Башҡортостан Республикаһы Йылайыр районы муниципаль районы йылайыр ауылы «Ҡайынҡай» дөйөм үҫтереү төрөндәге балалар баҡса3ы мектепкесе белембиреү муниципаль автономлы учреждение3ы
453680,Йылайырауылы,Столичный урамы,11а,
тел.8(34752)2-33-75
ОКПО55832957,ОГРН1020201547453
ИНН/КПП 0223003196/022301001

Муниципальное автономное дошкольное образовательное учреждение Детский сад общеразвивающего вида «Березка» с. Зилаир муниципального района Зилаирский район Республики Башкортостан,
453680,с.Зилаир,ул.Столичная 11 а,
тел.8(34752)2-33-75
ОКПО55832957,ОГРН1020201547453
ИНН/КПП 0223003196/0223010014536

БОЙОРОК: **ПРИКАЗ:**

29.08.2025й. № 45 29.08.2025г.

О назначении ответственного за информационную безопасность

В соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Постановлением Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»,

ПРИКАЗЫВАЮ:

1. Назначить старшего воспитателя Каплину Юлию Владимировну ответственным за информационную безопасность.
2. Возложить на сотрудника, указанного в пункте 1 настоящего приказа, выполнение следующих обязанностей:
   - организация комплексной защиты информации в МАДОУ д/с «Березка» с.Зилаир;
   - оценка рисков при использовании сотрудниками МАДОУ д/с «Березка» с.Зилаир;
   - информационных систем;
   - организация исполнения и применения процедур безопасности при использовании сотрудниками МАДОУ д/с «Березка» с.Зилаир информационных систем;
   - организация обновления программ безопасности (антивирусных программ, версий программного обеспечения);
   - обеспечение восстановления информационных систем после атак или иных отказов в работе;
   - разработка проектов локальных нормативных актов в сфере обеспечения информационной безопасности при использовании информационных систем МАДОУ д/с «Березка» с.Зилаир;
   систематическое разъяснение сотрудникам МАДОУ д/с «Березка» с.Зилаир требований информационной безопасности, установленных законодательством РФ.
3. Утвердить меры по обеспечению безопасности персональных данных, реализуемые в рамках защиты персональных данных с учетом актуальных угроз безопасности и применяемых информационных технологий (Приложение 1).
4. Утвердить план мероприятий по защите персональных данных (Приложение 2).
5. Утвердить форму журнала учета событий информационной безопасности (Приложение 3).
6. Контроль за исполнением настоящего приказа оставляю за собой.

Подписано цифровой подписью: МУНИЦИПАЛЬНОЕ АВТОНОМНОЕ ДОШКОЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ДЕТСКИЙ САД ОБЩЕРАЗВИВАЮЩЕГО ВИДА "БЕРЕЗКА" С. ЗИЛАИР МУНИЦИПАЛЬНОГО РАЙОНА ЗИЛАИРСКИЙ РАЙОН РЕСПУБЛИКИ БАШКОРТОСТАН
DN: E=uc_fk@roskazna.ru, S=77 Москва, ИНН КЛ=7710568760, ОГРН=1047797019830, STREET="Большой Златоустинский переулок, д. 6, строение 1", L=г. Москва, C=RU, O=Казначейство России, CN=Федеральное казначейство
Причина: Заведующий Чекалова Любовь Васильевна
Местонахождение: с. Зилаир Зилаирский район Республики Башкортостан
Дата: 12 Февраль 2026 г. 9:51:08

Приложение № 1

Меры по обеспечению безопасности персональных данных, реализуемых в рамках защиты персональных данных с учетом актуальных угроз безопасности и применяемых информационных технологий

№	Перечень мер	Цель реализации
1	Идентификация и аутентификация субъектов доступа и объектов доступа	Обеспечение присвоения субъектам и объектам доступа уникального признака (идентификатора), сравнения предъявляемого субъектом (объектом) доступа идентификатора с перечнем присвоенных идентификаторов, а также проверка принадлежности субъекту (объекту) доступа предъявленного им идентификатора (подтверждение подлинности)
2	Управление доступом субъектов доступа к объектам доступа	Обеспечение управления правами и привилегиями субъектов доступа, разграничения доступа субъектов доступа к объектам доступа на основе совокупности установленных в информационной системе правил разграничения доступа, а также контроля за соблюдением этих правил
3	Ограничение программной среды	Обеспечение установки и (или) запуска, только разрешенного к использованию в информационной системе программного обеспечения или исключение возможности установки и (или) запуска, запрещенного к использованию в информационной системе программного обеспечения
4	Защита машинных носителей информации, на которых хранятся и (или) обрабатываются персональные данные	Исключение возможности несанкционированного доступа к машинным носителям и хранящимся на них персональным данным, а также несанкционированного использования съемных машинных носителей персональных данных
5	Регистрация событий безопасности	Обеспечение сбора, записи, хранения и защиты информации о событиях безопасности в информационной системе, а также возможности просмотра и анализа информации о таких событиях и реагирования на них
6	Антивирусная защита	Обнаружение в информационной системе компьютерных программ либо иной компьютерной информации, предназначенной для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты информации, а также реагирование на обнаружение этих программ и информации
7	Обнаружение (предотвращение) вторжений	Обнаружение действий в информационной системе, направленных на несанкционированный доступ к информации, специальные воздействия на информационную систему и (или) персональные данные в целях добывания, уничтожения, искажения и блокирования доступа к персональным данным, а также реагирование на эти действия

8	Контроль (анализ) защищенности персональных данных	Обеспечение контроля уровня защищенности персональных данных, обрабатываемых в информационной системе, путем проведения систематических мероприятий по анализу защищенности информационной системы и тестированию работоспособности системы защиты персональных данных
9	Обеспечение целостности информационной системы и персональных данных	Обнаружение фактов несанкционированного нарушения целостности информационной системы и содержащихся в ней персональных данных, а также возможность восстановления информационной системы и содержащихся в ней персональных данных
10	Обеспечение доступности персональных данных	Авторизованный доступ пользователей, имеющих права по доступу, к персональным данным, содержащимся в информационной системе, в штатном режиме функционирования информационной системы
11	Защита среды виртуализации	Исключение несанкционированного доступа к персональным данным, обрабатываемым в виртуальной инфраструктуре, и к компонентам виртуальной инфраструктуры и (или) воздействия на них, в том числе к средствам управления виртуальной инфраструктурой, монитору виртуальных машин (гипервизору), системечерез элементы виртуальной или физической инфраструктуры, гостевым операционным системам, виртуальным машинам (контейнерам), системе и сети репликации, терминальным и виртуальным устройствам, а также системе резервного копирования и создаваемым ею копиям хранения данных (включая систему хранения образов виртуальной инфраструктуры), сети передачи данных
12	Защита технических средств	Исключение несанкционированного доступа к стационарным техническим средствам, обрабатывающим персональные данные, средствам, обеспечивающим функционирование информационной системы, и в помещения, в которых они постоянно расположены, защиту технических средств от внешних воздействий, а также защиту персональных данных, представленных в виде информативных электрических сигналов и физических полей
13	Защита информационной системы, ее средств, систем связи и передачи данных	Обеспечение защиты персональных данных при взаимодействии информационной системы или ее отдельных сегментов с иными информационными системами и информационно-телекоммуникационными сетями посредством применения архитектуры информационной системы и проектных решений, направленных на обеспечение безопасности персональных данных

14	Выявление инцидентов (одного события или группы событий), которые могут привести к сбоям или нарушению функционирования информационной системы и (или) к возникновению угроз безопасности персональных данных (далее - инциденты), и реагирование на них	Обеспечение обнаружения, идентификации, анализа инцидентов в информационной системе, а также принятия мер по устранению и предупреждению инцидентов
15	Управление конфигурацией информационной системы и системы защиты персональных данных	Обеспечение управления изменениями конфигурации информационной системы и системы защиты персональных данных, анализ потенциального воздействия планируемых изменений на обеспечение безопасности персональных данных, а также документирования этих изменений

Приложение № 2

Утверждено:
Заведующий
МАДОУ д/с «Березка» с.Зилаир
Л.В.Чекалова
Приказ № 45 от «29» августа 2025г.

План мероприятий по защите персональных данных в МАДОУ д/с «Березка» с.Зилаир

№	Наименование	Сроки	Ответственные	Примечание
1	Актуализация локальных актов, регламентирующих защиту персональных данных	По мере необходимости	Каплина Ю.В.	Необходимость определяется внесением изменений в действующее законодательство РФ
2	Определение уровня защищенности персональных данных при их обработке в информационных системах персональных данных (ИСПДн)	По мере необходимости	Каплина Ю.В.	Проводится при оформлении доступа к ИСПДн, при выявлении в ИСПДн изменения ее состава или структуры
3	Внутренний контроль соответствия обработки персональных данных требованиям к защите персональных данных	Ежеквартально	Каплина Ю.В.	Проводится путем непосредственной проверки на рабочих местах ответственных сотрудников
4	Проверка сведений, содержащихся в уведомлении об обработке персональных данных, размещенных в Реестре операторов персональных данных на сайте Роскомнадзора	По мере необходимости	Каплина Ю.В.	В Роскомнадзор направляется актуальная редакция уведомления об обработке персональных данных
5	Уничтожение персональных данных при достижении целей их обработки и сроков хранения	Ежемесячно	Каплина Ю.В.	Проводится по представлению ответственного по ИБ
6	Контроль эффективности средств защиты персональных данных	Раз в год	Каплина Ю.В.	При необходимости привлекается организация, имеющая лицензию на осуществление деятельности по технической защите конфиденциальной информации