**Муниципальное бюджетное дошкольное образовательное учреждение**
**«Детский сад комбинированного вида №18»**
**(МБДОУ «ДСКВ № 18)**

СОГЛАСОВАНО:
Председатель ПК МБДОУ «ДСКВ №18»
_____ /Т.А.Мандрыкина/

УТВЕРЖДАЮ:
Заведующий МБДОУ «ДСКВ №18»
_____/Г.И.Селиванова/
Приказ № 66од от 16.06.2021г.

ПРИНЯТО:
На общем собрании трудового коллектива
протокол № 4 от 15.06.2021г.

Селиванова Галина Ивановна

Подписано цифровой подписью: Селиванова Галина Ивановна
Дата: 2021.09.30 11:14:02 +03'00'

# Положение
# об обработке и защите персональных данных в информационных системах МБДОУ «Детский сад комбинированного вида №18»

## 1. Общие положения

1.1. Настоящее «Положение об обработке и защите персональных данных в информационных системах МБДОУ «Детский сад комбинированного вида №18» (далее – Положение) разработано в соответствии с Законом Российской Федерации от 27 июля 2006 года №152-ФЗ «О персональных данных», Постановлением Правительства Российской Федерации от 17 ноября 2007 года № 781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных», методическими рекомендациями ФСТЭК России и ФСБ России.

1.2. Положение разработано в целях обеспечения безопасности персональных данных (далее – ПДн) при их обработке в информационных системах персональных данных МБДОУ (далее – ИСПДн).

1.3. Положение определяет порядок работы коллектива МБДОУ «ДСКВ №18» (далее – ДОУ) в ИСПДн в части обеспечения безопасности ПДн при их обработке, порядок использования средств защиты информации, разработку и принятие мер по предотвращению возможных опасных последствий таких нарушений, порядок приостановки предоставления ПДн в случае обнаружения нарушений при их обработке, порядок обучения коллектива ОУ практике работы в ИСПДн, порядок контроля соблюдения условий использования средств защиты информации, предусмотренные эксплуатационной и технической документацией, правила обновления общесистемного и прикладного программного обеспечения, правила организации антивирусной защиты и парольной защиты ИСПДн, порядок охраны и допуска посторонних лиц в защищаемые помещения.

## 2. Порядок предоставления допуска пользователей к работе в ИСПДн

2.1. Настоящий порядок определяет действия коллектива ДОУ в ИСПДн в части обеспечения безопасности ПДн при их обработке в ИСПДн.

2.2. Первоначальный допуск пользователей к работе в ИСПДн осуществляется на основании приказа, который издается заведующим ДОУ (далее - Заведующий). В приказе определяется список сотрудников, допущенных к работе в ИСПДн. С целью обеспечения ответственности за ведение, нормальное функционирование и контроль работы средств защиты информации и выполнения необходимых мероприятий по обеспечению безопасности в ИСПДн заведующим на основании приказа назначается ответственный за организацию обработки персональных данных. Ответственный за организацию обработки персональных данных обязан, ознакомится с инструкцией ответственного за организацию обработки персональных данных под роспись (Приложение 1).

2.3. С целью соблюдения принципа персональной ответственности за свои действия каждому сотруднику, допущенному к работе в ИСПДн, должно быть сопоставлено персональное уникальное имя (учетная запись пользователя), под которым он будет

регистрироваться, и работать в ИСПДн. Использование несколькими сотрудниками при работе в ИСПДн одного и того же имени пользователя запрещено. В дальнейшем, процедура регистрации (создания учетной записи) пользователя и предоставления ему (или изменения его) прав доступа к ресурсам ИСПДн инициируется ответственным за организацию обработки персональных Сотруднику, зарегистрированному в качестве нового пользователя ИСПДн, сообщается имя соответствующего ему пользователя и может выдаваться персональный идентификатор (для работы в режиме усиленной аутентификации) и начальное значение пароля, которое он обязан сменить при первом же входе в систему. Привилегии пользователей задаются в разрешительной системе доступа к ИСПДн. Логины и пароли доступа к ИСПДн заносятся в журнал паролей (Приложение 2).

**3. Порядок работы пользователей ИСПДн в части обеспечения безопасности ПДн при их обработке в ИСПДн**

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

3.2. Пользователь несет ответственность за правильность включения и выключения средств вычислительной техники (СВТ), входа в систему и все действия при работе в ИСПДн. Перед началом работы в ИСПДн, сотрудники ОУ, допущенные к работе с ПДн, принимают под роспись обязательство о неразглашении персональных данных (Приложение 3).

3.3. Пользователь обязан, ознакомится с инструкцией пользователя, осуществляющего обработку персональных данных на объектах вычислительной техники МБДОУ «ДСКВ №18» (Приложение 4), а также с инструкцией пользователя, по проведению антивирусного контроля на объектах вычислительной техники МБДОУ «ДСКВ №18» (Приложение 6) под роспись.

3.4. Вход пользователя в систему должен осуществляться по выдаваемому ему электронному идентификатору и по персональному паролю; Запись информации, содержащей ПДн, должна осуществляться только на машинные носители информации, соответствующим образом учтенные в Журнале учета защищаемых носителей информации. При работе со съемными машинными носителями информации пользователь каждый раз перед началом работы обязан проверить их на отсутствие вирусов с использованием штатных антивирусных программ, установленных на компьютерах ИСПДн. В случае обнаружения вирусов пользователь обязан немедленно прекратить их использование и действовать в соответствии с требованиями данного Положения;

3.5. Каждый сотрудник, участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки ПДн и имеющий доступ к аппаратным средствам, программному обеспечению и данным ИСПДн, несет персональную ответственность за свои действия и обязан:

- строго соблюдать установленные правила обеспечения безопасности информации при работе с программными и техническими средствами ИСПДн;
- знать и строго выполнять правила работы со средствами защиты информации, установленными на компьютерах ИСПДн;
- хранить в тайне свой пароль (пароли).

В соответствии с п. 7. данного Положения и с установленной периодичностью менять свой пароль (пароли); хранить установленным порядком свое индивидуальное устройство идентификации (ключ) и другие реквизиты в недоступном для посторонних месте; выполнять требования Положения по организации антивирусной защиты в полном объеме. Немедленно известить заведующего (или лицо его замещающего) в случае утери индивидуального устройства идентификации (ключа) или при подозрении компрометации личных ключей и паролей, а также при обнаружении: фактов совершения попыток несанкционированного доступа (далее - НСД) к ИСПДн; несанкционированных изменений в конфигурации программных или аппаратных средств ИСПДн; отклонений в нормальной работе системных и прикладных программных средств, затрудняющих эксплуатацию СВТ, выхода из строя или неустойчивого функционирования узлов СВТ или периферийных устройств (сканера, принтера и т.п.), а также перебоев в системе электроснабжения; некорректного функционирования установленных на компьютеры

технических средств защиты; непредусмотренных отводов кабелей и подключенных устройств.

3.6. Пользователю категорически запрещается:

- использовать компоненты программного и аппаратного обеспечения ПЭВМ в неслужебных целях;
- самовольно вносить какие-либо изменения в конфигурацию аппаратно-программных средств ИСПДн или устанавливать дополнительно любые программные и аппаратные средства, не предусмотренные архивом дистрибутивов установленного программного обеспечения;
- осуществлять обработку ПДн в присутствии посторонних (не допущенных к данной информации) лиц;
- записывать и хранить ПДн на неучтенных машинных носителях информации;
- оставлять включенным без присмотра компьютер, не активизировав средства защиты от НСД (временную блокировку экрана и клавиатуры);
- оставлять без личного присмотра на рабочем месте или где бы то ни было свое персональное устройство идентификации, машинные носители и распечатки, содержащие ПДн;
- умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты, которые могут привести к нарушению конфиденциальности ПДн;
- размещать средства отображения информации (монитор, принтер и т.п.) таким образом, чтобы с них существовала возможность визуального считывания информации посторонними лицами.

3.7. Администратор безопасности обязан: знать состав основных и вспомогательных технических систем и средств (далее - ОТСС и ВТСС) установленных и смонтированных в ИСПДн, перечень используемого программного обеспечения (далее - ПО) в ИСПДн; производить необходимые настройки подсистемы управления доступом установленных в ИСПДн СЗИ от НСД и сопровождать их в процессе эксплуатации, при этом: реализовывать полномочия доступа (чтение, запись) для каждого пользователя к элементам защищаемых информационных ресурсов (файлам, каталогам, принтеру и т.д.); вводить описания пользователей ИСПДн в информационную базу системы разграничения доступа в ИСПДн; своевременно удалять описания пользователей из базы данных СЗИ при изменении списка допущенных к работе лиц; проводить инструктаж сотрудников - пользователей компьютеров по правилам работы с используемыми техническими средствами и системами защиты информации; контролировать своевременное (не реже чем один раз в течение 360 дней) проведение смены паролей для доступа пользователей к компьютерам и ресурсам ИСПДн; обеспечивать постоянный контроль выполнения сотрудниками установленного комплекса мероприятий по обеспечению безопасности информации в ИСПДн; осуществлять контроль порядка создания, учета, хранения и использования резервных и архивных копий массивов данных; настраивать и сопровождать подсистемы регистрации и учета действий пользователей при работе в ИСПДн; организовывать печать файлов пользователей на принтере и осуществлять контроль соблюдения установленных правил и параметров регистрации и учета бумажных носителей информации; периодически тестировать функции СЗИ от НСД с использованием специальных средств анализа защищенности, особенно при изменении программной среды и полномочий исполнителей; восстанавливать программную среду, программные средства и настройки СЗИ при сбоях; вести две копии программных средств СЗИ от НСД и контролировать их работоспособность; периодически обновлять антивирусные средства (базы данных), контролировать соблюдение пользователями порядок и правила проведения антивирусного тестирования; проводить работу по выявлению возможных каналов вмешательства в процесс функционирования ИСПДн и осуществления несанкционированного доступа к информации и техническим средствам вычислительной техники; обеспечивать строгое выполнение требований по обеспечению безопасности информации при организации технического обслуживания ИСПДн и отправке его в ремонт (контролировать затирание персональных данных на носителях информации); присутствовать (участвовать) в работах по внесению изменений в

аппаратно-программную конфигурацию ИСПДн; вести документацию на ИСПДн в соответствии с требованиями нормативных документов.

**4. Порядок резервирования и восстановления работоспособности технических средств, программного обеспечения, баз данных, защищаемой информации и средств защиты информации**

4.1. Настоящий порядок определяет организацию резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации.

4.2. К использованию, для создания резервной копии в ИСПДн, допускаются только зарегистрированные в Журнале учета носители. Администратор безопасности обязан осуществлять периодическое резервное копирование персональных данных. Носители информации, предназначенные для создания резервной копии и хранения персональных данных, выдаются установленным порядком администратором безопасности. По окончании процедуры резервного копирования электронные носители сдаются на хранение администратору безопасности, или заведующему. При восстановлении работоспособности программного обеспечения сначала осуществляется резервное копирование защищаемой информации, затем производится полная деинсталляция некорректно работающего программного обеспечения. Восстановление программного обеспечения производится путем его инсталляции с использованием эталонных дистрибутивов, хранение которых осуществляется администратором безопасности в специальном хранилище.

4.3. При работе на компьютерах ИСПДн рекомендуется использовать источники бесперебойного питания, с целью предотвращения повреждения технических средств и(или) защищаемой информации в результате сбоев в сети электропитания. При восстановлении работоспособности средств защиты информации следует выполнить их настройку в соответствии с требованиями безопасности информации, изложенными в техническом задании на создание системы защиты персональных данных. Восстановление средств защиты информации производится с использованием эталонных сертифицированных дистрибутивов, которые хранятся у администратора безопасности. После успешной настройки средств защиты информации необходимо выполнить резервное копирование настроек данных средств с помощью встроенных в них функций на зарегистрированный носитель. Ответственность за проведение резервного копирования, мероприятий по восстановлению работоспособности технических средств, мероприятий по восстановлению средств защиты информации возлагается на администратора безопасности.

**5. Порядок обучения персонала практике работы в ИСПДн в части обеспечения безопасности персональных данных**

5.1. Перед началом работы в ИСПДн пользователи должны ознакомиться с требованиями настоящего Положения под роспись;

5.2. Пользователи должны продемонстрировать администратору безопасности наличие необходимых знаний и умений для выполнения требований настоящего Положения;

5.3. Ответственным за организацию обучения и оказание методической помощи в ДОУ является администратор безопасности;

**6. Правила антивирусной защиты**

6.1. Настоящие правила определяют требования к организации защиты объекта ИСПДн от разрушающего воздействия вредоносного программного обеспечения, компьютерных вирусов и устанавливает ответственность руководителя и сотрудников, эксплуатирующих и сопровождающих компьютеры в составе ИСПДн, за их выполнение.

6.2. К использованию на компьютерах допускаются только лицензионные антивирусные средства; Установка и начальная настройка средств антивирусного контроля на компьютерах осуществляется администратором безопасности; Администратор безопасности осуществляет периодическое обновление антивирусных средств и контроль их работоспособности; Ярлык (ссылка) для запуска антивирусной программы должен быть доступен всем пользователям информационной системы;

6.3. Еженедельно в начале работы, после загрузки компьютера в автоматическом режиме должен проводиться антивирусный контроль всех дисков и файлов компьютеров; Обязательному антивирусному контролю подлежит любая информация (текстовые файлы

любых форматов, файлы данных, исполняемые файлы), информация на съемных носителях (магнитных дисках, лентах, CD-ROM и т.п.). Контроль исходящей информации необходимо проводить непосредственно перед архивированием и отправкой (записью на съемный носитель); Файлы, помещаемые в электронный архив на магнитных носителях, должны в обязательном порядке проходить антивирусный контроль; Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено на отсутствие вирусов. Непосредственно после установки (изменения) программного обеспечения компьютера, администратором безопасности должна быть выполнена антивирусная проверка ИСПДн; На компьютеры пользователей запрещается установка программного обеспечения, не связанного с выполнением функций, предусмотренных технологическим процессом обработки информации; При возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.) пользователь самостоятельно (или вместе с администратором безопасности) должен провести внеочередной антивирусный контроль компьютера. В случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов пользователь обязан: приостановить обработку данных в ИСПДн; немедленно поставить в известность о факте обнаружения зараженных вирусом файлов администратора безопасности, а также смежные подразделения, использующие эти файлы в работе; совместно с владельцем зараженных вирусом файлов провести анализ возможности, дальнейшего их использования; провести лечение или уничтожение зараженных файлов. Ответственность за организацию антивирусного контроля в ИСПДн в соответствии с требованиями настоящего Положения возлагается на администратора безопасности; Ответственность за проведение мероприятий антивирусной защиты в конкретной ИСПДн и соблюдение требований настоящего Положения возлагается на администратора безопасности и всех пользователей данной ИСПДн.

**7. Порядок контроля обеспечения защиты информации в ИСПДн и приостановки предоставления ПДн в случае обнаружения нарушений порядка их предоставления.**

Контроль защиты информации в ИСПДн - комплекс организационных и технических мероприятий, которые организуются и осуществляются в целях предупреждения и пресечения возможности получения посторонними лицами охраняемых сведений, выявления и предотвращения утечки информации по техническим каналам, исключения или существенного затруднения несанкционированного доступа к информации, хищения технических средств и носителей информации, предотвращения специальных программно-технических воздействий, вызывающих нарушение характеристик безопасности информации или работоспособности систем информатизации. Основными задачами контроля являются: проверка организации выполнения мероприятий по защите информации в учреждении, учета требований по защите информации в разрабатываемых плановых и распорядительных документах; выявление демаскирующих признаков объектов ИСПДн; уточнение зон перехвата обрабатываемой на объектах информации, возможных каналов утечки информации, несанкционированного доступа к ней и программно-технических воздействий на информацию; проверка выполнения установленных норм и требований по защите информации от утечки по техническим каналам, оценка достаточности и эффективности мероприятий по защите информации; проверка выполнения требований по защите ИСПДн от несанкционированного доступа; проверка выполнения требований по антивирусной защите автоматизированных систем и автоматизированных рабочих мест; проверка знаний работников по вопросам защиты информации и их соответствия требованиям уровня подготовки для конкретного рабочего места; оперативное принятие мер по пресечению нарушений требований (норм) защиты информации в ИСПДн; разработка предложений по устранению (ослаблению) демаскирующих признаков и технических каналов утечки информации.

**8. Порядок охраны и допуска посторонних лиц в помещения ИСПДн.**

В ДОУ должна быть предусмотрена физическая охрана технических средств ИСПДн (устройств и носителей информации), предусматривающая контроль доступа в помещения посторонних лиц, наличие надежных препятствий для несанкционированного проникновения в помещения и хранилище носителей информации. В помещениях должна быть установлена охранная и пожарная сигнализация. Серверное и коммутационное

оборудование ИСПДн должно находиться под надежным замком, в отдельном помещении или запирающемся шкафу, ключ должен храниться у администратора безопасности. Вскрытие и закрытие помещений осуществляется сотрудниками, работающими в данных помещениях. При обнаружении повреждения замков, дверей или наличия других признаков, указывающих на возможное проникновение в помещение посторонних лиц, помещение не вскрывается, а составляется акт, в присутствии сторожа. О происшествии немедленно сообщается заведующему.

**9. Заключительные положения**

Требования настоящего Положения обязательны для всего коллектива ДОУ, обрабатывающих персональные данные. Нарушение требований настоящего Положения влечет за собой дисциплинарную, гражданско-правовую, административную или уголовную ответственность в соответствии с законодательством Российской Федерации.