанностям Пользователя, указанным в заключенном с ним договоре, его должностной инструкции и других документах, регламентирующих рабочий процесс;

2.3. располагать экраны устройств вывода информации (мониторов) таким образом, чтобы исключить возможность ознакомления с отображаемой на них информацией посторонними лицами;

2.5. соблюдать установленный режим разграничения доступа к информационным ресурсам, получать средства доступа к ИСПДн (логины и пароли) только от уполномоченных сотрудников, самостоятельно изменять их и хранить в тайне;

2.6. немедленно докладывать Ответственному лицу обо всех фактах и попытках несанкционированного доступа к персональным данным, обрабатываемым в ИСПДн, а равно об иных нарушениях их безопасности (уничтожении, искажении, блокировании);

2.7. не подключать съемные носители информации к устройствам, предназначенным для доступа к ИСПДн;

2.8. не осуществлять хранение персональных данных, обрабатываемых в рамках выполнения служебных обязанностей Пользователя, на локальных дисках своих рабочих ноутбуков и иных персональных компьютеров;

2.9. блокировать рабочие персональные компьютеры, устройства при покидании рабочего места, чтобы исключить возможность ознакомления с отображаемой и хранящейся на них информацией посторонними лицами.

3. Пользователям запрещается:

3.1. хранить персональные данные на съемных носителях информации;

3.2. выносить рабочие персональные компьютеры за пределы служебных помещений за исключением случаев, когда это прямо предусмотрено локальными нормативными актами МАДОУ, распоряжением работодателя или трудовым договором;

3.3. отключать (блокировать) средства защиты информации, функционирующие на устройствах Пользователя;

3.4. производить изменения в монтаже и размещении рабочих технических средств;

3.5. самостоятельно устанавливать или модифицировать программное обеспечение, изменять установленный алгоритм функционирования технических и программных средств;

3.6. сообщать или передавать другим лицам (в том числе, другим сотрудникам) личные средства доступа к ИСПДн или рабочим устройствам Пользователя;

3.7. работать на устройствах, используемых для доступа к ИСПДн, при обнаружении их неисправностей до их устранения Ответственным лицом;

3.8. привлекать посторонних лиц для целей ремонта или технического обслуживания устройств, используемых для доступа к ИСПДн без согласования с Ответственным лицом.

4. Пользователи обязаны выполнять указания уполномоченных лиц МАДОУ, направленные на обеспечение возможности обслуживания технических средств ИСПДн, установки необходимого программного обеспечения, его обновления, а также проведения работ по резервированию технических средств и обрабатываемых с их помощью персональных данных.

Приложение 2
к приказу № 460 от 15.09.2020г.

Инструкция персонала на случай возникновения внештатных ситуаций в МАДОУ «Центр развития ребенка – детский сад «Сказка» г. Белоярский»

1. Настоящая Инструкция определяет возможные внештатные ситуации, связанные с функционированием объектов вычислительной техники МАДОУ «Центр развития ребенка – детский сад «Сказка» г. Белоярский» (далее – МАДОУ), меры и средства поддержания непрерывности работы и восстановления работоспособности информационных систем персональных данных (далее – «ИСПДн»). Под внештатной ситуацией понимается происшествие, связанное со сбоем в функционировании элементов ИСПДн, создающее угрозу безопасности (целостности, конфиденциальности или доступности) персональных данных.
2. Действие настоящей Инструкции распространяется на всех пользователей объектов вычислительной техники, участвующих в автоматизированной обработке персональных данных (далее – «Пользователи»).
3. По степени серьезности и размерам наносимого ущерба внештатные ситуации разделяются на следующие категории:
3.1. угрожающая ситуация – приводит к полному выходу ИСПДн из строя и ее неспособности выполнять свои функции, а также к уничтожению, блокированию, неправомерной модификации или разглашению персональных данных;
3.2. серьезная ситуация – приводит к выходу из строя отдельных компонентов ИСПДн (частичной потере работоспособности), потере производительности, а также к незначительному нарушению целостности и доступности данных.
4. В случае возникновения угрожающей или серьезной внештатной ситуации действия персонала включают следующие этапы:
4.1. немедленная реакция;
4.2. восстановление работоспособности ИСПДн и возобновление обработки данных;
4.3. расследование причин внештатной ситуации и установление виновных.
5. Немедленная реакция включает следующие действия:
5.1. Пользователь, выявивший соответствующее происшествие, в кратчайшие сроки после выявления внештатной ситуации любым возможным способом уведомляет о ней Ответственного за обработку персональных данных, а также оказывает ему содействие, необходимое для устранения и расследования причин внештатной ситуации;
5.2. Ответственный за обработку персональных данных:

5.2.1. ставит в известность Пользователей всех смежных систем о факте возникновения внештатной ситуации для их перехода на аварийный режим работы (приостановки работы);

5.2.2. определяет степень серьезности происшествия;

5.2.3. оповещает Пользователей ИСПДн и взаимодействующих систем о характере внештатной ситуации и ориентировочном времени возобновления работы.

6. Восстановление работоспособности ИСПДн и возобновление обработки данных включают следующие действия:

6.1. Ответственный за обработку персональных данных:

6.1.1. обеспечивает отключение пораженных компонентов или переключение на использование дублирующих ресурсов (резерва);

6.1.2. обеспечивает восстановление работоспособности поврежденных аппаратных средств и другого оборудования, при необходимости – замену отказавших узлов и блоков резервными;

6.1.3. обеспечивает восстановление необходимых данных, используя резервные копии;

6.1.4. проверяет работоспособность поврежденной ИСПДн, удостоверяясь в том, что последствия внештатной ситуации не оказывают воздействия на дальнейшую работу системы;

6.1.5. уведомляет Пользователей о готовности к работе;

6.2. в случае нарушения целостности данных Пользователи повторяют действия, выполненные в течение периода, прошедшего с даты последнего резервирования данных.

7. Расследование причин возникновения внештатной ситуации включает определение следующих факторов, которые устанавливаются Ответственным за обработку персональных данных:

7.1. характер ситуации (случайный или преднамеренный);

7.2. прогнозируемость ситуации;

7.3. причины ситуации (неэффективность средств защиты, нарушение требований локальных нормативных актов, другие);

7.4. степень нанесенного ущерба;

7.5. соответствие фактического ущерба прогнозу;

7.6. возможность восполнения ущерба;

7.7. повторяемость ситуации;

7.8. виновные лица;

7.9. меры, необходимые для исключения повторения внештатной ситуации.

8. Отчет о результатах расследования и предложения по совершенствованию системы защиты ИСПДн направляется заведующему МАДОУ.

Приложение 3
к приказу № 460 от 15.09.2020г.

Инструкция
по порядку учёта и хранения съёмных носителей персональных данных
в МАДОУ «Центр развития ребенка – детский сад «Сказка» г. Белоярский»

1. Общие положения

1.1. Настоящая «Инструкция по учёту и хранению съёмных носителей персональных данных» (далее - Инструкция) определяет порядок работы со съёмными носителями персональных данных в МАДОУ «Центр развития ребенка – детский сад «Сказка» Белоярский» (далее - Оператор) в соответствии с Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных», постановлением Правительства РФ от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», иными нормативными правовыми актами РФ в области защиты персональных данных.

1.2. С Инструкцией знакомятся под подпись и выполняют её все лица, допущенные к обработке персональных данных в соответствии с утвержденным заведующим МАДОУ списком лиц, допущенных к обработке персональных данных в МАДОУ «Центр развития ребенка - детский сад «Сказка г. Белоярский».

2. Определения

Съёмный носитель персональных данных — носитель информации, используемый для хранения и передачи персональных данных в электронной форме.

Пользователь - работник Оператора или сотрудник по договору гражданско-правового характера, допущенный к обработке персональных данных «Приказом о допуске к обработке персональных данных».

3. Порядок работы со съёмными носителями

3.1. Ответственный за обеспечение безопасности персональных данных, либо уполномоченный им работник, выдаёт съёмные носители пользователям только в случаях производственной необходимости.

3.2. Все съёмные носители персональных данных учитываются и выдаются пользователям под подпись.

3.3. Пользователям, получившим съёмные носители персональных данных под подпись, запрещается передавать их третьим лицам.

3.4. Ответственный за обеспечение безопасности персональных данных, либо уполномоченный им работник, изымает съёмные носители персональных данных при увольнении пользователя.

3.5. Все съёмные носители персональных данных хранятся в запираемых шкафах или сейфах (металлических шкафах) с кодовыми или внутренними замками (с не менее чем двумя дубликатами ключей).

3.6. Допускается хранение съёмных носителей персональных данных вне запираемых шкафов или сейфов (металлических шкафов) при условиях уничтожения персональных данных в соответствии с Инструкцией по порядку уничтожения и обезличивания персональных данных, либо если на съёмном носителе персональных данных хранятся только персональные данные в зашифрованном или обезличенном виде.

3.7. Право на перемещение съёмных носителей информации за пределы территории, на которой осуществляется обработка, имеют только те лица, которым это необходимо для выполнения своих должностных обязанностей.

3.8. Использование неучтённых съёмных носителей для обработки персональных данных фиксируется как несанкционированное, а ответственный за обеспечение безопасности персональных данных инициирует служебную проверку. По факту выясненных обстоятельств составляется Акт проведения расследования инцидента.

3.9. Пользователи, в случаях утраты или кражи съёмных носителей персональных данных, сообщают об этом ответственному за обеспечение безопасности персональных данных.

3.10. Съёмные носители персональных данных, пришедшие в негодность, или отслужившие в установленный срок, подлежат уничтожению в соответствии с Инструкцией по порядку уничтожения и обезличивания персональных данных. По результатам уничтожения составляется Акт уничтожения персональных данных.

4. Порядок организации учёта съёмных носителей

4.1. На каждом съёмном носителе персональных данных размещается этикетка с уникальным учётным номером.

4.2. Ответственный за обеспечение безопасности персональных данных, либо уполномоченный им работник, при выдаче, приёме, уничтожении съёмных носителей персональных данных вносит в Журнал учета съёмных носителей персональных данных (Приложение 1):

- учётный номер, размещённый на этикетке на съёмном носителе персональных данных;
- тип съёмного носителя (USB-накопитель, внешний жёсткий диск, CD/DVD диск);
- серийный или инвентарный номер съёмного носителя;
- место хранения (номер запираемого шкафа или сейфа, номер помещения);

- дату и номер Акта уничтожения персональных данных в случае уничтожения съёмного носителя;
- подпись.

4.3. Пользователи при получении либо сдаче съёмных носителей персональных данных заносят в Журнал учёта съёмных носителей персональных данных свои фамилию, имя, отчество, ставят дату и подпись.

5. Ответственность

5.1. Все работники Оператора, допущенные в установленном порядке к работе с персональными данными, несут административную, материальную, уголовную ответственность в соответствии с действующим законодательством за обеспечение сохранности и соблюдению правил работы с персональными данными.

5.2. Ответственность за доведение требований настоящей Инструкции до работников Оператора несёт ответственный за организацию обработки персональных данных.

5.3. Ответственность за обеспечение мероприятий по реализации требований настоящей Инструкции, в том числе учёт, выдачу, уничтожение съёмных носителей персональных данных несёт ответственный за обеспечение безопасности персональных данных.

Приложение 4
к приказу № 460 от 15.09.2020г.

Инструкция, определяющая порядок охраны, внутри объектовый режим и порядок допуска лиц в помещения, в которых ведется обработка персональных данных в МАДОУ «Центр развития ребенка – детский сад «Сказка» г. Белоярский»

1. Общие положения

1.1. Настоящая Инструкция определяет процедуру доступа работников МАДОУ «Центр развития ребенка – детский сад «Сказка» г. Белоярский» (далее – МАДОУ) в помещения, в которых ведется обработка персональных данных и разработан в соответствии с постановлением Правительства Российской Федерации от 21 марта 2012 года № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом от 27.07.2006 №152-ФЗ «О персональных данных».

1.2. Целью настоящей Инструкции является обеспечение исключения неправомерного или случайного доступа к материальным носителям персональных данных и техническим средствам их обработки, а также иных неправомерных действий в отношении персональных данных.

2. Порядок доступа в помещения, в которых ведется обработка персональных данных

2.1. Доступ работников МАДОУ, в помещения, в которых ведется обработка персональных данных, осуществляется согласно списку работников МАДОУ, допущенных к обработке персональных данных, утвержденным приказом заведующего МАДОУ.

2.2. Пребывание посторонних лиц в кабинетах, в которых ведется обработка персональных данных, допускается только в присутствии работников, указанных в списке работников МАДОУ, допущенных к обработке персональных данных, утвержденным приказом заведующего МАДОУ.

2.3. Работники контролирующих органов допускаются в помещение (отделения), в котором ведется обработка персональных данных, при наличии соответствующего предписания на проведение контрольных мероприятий с разрешения заведующего МАДОУ, в его присутствии или лица, его замещающего.

2.4. Работники сторонних организаций, прибывшие в помещение, в котором ведется обработка персональных данных, для выполнения работ, оказания услуг в соответствии с заключенными МАДОУ государственными контрактами (договорами) допускаются в

помещение с разрешения заведующего МАДОУ (лица его замещающего) на основании информации, полученной от ответственного за организацию и выполнение работ по государственному контракту (договору).

2.5. При проведении таких работ работники, допущенные к работе с персональными данными, по приказу заведующего МАДОУ обязаны принять меры по исключению ознакомления работников сторонних организаций с персональными данными.

3. Порядок вскрытия и сдачи под охрану помещений, в которых ведется обработка персональных данных.

3.1. Помещения, в которых ведется обработка персональных данных, по окончании рабочего дня должны закрываться на ключ. Ключи от замков передаются и находятся на ответственном хранении у сотрудников МАДОУ, работающих в служебных помещениях, а также у сотрудника, уполномоченного хранить резервные ключи от замков всех помещений.

3.2. Вскрытие и закрытие помещения осуществляют сотрудники МАДОУ, допущенные в данное помещение.

3.3. При завершении рабочего дня сотрудники МАДОУ, допущенные к обработке персональных данных, утвержденные приказом заведующего МАДОУ, обязаны выполнить следующие мероприятия:

- убрать документы с персональными данными в шкафы, сейфы или запирающиеся на ключ шкафы;
- выключить установленным порядком вычислительную технику и оргтехнику;
- закрыть окна;
- выключить электроприборы;
- выключить свет;
- закрыть входную дверь на замок;
- ключ от входной двери в помещение сотрудник сохраняет у себя.

3.4. Сотрудники, вскрывающие помещение, в котором ведется обработка персональных данных, обязаны выполнить следующие мероприятия:

- проверить целостность входной двери помещения;
- вскрыть помещение;
- проверить целостность сейфа (шкафа, тумбочек), наличие и целостность компьютерной и оргтехники;
- при обнаружении нарушения целостности двери, сейфа, шкафа, тумбочек, отсутствии или нарушении целостности вычислительной техники, других нарушениях сотрудник,

вскрывающий помещение, в котором ведется обработка персональных данных, обязан прекратить вскрытие помещения, доложить о выявленных нарушениях своему непосредственному руководителю.

4. Запрещается

4.1. Запрещается оставлять помещения, в которых ведется обработка персональных данных, без присмотра работников, имеющих допуск в помещения, где ведется обработка персональных данных.

4.2. Запрещается оставлять без присмотра находящихся в помещении, в которых ведется обработка персональных данных, посторонних лиц, а также, работников, не имеющих допуск в помещения, в которых ведется обработка персональных данных.

5. Внутренний контроль

5.1. Внутренний контроль за соблюдением порядка доступа в помещения, в которых ведется обработка персональных данных, осуществляется лицом, ответственным за обработку персональных данных.

6. Ответственность

6.1. Работники, нарушившие нормы настоящей Инструкции, несут ответственность в соответствии с действующим законодательством.

Приложение 5
к приказу № 460 от 15.09.2020г.

Инструкция о порядке резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации информационных систем персональных данных в МАДОУ «Центр развития ребенка – детский сад «Сказка» г. Белоярский»

1. Назначение и область действия

Порядок резервирования и восстановления работоспособности ТС и ПО, баз данных и СЗИ определяет действия (далее - Инструкция), связанные с функционированием ИСПДн, меры и средства поддержания непрерывности работы и восстановления работоспособности ИСПДн МАДОУ «Центр развития ребенка – детский сад «Сказка» г. Белоярский» (далее - МАДОУ).

Целью настоящего документа является превентивная защита элементов ИСПДн от предотвращения потери защищаемой информации.

Задачей данной Инструкции является: определение мер защиты от потери информации; определение действий восстановления в случае потери информации. Действие настоящей Инструкции распространяется на всех пользователей МАДОУ, имеющих доступ к ресурсам ИСПДн, а также основные системы обеспечения непрерывности работы и восстановления ресурсов при возникновении аварийных ситуаций, в том числе:

- системы жизнеобеспечения;
- системы обеспечения отказоустойчивости;
- системы резервного копирования и хранения данных;
- системы контроля физического доступа.

Пересмотр настоящего документа осуществляется по мере необходимости, но не реже раза в два года. Ответственным сотрудником за реагирование на инциденты безопасности, приводящие к потере защищаемой информации, назначается Ответственный за обработку ИСПДн МАДОУ.

2.Порядок реагирования на инцидент.

В настоящем документе под Инцидентом понимается некоторое происшествие, связанное со сбоем в функционировании элементов ИСПДн, предоставляемых пользователям ИСПДн, а также потерей защищаемой информации. Происшествие, вызывающее инцидент, может произойти:

- В результате непреднамеренных действий пользователей.

- В результате преднамеренных действий пользователей и третьих лиц.

- В результате нарушения правил эксплуатации технических средств ИСПДн.

- В результате возникновения внештатных ситуаций и обстоятельств непреодолимой силы.

Все действия в процессе реагирования на Инцидент должны документироваться ответственным за реагирование сотрудником в «Журнале по учету мероприятий по контролю». В кратчайшие сроки, не превышающие одного рабочего дня, ответственные за реагирование сотрудники МАДОУ (Ответственный за обработку ПД, Операторы ИСПДн), предпринимают меры по восстановлению работоспособности. Предпринимаемые меры по возможности согласуются с вышестоящим руководством. Меры обеспечения непрерывности работы и восстановления ресурсов при возникновении инцидентов

2.1. Технические меры

К техническим мерам обеспечения непрерывной работы и восстановления относятся программные, аппаратные и технические средства и системы, используемые для предотвращения возникновения Инцидентов, такие как:

- системы жизнеобеспечения;

- системы обеспечения отказоустойчивости;

- системы резервного копирования и хранения данных; системы контроля физического доступа.

Системы жизнеобеспечения ИСПДн включают: пожарные сигнализации и системы пожаротушения; системы вентиляции и кондиционирования; системы резервного питания. Все критичные помещения МАДОУ (помещения, в которых размещаются элементы ИСПДн и средства защиты) должны быть оборудованы средствами пожарной сигнализации и пожаротушения. Для выполнения требований по эксплуатации (температура, относительная влажность воздуха) программно-аппаратных средств ИСПДн в помещениях, где они установлены, должны применяться системы вентиляции и по возможности, кондиционирования воздуха. Для предотвращения потерь информации при кратковременном отключении электроэнергии все ключевые элементы ИСПДн, сетевое и коммуникационное оборудование, а также наиболее критичные рабочие станции должны подключаться к сети электропитания через источники бесперебойного питания. В зависимости от необходимого времени работы ресурсов после потери питания могут применяться следующие методы резервного электропитания:

- локальные источники бесперебойного электропитания с различным временем питания для защиты отдельных компьютеров;

- источники бесперебойного питания с дополнительной функцией защиты от скачков напряжения;

- дублированные системы электропитания в устройствах (серверы, концентраторы, мосты и т. д.);

- резервные линии электропитания в пределах комплекса зданий; аварийные электрогенераторы.

Системы обеспечения отказоустойчивости:

- кластеризация;

- технология RAID.

Для обеспечения отказоустойчивости критичных компонентов ИСПДн при сбое в работе оборудования и их автоматической замены без простоев должны использоваться методы кластеризации. Могут использоваться следующие методы кластеризации: для наиболее критичных компонентов ИСПДн должны использоваться территориально удаленные системы кластеров. Для защиты от отказов отдельных дисков серверов, осуществляющих обработку и хранение защищаемой информации, должны использоваться технологии RAID, которые (кроме RAID-O) применяют дублирование данных, хранимых на дисках. Система резервного копирования и хранения данных, должна обеспечивать хранение защищаемой информации на твердый носитель (ленту, жесткий диск и т.п.).

2.2. Организационные меры. Резервное копирование и хранение данных должно осуществлять на периодической основе:

- для обрабатываемых персональных данных - не реже раза в год;

- для технологической информации - не реже раза в полгода;

эталонные копии программного обеспечения (операционные системы, штатное и специальное программное обеспечение, программные средства защиты), с которых осуществляется их установка на элементы ИСПДн - не реже раза в месяц, и каждый раз при внесении изменений в эталонные копии (выход новых версий). Носители, на которые произведено резервное копирование, должны быть пронумерованы: номером носителя, датой проведения резервного копирования. Носители должны храниться у ответственного лица (делопроизводитель). Носители должны храниться не менее года, для возможности восстановления данных.

3.Ответственность.

Ответственность за поддержание установленного в настоящей Инструкции порядка проведения резервирования и восстановления работоспособности технических средств и

программного обеспечения, баз данных и средств защиты информации в информационных системах персональных данных возлагается на Ответственного за обработку персональных данных.