муниципальное казенное дошкольное образовательное учреждение
«Детский сад комбинированного вида №20»
(МКДОУ «Детский сад №20»)

ПРИКАЗ

06.10.2020 № 83/1-о

Новомосковск

Об утверждении Политики в
отношении обработки персональных
данных, положений

В соответствии с п. 2 ч. 1, ч. 2 ст. 18.1. Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», на основании ст. 6.7 Устава МКДОУ «Детский сад №20»,

ПРИКАЗЫВАЮ:

1. Утвердить положения по персональным данным:

- Политику МКДОУ «Детский сад №20» в отношении обработки персональных данных (Приложение№1);
- положение о порядке организации и проведения работ по защите конфиденциальной информации в МКДОУ «Детский сад № 20»; (Приложение№2);
- инструкция по антивирусной защите в информационных системах МКДОУ «Детский сад № 20» (Приложение№3);
- инструкция по организации парольной защиты в информационных системах МКДОУ «Детский сад № 20» (Приложение№4);
- инструкция по обработке персональных данных, осуществляемой без использования средств автоматизации в МКДОУ «Детский сад № 20»;
- регламент резервного копирования и восстановления информации в МКДОУ «Детский сад № 20» (Приложение№5);
- инструкция пользователя информационных систем МКДОУ «Детский сад № 20» (Приложение№6).

2. Опубликовать Политику МКДОУ «Детский сад №20» в отношении обработки персональных данных» на официальном сайте организации в течение 10 дней с момента утверждения.

3. Приказ вступает в силу со дня подписания.

Контроль над исполнением настоящего приказа оставляю за собой.

Заведующий Е.И.Аппоротова

Приложение №1
к Приказу МКДОУ «Детский сад №20»
от 06.10.2020. № 83/1-о

Политика муниципального казенного дошкольного образовательного учреждения «Детский сад комбинированного вида №20» в отношении обработки персональных данных

1. Общие положения

1.1. Настоящая Политика Муниципального казенного дошкольного образовательного учреждения «Детский сад комбинированного вида №20» в отношении обработки персональных данных (далее - Политика) разработана в соответствии с требованиями Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных».

1.2. Политика определяет цели, принципы обработки и реализуемые требования к защите персональных данных в Муниципальном казенное дошкольном образовательном учреждении «Детский сад комбинированного вида №20» (далее организация). Персональные данные являются информацией ограниченного доступа и подлежат защите в соответствии с законодательством Российской Федерации.

2. Основные понятия

2.1. В настоящей Политике используются следующие основные понятия:

2.1.1. Субъектами персональных данных организации являются:

- работники организации;
- студенты, проходящие практику в организации;
- клиенты (контрагенты) организации;
- лица, состоящие в договорных или иных отношениях с организации.

Персональные данные - любая информация, относящаяся к прямо или косвенно определенному, или определяемому физическому лицу (субъекту персональных данных).

2.1.2. Обработка персональных данных - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

2.1.3. Конфиденциальность персональных данных – обязанность оператора и иных лиц, получивших доступ к персональным данным, не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.

2. Принципы и цели обработки персональных данных

3.1. Организация в своей деятельности по обработке персональных данных руководствуется следующими принципами:

3.1.1. Обработка персональных данных осуществляется на законной и справедливой основе.

3.1.2. Цели обработки персональных данных соответствуют полномочиям организации.

3.1.3. Содержание и объем обрабатываемых персональных данных соответствуют целям обработки персональных данных.

3.1.4. Достоверность персональных данных, их актуальность и достаточность для целей обработки, недопустимость обработки избыточных по отношению к целям сбора персональных данных.

3.1.5. Ограничение обработки персональных данных при достижении конкретных и законных целей, запрет обработки персональных данных, несовместимых с целями сбора персональных данных.

3.1.6. Запрет объединения баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой.

3.1.7. Осуществление хранения персональных данных в форме, позволяющей определить субъекта персональных данных, не дольше, чем это требуют цели обработки персональных данных, если срок хранения персональных данных не установлен действующим законодательством.

3.1.8. Обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижению целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено действующим законодательством.

3.2. Обработка персональных данных работников организации осуществляется в целях обеспечения соблюдения Конституции Российской Федерации, федеральных законов и иных нормативных правовых актов Российской Федерации, заключения и исполнения трудовых договоров, ведения воинского учета, исполнения требований по охране труда.

3.3. Обработка персональных данных граждан, не являющихся работниками организации, осуществляется с целью реализации полномочий организации в соответствии с Уставом, а также с целью отбора претендентов на замещение вакантных должностей организации.

3. Перечень мер по обеспечению безопасности персональных данных при их обработке

4.1. Организация при обработке персональных данных принимает все необходимые правовые, организационные и технические меры для их защиты от неправомерного или случайного доступа, уничтожения, изменения, блокирования, копирования, предоставления, распространения, а также иных неправомерных действий в отношении них. Обеспечение безопасности персональных данных достигается, в частности, следующими способами:

4.1.1. Назначением ответственного за организацию обработки персональных данных.

4.1.2. Утверждением локальных актов по вопросам обработки персональных данных, а также локальных актов, устанавливающих процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений.

4.1.3. Осуществлением внутреннего контроля соответствия обработки персональных данных Федеральному закону от 27.07.2006 №152-ФЗ "О персональных данных" и принятыми в соответствии с ним нормативными правовыми актами, требованиям к защите персональных данных.

4.1.4. Ознакомлением работников организации, непосредственно осуществляющих обработку персональных данных, с требованиями законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных, локальными актами в отношении обработки персональных данных, и обучением указанных работников.

4.1.5. Выполнением требований, установленных постановлением Правительства Российской Федерации от 15 сентября 2008 года № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» при обработке персональных данных, осуществляемой без использования средств автоматизации.

4.1.6. Применением прошедших в установленном порядке процедуру оценки соответствия средств защиты информации.

4.1.7. Учетом машинных носителей персональных данных.

4.1.8. Выявлением фактов несанкционированного доступа к персональным данным и принятием мер.

4.1.9. Восстановлением персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним.

4.1.10. Установлением правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечением регистрации и учета всех действий, совершаемых в информационной системе персональных данных.

4.2. Работники организации, виновные в нарушении порядка обращения с персональными данными, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с законодательством Российской Федерации.

Заведующий Е.И.Аппоротова

Приложение №2
к Приказу МКДОУ «Детский сад
№20»
от 06.10.2020. № 83/1-о

Положение
о порядке организации и проведения работ по защите конфиденциальной информации в МКДОУ «Детский сад № 20»

I. Общие положения

1. Настоящее Положение устанавливает порядок организации и проведения работ по защите конфиденциальной информации в Муниципальном казенном дошкольном образовательном учреждении «Детский сад комбинированного вида №20» (далее – Учреждение).

2. Действие настоящего Положения не распространяется на правоотношения, связанные с обращением со сведениями, составляющими государственную тайну.

3. В настоящем Положении под конфиденциальной информацией (информацией конфиденциального характера, сведениями конфиденциального характера) понимается информация ограниченного доступа, свободный доступ к которой ограничен в соответствии с федеральным законодательством, а также служебная информация, доступ к которой ограничен обладателем информации.

4. В настоящем Положении используются основные понятия в значении, определенном Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», а также следующие понятия:

автоматизированная система (АС) – система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций;

допуск к конфиденциальной информации – процедура оформления права граждан на доступ к сведениям конфиденциального характера;

защищаемые помещения (ЗП) – помещения (кабинеты, актовые, конференц-залы и т.д.), специально предназначенные для проведения конфиденциальных мероприятий (совещаний, конференций, переговоров и т.п.), связанных с обсуждением и (или) оглашением информации конфиденциального характера;

контролируемая зона (КЗ) – пространство (территория, здание, помещение или их часть), в котором исключено неконтролируемое пребывание лиц, не имеющих допуска, а также транспортных, технических и иных материальных средств;

несанкционированный доступ (несанкционированные действия) – доступ к информации или действия с информацией, осуществляемые с

нарушением установленных прав и (или) правил доступа к информации или действий с ней с применением штатных средств информационной системы или средств, аналогичных им по функциональному предназначению и техническим характеристикам;

носитель информации – физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин;

перехват (информации) – неправомерное получение информации с использованием технического средства, осуществляющего обнаружение, прием и обработку информационных сигналов;

ресурс информационной системы – именованный элемент системного, прикладного или аппаратного обеспечения функционирования информационной системы;

служебная информация ограниченного распространения – информация, касающаяся деятельности Учреждения, ограничение на распространение которой диктуются служебной необходимостью;

средство защиты информации (СЗИ) – техническое, программное, программно- техническое средство, предназначенное (используемое) для защиты информации;

утечка (защищаемой) информации по техническим каналам – неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации.

5. Защита конфиденциальной информации осуществляется на основании действующего законодательства Российской Федерации.

6. Доступ к сведениям конфиденциального характера Учреждение, в том числе содержащимся в информационных системах, может быть предоставлен с согласия обладателя информации и (или) в случаях, установленных законодательством.

7. В Учреждении осуществляется разрешение или ограничение доступа к информации, определяется порядок и условия такого доступа.

8. Сведения конфиденциального характера, в том числе служебную информацию, ставшие известными работнику вследствие выполнения должностных обязанностей, запрещается использовать в личных целях и в целях причинения имущественного ущерба, морального вреда.

II. Принципы ограничения доступа к сведениям

9. Основными принципами ограничения доступа являются законность, обоснованность и своевременность.

10. Законность ограничения доступа заключается в выполнении требований законодательства при отнесении сведений к категории конфиденциальной информации. При этом учитываются как нормы, предписывающие налагать ограничения на доступ к этим сведениям, так и

запрещающие такие ограничения.

11. Обоснованность ограничения доступа заключается в установлении путем экспертной оценки целесообразности ограничения доступа, вероятных последствий этого акта, исходя из законных интересов Учреждения.

12. Своевременность ограничения доступа заключается в установлении ограничений на разглашение и (или) распространение сведений с момента их получения (разработки) или заблаговременно.

III. Порядок отнесения сведений к категории конфиденциальной информации

13. Решение об отнесении сведений к категории конфиденциальной информации принимает руководитель Учреждения путем утверждения перечня сведений конфиденциального характера (далее – Перечень сведений).

14. Для включения в Перечень сведений осуществляется анализ информации, содержащейся в утверждаемых руководителем документах, документах текущей деятельности (информационных потоках), обрабатываемых как в интересах обладателя информации, так и в интересах других лиц.

15. С целью обеспечения принципа обоснованности рассматривается возможный ущерб, который может быть нанесен государству, Учреждению, иным лицам в результате разглашения или распространения конфиденциальной информации, с затратами, необходимыми на ограничение доступа к ней.

16. Возможный ущерб оценивается исходя из наличия материальных, финансовых, репутационных и иных рисков или морального вреда в результате несанкционированного разглашения или распространения конфиденциальной информации.

17. При определении размера (степени) ущерба прогнозируются возможные потери и риски, возникающие не только в настоящее время, но и те, которые могут возникнуть в будущем.

18. При рассмотрении вопросов отнесения сведений к категории конфиденциальной информации учитываются следующие отрицательные факторы разглашения конфиденциальной информации:

нарушение федеральных законов и иных нормативных правовых актов по ограничению доступа к информации;

разрыв отношений (или их осложнение) с деловыми партнерами, юридическими и физическими лицами по причине разглашения сведений;

срыв или невыполнение договорных обязательств, контрактов; создание трудностей при взаимодействии;

экономические, судебные и иные санкции со стороны юридических и физических лиц за незаконное разглашение сведений о них;

потеря, блокирование или искажение информации в базах данных; несанкционированная передача баз данных или их части; раскрытие действующей

системы защиты информации.

19. Информация, полученная в результате взаимодействия Учреждения с контрагентами в процессе хозяйственной деятельности, может быть отнесена к категории конфиденциальной положениями заключаемых договоров, соглашений, в которых также отражаются взаимные обязательства и ответственность сторон за сохранность этой информации.

Такая информация в Перечень сведений не включается.

IV. Обязанности по защите конфиденциальной информации и ответственность

20. В Учреждении назначается лица, ответственные:

за организацию обработки персональных данных;

за обеспечение безопасности конфиденциальной информации (в том числе персональных данных), администратор безопасности.

21. Указанные в пункте 20 ответственные лица в пределах своей компетенции организуют:

контролируемый допуск работников Учреждения к информации конфиденциального характера;

учет, хранение и уничтожение документов и машинных носителей с конфиденциальной информации;

обработку конфиденциальной информации с помощью средств вычислительной техники;

выполнение мероприятий по защите конфиденциальной информации;

контроль соблюдения порядка работы с конфиденциальной информацией.

22. Не допускается хранение и обработка конфиденциальной информации на территории иностранных государств, если иное не предусмотрено действующими международными соглашениями Российской Федерации.

23. Доступ к конфиденциальной информации осуществляется в соответствии с разрешительной системой доступа (матрицей доступа), утверждаемой руководителем Учреждения.

24. За разглашение конфиденциальной информации, а также нарушение порядка обращения с ней, работник Учреждения может быть привлечен к дисциплинарной и (или) иной ответственности, предусмотренной действующим законодательством.

25. Не реже одного раза в год в Учреждении осуществляется контроль (аудит) соблюдения порядка работы с конфиденциальной информацией.

V. Порядок обмена конфиденциальной информации

26. Предоставление (передача) конфиденциальной информации может производиться только на основании решения руководителя Учреждения при условии соблюдения требований по защите информации.

27. Информация конфиденциального характера предоставляется органам государственной власти, государственным учреждениям и органам местного самоуправления Тульской области на безвозмездной основе.

28. Предоставление конфиденциальной информации иным лицам, если иное не установлено законодательством, регулируется заключаемыми договорами, устанавливающими права, обязанности и ответственность сторон, перечень предоставляемых конфиденциальных сведений и компенсацию за разглашение и иное распространение указанных сведений.

29. При направлении сторонним организациям (учреждениям, предприятиям) сведений и документов, содержащих конфиденциальную информацию, в сопроводительном письме необходимо уведомлять (информировать) получателя о законном требовании соблюдения конфиденциальности полученной им информации и ответственности за ее разглашение или распространение. При обмене конфиденциальной информацией между органами власти, учреждениями делать указанное уведомление не обязательно.

30. Передача конфиденциальной информации в электронном виде разрешается только по защищенным каналам связи, оборудованным сертифицированными средствами защиты.

31. Не допускается речевая передача конфиденциальной информации по открытым проводным каналам связи, выходящим за пределы КЗ, и радиоканалам. При необходимости передачи конфиденциальной информации следует использовать защищенные линии связи.

32. Проведение конфиденциальных мероприятий (в том числе совещаний, комиссий,собраний, обсуждений и т. п.) разрешается только в ЗП, исключающих возможность перехвата речевой информации конфиденциального характера.

33. При необходимости ЗП оборудуются сертифицированными средствами защиты информации. ЗП должны быть аттестованы по требованиям безопасности информации и размещаться в пределах контролируемой зоны органа власти.

34. В Учреждении в соответствии с установленными требованиями по защите информации определяется перечень ЗП и лиц, ответственных за их эксплуатацию.

35. Во время проведения конфиденциальных мероприятий запрещается использование в ЗП радиотелефонов, устройств сотовой, пейджинговой и транкинговой связи.

VI. Организация и проведение работ по защитеконфиденциальной информации

36. Проведение работ по защите конфиденциальной информации осуществляется путем: выполнения комплекса мероприятий (правовых, организационных, технических),

направленных на предотвращение утечки информации (в том числе по техническим каналам), несанкционированного доступа к ней, преднамеренных программно-технических воздействий с целью разрушения (уничтожения) или искажения информации в процессе обработки, передачии хранения;

проведения специальных работ, порядок организации и выполнения которых определяется Правительством Российской Федерации и федеральными органами

исполнительной власти, уполномоченными в области обеспечения безопасности, противодействия техническим разведкам и технической защиты информации, в пределах их полномочий.

37. Организация мероприятий по защите конфиденциальной информации возлагается на ответственных лиц, указанных в пункте 20 настоящего Положения.

38. Обработка конфиденциальной информации допускается только на АС Учреждения, оснащенных сертифицированными по требованию законодательства программными, техническими и программно-техническими средствами защиты информации.

39. АС обработки такой информации должны быть аттестованы по требованиям безопасности информации, а применяемое в них программное обеспечение должно быть лицензионным.

40. При обработке конфиденциальной информации с использованием АС необходимо неукоснительно выполнять требования утвержденных руководителем Учреждения локальных актов, регламентирующих:

антивирусную защиту информации; использование программного обеспечения; применение машинных носителей информации; организацию сетевой защиты информации; авторизацию пользователей;

иные аспекты защиты информации.

Заведующий Е.И.Аппоротова

Приложение №3
к Приказу МКДОУ «Детский сад №20»
от 06.10.2020. № 83/1-о

ИНСТРУКЦИЯ
по антивирусной защите в информационных системах

1. Настоящая инструкция предназначена для ответственного за обеспечение безопасности персональных данных в информационных системах Муниципального казенного дошкольного образовательного учреждения «Детский сад комбинированного вида №20» (далее – Ответственный) и пользователей, обрабатывающих персональные данные на автоматизированных рабочих местах (далее АРМ) информационных систем Муниципального казенного дошкольного образовательного учреждения «Детский сад комбинированного вида №20» (далее организация).
2. В целях обеспечения антивирусной защиты на АРМ производится антивирусный контроль.
3. Ответственность за поддержание установленного в настоящей инструкции порядка проведения антивирусного контроля возлагается на ответственного за обеспечение безопасности персональных данных в информационных системах организации.
4. К применению на АРМ допускаются только лицензионные и сертифицированные ФСТЭК России антивирусные средства.
5. На АРМ запрещается установка программного обеспечения, не связанного с выполнением функций организации.
6. Пользователи АРМ при работе с носителями информации обязаны перед началом работы осуществить проверку их на предмет отсутствия компьютерных вирусов.
7. Обновление антивирусных баз осуществляется ежедневно путем настройки в антивирусном средстве доступа к серверам обновлений разработчика антивирусного средства. В случае невозможности настроить доступ к серверам обновлений разработчика антивирусного средства, Ответственный один раз в неделю осуществляет установку пакетов обновлений антивирусных баз, осуществляет контроль их подключения к антивирусному программному обеспечению и проверку жесткого диска и съемных носителей на наличие вирусов.
8. При обнаружении компьютерного вируса пользователи обязаны немедленно поставить в известность Ответственного и прекратить какие-либо действия на АРМ.
9. Ответственный проводит расследование факта заражения АРМ компьютерным вирусом. «Лечение» зараженных файлов осуществляется путем

выбора соответствующего пункта меню антивирусной программы и после этого вновь проводится антивирусный контроль.

10. В случае обнаружения вируса, не поддающегося лечению, Ответственный обязан удалить инфицированный файл в соответствующую папку антивирусного пакета, и проверить работоспособность АРМ. В случае отказа АРМ – произвести восстановление соответствующего программного обеспечения.

11. Обо всех фактах заражения АРМ, Ответственный обязан ставить в известность ответственного за организацию обработки персональных данных и своего непосредственного руководителя.

Заведующий Е.И.Аппоротова

Приложение №4
к Приказу МКДОУ «Детский сад
№20»
от 06.10.2020. № 83/1-о

Инструкция
по организации парольной защиты в информационных системах МКДОУ «Детский сад № 20»

1. Общие положения

1.1 Инструкция по организации парольной защиты (далее – Инструкция) регламентирует организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей (удаления учетных записей пользователей) в информационных системах дошкольного образовательного учреждения (далее - ДОУ), а также контроль за действиями пользователей и обслуживающего персонала системы при работе с паролями.

1.2. Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей во всех подсистемах информационной системы (далее - ИС) ДОУ и контроль за действиями исполнителей и обслуживающего персонала при работе с паролями возлагается на администратора безопасности ДОУ.

2. Правила формирования паролей

2.1. Личные пароли выбираются пользователями информационной системы самостоятельно с учетом следующих требований:

- пароль должен состоять не менее чем из восьми символов;
- в пароле обязательно должны присутствовать буквы из верхнего и нижнего регистров, цифры и специальные символы (©,#,$,&, *, % и т. п.);
- пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, известные названия, словарные и жаргонные слова и т. д.), последовательности символов и знаков (111, qwerty, abed и т. д.),

общепринятые сокращения (ЭВМ, ЛВС, USER и т. п.), аббревиатуры, клички домашних животных, номера автомобилей, телефонов и другие значимые сочетания букв и знаков, которые можно угадать, основываясь на информации о пользователе;

- при смене пароля новый пароль должен отличаться от старого не менее чем в шести позициях.

2.2. При технологической необходимости использования имен и паролей некоторых работников (исполнителей) в их отсутствие (в случае возникновения нештатных ситуаций, форс-мажорных обстоятельств и т. п.) такие работники

обязаны сразу же после смены своих паролей их новые значения (вместе с именами своих учетных записей) передать на хранение руководителю.

3. Ввод пароля

3.1. При вводе пароля пользователю необходимо исключить произнесение его вслух, возможность его подсматривания посторонними лицами.

4. Порядок смены личных паролей

4.1. Смена паролей проводится регулярно, не реже одного раза в год.

4.2. В случае прекращения полномочий пользователя (увольнение, переход на другую работу и т. п.) администратор безопасности должен немедленно удалить его учетную запись сразу после окончания последнего сеанса работы данного пользователя с системой.

4.3. Срочная (внеплановая) полная смена паролей производится в случае прекращения полномочий (увольнение, переход на другую работу и т. п.) администраторов информационной системы и других работников, которым по роду работы были предоставлены полномочия по управлению системой парольной защиты.

4.4. Смена пароля производится самостоятельно каждым пользователем в соответствии с п. 2.1 Инструкции.

5. Хранение пароля

5.1. Хранение пользователем своего пароля на бумажном носителе сейфе у руководителя.

5.2. Запрещается записывать пароли на бумаге, в файле, электронной записной книжке и других носителях информации.

5.3. Запрещается сообщать другим пользователям личный пароль и регистрировать их в системе под своим паролем.

Заведующий Е.И.Аппоротова

Приложение №5
к Приказу МКДОУ «Детский сад
№20»
от 06.10.2020. № 83/1-о

ИНСТРУКЦИЯ
по обработке персональных данных, осуществляемой без использования средств автоматизации в МКДОУ «Детский сад № 20»

I. Общие положения

1. Настоящая инструкция по обработке персональных данных, осуществляемой без использования средств автоматизации, в Муниципальном казенном дошкольном образовательном учреждении «Детский сад комбинированного вида №20» (далее - Инструкция) устанавливают порядок обработки персональных данных, осуществляемой без использования средств автоматизации, а также порядок заполнения типовых форм документов Муниципальном казенном дошкольном образовательном учреждении «Детский сад комбинированного вида №20» (далее – Учреждение), характер информации в которых предполагает или допускает включение в них персональных данных (далее - типовая форма).

2. Основные понятия, используемые в настоящих Правилах, соответствуют основным понятиям, установленным Федеральным законом от 27 июля 2006 № 152-ФЗ «О персональных данных».

II. Особенности организации обработки персональных данных, осуществляемой безиспользования средств автоматизации

3. При фиксации персональных данных на материальных носителях не допускается фиксация на одном материальном носителе персональных данных, цели обработки которых заведомо не совместимы.

4. Работники Учреждения, осуществляющие обработку персональных данных без использования средств автоматизации, а также лица, осуществляющие такую обработку по договору с Учреждением, информируются о факте обработки ими персональных данных, обработка которых осуществляется без использования средств автоматизации, категориях обрабатываемых персональных данных, а также об особенностях и правилах осуществления такой обработки, установленных нормативными правовыми актами федеральных органов исполнительной власти, органов исполнительной

власти Тульской области, а также локальными правовыми актами Учреждения. По факту информирования указанные лица подписывают обязательства о неразглашении персональных данных.

5. При хранении материальных носителей персональных данных, обрабатываемых без использования средств автоматизации, с целью соблюдения условий, обеспечивающих сохранность персональных данных и исключающих несанкционированный к ним доступ, применяются следующие меры:

5.1. Хранение материальных носителей персональных данных, обрабатываемых без использования средств автоматизации, осуществляется в местах, установленных локальными актами Учреждения.

5.2. Обеспечивается раздельное хранение персональных данных, обработка которых осуществляется в несовместимых целях.

5.3. Руководитель Учреждения устанавливает перечень лиц, осуществляющих обработку персональных данных либо имеющих к ним доступ.

6. Работник Учреждения, ответственный за организацию обработки персональных данных, совместно с администратором безопасности контролирует реализацию мер, указанных в п.п. 5.1.-5.3. Инструкции, а также порядок их принятия.

III. Порядок заполнения типовых форм

7. Учреждение является оператором, осуществляющим обработку персональных данных, адрес: Тульская область, г. Новомосковск, ул. Садовского д.17.

Целями обработки персональных данных является осуществление деятельности, реализация полномочий Учреждения, в том числе кадровый учет, исполнение трудовых договоров, рассмотрение кандидатур на замещение вакантных должностей, антикоррупционная деятельность, воинский учет, публикация информации о деятельности Учреждения.

Источником получения персональных данных, обрабатываемых без использования средств автоматизации, является непосредственно субъект персональных данных, либо его официальный представитель.

Сроки обработки персональных данных устанавливаются локальными актами Учреждения.

Персональные данные обрабатываются смешанным образом. Перечень действий с персональными данными, обрабатываемыми без использования средств автоматизации: сбор, запись, систематизация, накопление, хранение, уточнение (обновление, изменение), использование, удаление, уничтожение персональных данных.

Заведующий Е.И.Аппоротова

Приложение №6
к Приказу МКДОУ «Детский сад
№20»
от 06.10.2020. № 83/1-о

Регламент резервного копирования и восстановления информации в МКДОУ «Детский сад № 20»

1. Общие положения

1.1. Настоящий регламент муниципального казенного дошкольного образовательного учреждения «Детский сад комбинированного вида №20» (далее ОО) разработан в соответствии с требованиями приказа ФСТЭК России «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» от 18.02.2013г. №21.

2. Термины и определения

2.1. Информационная система персональных данных (ИСПДн) - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств *(ст. 3 ФЗ РФ от 27.07.2006 г. N 152-ФЗ «О персональных данных»)*.

2.2. Резервное копирование - процесс создания копии данных на носителе (дисковом массиве, магнитной ленте и т. д.), предназначенном для восстановления данных в оригинальном месте их расположения в случае их повреждения или разрушения.

2.3. Система резервного копирования - совокупность программного и аппаратного обеспечения, выполняющая задачу резервного копирования информации.

3. Порядок резервного копирования

3.1. Резервному копированию подлежит информация следующих основных категорий:

- базы данных, содержащие персональные данные субъектов.

3.2. Система резервного копирования должна обеспечивать производительность, достаточную для сохранения информации, в установленные сроки – 1 раз в месяц.

3.3. Копии хранятся на съемном носителе.

4. Контроль результатов резервного копирования

4.1. Контроль результатов всех процедур резервного копирования осуществляетсяадминистратором безопасности ИСПДн.

5. Восстановление информации из резервной копии

5.1. В случае необходимости, восстановление данных из резервных копий производится на основании заявки пользователя ИСПДн в течении 1 (Одного) рабочего дня.

5.2. Любое восстановление информации выполняется на основании заявки пользователя администратору безопасности ИСПДн или в случае необходимости восстановления утерянной или повреждённой информации, подлежащей резервированию. В процессе восстановления резервной копии следует руководствоваться инструкциями по восстановлению информации из резервных копий, описанных в документации, прилагающейся к системе резервного копирования ПО, входящее в ОС Windows.

Заведующий Е.И.Аппоротова

Приложение №7
к Приказу МКДОУ «Детский сад №20»
от 06.10.2020. № 83/1-о

Инструкция пользователя информационных систем МКДОУ «Детский сад № 20»

1. Общие положения

1.1. Пользователь информационных систем персональных данных (ИСПДн) (далее – Пользователь) осуществляет обработку персональных данных в информационной системе персональных данных.

1.2. Пользователем является каждый сотрудник муниципального казенного дошкольного образовательного учреждения «Детский сад№20» (далее — учреждение) участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки информации и имеющий доступ к аппаратным средствам, программному обеспечению, данным и средствам защиты.

1.3. Пользователь несёт персональную ответственность за свои действия.

1.4. Пользователь в своей работе руководствуется настоящей инструкцией и регламентирующими документами учреждения. Руководство работой пользователя осуществляется ответственным за обеспечение защиты персональных данных.

2. Обязанности пользователя

Пользователь обязан:

2.1. Знать и выполнять требования действующих нормативных и руководящих документов, а также внутренних инструкций, руководства по защите информации и распоряжений, регламентирующих порядок действий по защите информации.

2.2. Выполнять на автоматизированном рабочем месте (АРМ) только те процедуры, которые определены для него в должностной инструкции.

2.3. Знать и соблюдать установленные требования по режиму обработки персональных данных, учету, хранению и пересылке носителей информации, обеспечению безопасности ПДн, а также руководящих и организационно-распорядительных документов.

2.4. Соблюдать требования парольной политики.

2.5. Соблюдать правила при работе в сетях общего доступа и (или) международного обмена – Интернет и других.

2.6. Экран монитора в помещении располагать во время работы так, чтобы исключалась возможность несанкционированного ознакомления с отображаемой на них информацией посторонними лицами, шторы на оконных проемах должны быть завешаны (жалюзи закрыты).

2.7. Обо всех выявленных нарушениях, связанных с информационной безопасностью, а так же для получения консультаций по вопросам информационной безопасности, необходимо обратиться к ответственному за обеспечение защиты ПД.

2.8. Для получения консультаций по вопросам работы и настройке элементов ИСПДн необходимо обращаться к руководителю учреждением.

2.9. Пользователям запрещается: разглашать защищаемую информацию третьим лицам; копировать защищаемую информацию на внешние носители без разрешения своего руководителя; самостоятельно устанавливать, тиражировать, или модифицировать программное обеспечение и аппаратное обеспечение, изменять установленный алгоритм функционирования технических и программных средств; несанкционированно открывать общий доступ к папкам на своей рабочей станции; запрещено подключать к рабочей станции и корпоративной информационной сети личные внешние носители и мобильные устройства;

отключать (блокировать) средства защиты информации;

обрабатывать на АРМ информацию и выполнять другие работы, неи предусмотренные перечнем прав пользователя по доступу к ИСПДн;

сообщать (или передавать) посторонним лицам личные ключи и атрибуты доступа к ресурсам ИСПДн;

привлекать посторонних лиц для производства ремонта или настройки АРМ, без согласования с ответственным за обеспечение

защиты персональных данных.

Принимать меры по реагированию, в случае возникновения внештатных ситуаций и аварийных ситуаций, с целью ликвидации их последствий, в пределах возложенных на него функций.

3. Правила работы в сетях общего доступа

3.1. Работа в сетях общего доступа (сети Интернет и других) (далее – Сеть) на элементах ИСПДн, должна проводиться при служебной необходимости.

3.2. При работе в Сети запрещается:

осуществлять работу при отключённых средствах защиты (антивирус и других);

передавать по Сети защищаемую информацию без использования средств шифрования;

запрещается скачивать из Сети программное обеспечение и другие файлы;

запрещается посещение сайтов сомнительной репутации (порно-сайты, сайты, содержащие нелегально распространяемое ПО и другие);

запрещается нецелевое использование подключения к Сети.

4. Права и ответственность пользователей ИСПДн

4.1 Пользователь имеет право в отведанное ему время решать поставленные задачи в соответствии с полномочиями доступа к ресурсам ИСПДн.

4.2 Пользователи, виновные в несоблюдении Настоящей инструкции расцениваются как нарушители Федерального закона РФ 27.07.2006 г. N 152-ФЗ «О персональных данных» и несут гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность.

Заведующий Е.И.Аппоротова

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 5AC42D0AD211267E71CAC7AEBAE330EDA5A25DE4
Владелец: Аппоротова Елена Ивановна
Действителен: с 19.11.2020 до 19.02.2022