Муниципальное бюджетное дошкольное образовательное учреждение
детский сад № 47

ПРИКАЗ

23 марта 2026года **№ 26**

Ковров

Об утверждении документов по защите информации

В соответствии с действующим законодательством Российской Федерации о защите информации, с целью обеспечения безопасности информации и персональных данных (ПДн) Муниципального бюджетного дошкольного образовательного учреждения детский сад № 47 (далее по тексту – МБДОУ № 47)

п р и к а з ы в а ю:

1. Утвердить следующие документы:

1.1. Политику МБДОУ № 47 в отношении обработки информации и ПДн согласно приложению № 1;

1.2. Инструкцию по работе пользователя в государственных, региональных и автоматизированных информационных системах, используемых в МБДОУ № 47 согласно приложению № 2;

1.3. Инструкцию по организации антивирусной защиты согласно приложению № 3;

1.4. Инструкцию по применению парольной политики согласно приложению № 4;

1.5. Перечень информационных систем в МБДОУ № 47 для обработки персональных данных и сопутствующей информации, не составляющей государственную тайну, согласно приложению № 5;

1.6. Положение по защите информации в государственной информационной системе «Региональный сегмент единой федеральной межведомственной системы учета контингента обучающихся по основным образовательным программам и дополнительным общеобразовательным программам» согласно приложению № 6;

1.7. Методику и акт определения класса защищенности государственной информационной системе «Региональный сегмент единой федеральной межведомственной системы учета контингента обучающихся по образовательным программам и дополнительным общеобразовательным программам» согласно приложению № 7;

1.8. Бланки уведомлений уполномоченных органов согласно приложению № 8;

1.9. Бланки уведомлений субъектов ПДн согласно приложению № 9;

1.10. Бланки заявлений субъектов ПДн согласно приложению № 10;

1.11. Форму обязательства о неразглашении информации, содержащей ПДн; согласно приложению № 11;

1.12. Инструкцию о порядке действий во внештатных ситуациях и восстановлению после сбоя согласно приложению № 12.

1.13. Инструкцию по работе с носителями персональных данных в МБДОУ № 47 согласно приложению № 13;

1.14. Порядок ознакомления работников МБДОУ № 47, непосредственно осуществляющих обработку персональных данных или осуществляющих доступ к ним согласно приложению № 14.

2. Утвердить следующие формы журналов:

– Журнал инструктажа по защите информации и ПДн согласно приложению № 15;

– Журнал учета средств защиты информации и эксплуатационной документации согласно приложению № 16;

– Журнал учета мероприятий по контролю над соблюдением режима защиты информации согласно приложению № 17;

– Журнал учета обращений субъектов ПДн согласно приложению № 18;

– Журнал учета процедур резервного копирования согласно приложению № 25;

– Журнал учета носителей персональных данных МБДОУ № 47 согласно приложению № 19.

3. Администраторам информационной безопасности проводить первичный/очередной инструктажи по утвержденным документам среди сотрудников МБДОУ № 47, участвующих в процессе обработки защищаемой информации, под подпись в Журнале инструктажей.

4. Должность ФИО разместить настоящий приказ на официальном сайте МБДОУ № 47.

5. Контроль исполнения настоящего приказа возложить на делопроизводителя Склярову Л.В.

Заведующий

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 008654EEC3742607C1D843EFF7FF719202
Владелец: Симонова Елена Петровна
Действителен: с 19.05.2025 до 12.08.2026

Е.П. Симонова

Приложение № 1
к приказук приказу №26
от 24.03.2026 г .

ПОЛИТИКА
МБДОУ № 47 в отношении обработки информации и персональных данных

1. Термины и определения

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

Оператор - государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку ПДн, а также определяющие цели обработки ПДн, состав ПДн, подлежащих обработке, действия (операции), совершаемые с ПДн.

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

Автоматизированная обработка ПДн - обработка ПДн с помощью средств вычислительной техники.

Распространение ПДн - действия, направленные на раскрытие ПДн неопределенному кругу лиц.

Предоставление ПДн - действия, направленные на раскрытие ПДн определенному лицу или определенному кругу лиц.

Блокирование ПДн - временное прекращение обработки ПДн (за исключением случаев, если обработка необходима для уточнения ПДн).

Уничтожение ПДн - действия, в результате которых становится невозможным восстановить содержание ПДн в ИСПДн и (или) в результате которых уничтожаются материальные носители ПДн.

Обезличивание ПДн - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность ПДн конкретному субъекту ПДн.

Трансграничная передача ПДн - передача ПДн на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

2. Назначение и правовая основа документа

Политика МБДОУ № 47 (далее по тексту – Политика) определяет систему взглядов на проблему обеспечения безопасности ПДн и представляет собой систематизированное изложение целей и задач защиты, как одно или несколько правил, процедур, практических приемов и руководящих принципов в области информационной безопасности, которыми руководствуется МБДОУ № 47 в своей

деятельности, а также основных принципов построения, организационных, технологических и процедурных аспектов обеспечения безопасности информации.

Законодательной основой настоящей Политики являются Конституция Российской Федерации, Гражданский, Уголовный кодексы, Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных», Федеральный закон РФ от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и защите информации», законы, указы, постановления, другие нормативные документы действующего законодательства Российской Федерации, документы ФСТЭК и ФСБ России.

Использование данной Политики в качестве основы для построения комплексной системы информационной безопасности информации МБДОУ № 47 позволит оптимизировать затраты на ее построение.

При разработке Политики учитывались основные принципы создания комплексных систем обеспечения безопасности информации, характеристики и возможности организационно-технических методов и современных аппаратно-программных средств защиты и противодействия угрозам безопасности информации.

Основные положения Политики базируются на качественном осмыслении вопросов безопасности информации и не затрагивают вопросов экономического (количественного) анализа рисков и обоснования необходимых затрат на защиту информации.

3. Основными объектами системы безопасности информации в МБДОУ № 47 являются:

– информационные ресурсы с ограниченным доступом, содержащие ПДн и сопутствующую информацию, не составляющую государственную тайну, в том числе о родившихся и зарегистрированных по месту жительства обучающихся, а также сведения обо всех этапах обучения детей;

– процессы обработки информации в информационных системах МБДОУ № 47, информационные технологии, регламенты и процедуры сбора, обработки, хранения и передачи информации, персонал пользователей системы и ее обслуживающий персонал;

– информационная инфраструктура, включающая системы обработки и анализа информации, технические и программные средства ее обработки, передачи и отображения, в том числе каналы информационного обмена и телекоммуникации, системы и средства защиты информации, объекты и помещения, в которых расположены технические средства обработки информации.

4. Интересы затрагиваемых субъектов информационных отношений

Субъектами информационных отношений при обеспечении безопасности информации **МБДОУ № 47** являются:

– **МБДОУ № 47**, как собственник информационных ресурсов и технических средств обработка информации;

– Субъекты персональных данных, в том числе родившиеся и зарегистрированные по месту жительства (обучающиеся).

Перечисленные субъекты информационных отношений заинтересованы в обеспечении:

– своевременного доступа к необходимой информации (доступность);

– достоверности (полноты, точности, адекватности, целостности) информации;

– конфиденциальности (сохранения в тайне) информации;

– защиты от навязывания им ложной (недостоверной, искаженной) информации;

– разграничения ответственности за нарушения их прав (интересов) и установленных правил обращения с информацией;

– возможности осуществления непрерывного контроля и управления процессами обработки и передачи информации;

– защиты информации от незаконного распространения.

4.1. Цели защиты

Основной целью, на достижение которой направлены все положения настоящей Политики, является защита субъектов информационных отношений МБДОУ № 47 от возможного нанесения им материального, физического, морального или иного ущерба, посредством случайного или преднамеренного воздействия на информацию, их носители, процессы обработки и передачи.

Указанная цель достигается посредством обеспечения и постоянного поддержания следующих свойств информации:

– доступности для легальных пользователей (устойчивого функционирования информационных систем МБДОУ № 47, при котором пользователи имеют возможность получения необходимой информации и результатов решения задач за приемлемое для них время);

– целостности и аутентичности (подтверждение авторства) ПДн, хранимых и обрабатываемых в информационных системах МБДОУ № 47 и передаваемой по каналам связи;

– конфиденциальности - сохранения в тайне определенной части информации, хранимой, обрабатываемой и передаваемой по каналам связи.

Необходимый уровень доступности, целостности и конфиденциальности информации обеспечивается соответствующими множеству значимых угроз методами и средствами.

4.2. Основные задачи системы обеспечения безопасности информации

Для достижения основной цели защиты и обеспечения указанных свойств информации система обеспечения информационной безопасности МБДОУ № 47 должна обеспечивать эффективное решение следующих задач:

– своевременное выявление, оценка и прогнозирование источников угроз информационной безопасности, причин и условий, способствующих нанесению ущерба заинтересованным субъектам информационных отношений, нарушению нормального функционирования информационных систем;

– создание механизма оперативного реагирования на угрозы безопасности информации и негативные тенденции;

– создание условий для минимизации и локализации наносимого ущерба неправомерными действиями физических и юридических лиц, ослабление негативного влияния и ликвидация последствий нарушения безопасности информации;

– защиту от вмешательства в процесс функционирования информационных систем посторонних лиц (доступ к информационным ресурсам должны иметь только зарегистрированные в установленном порядке пользователи);

– разграничение доступа пользователей к информационным, аппаратным, программным и иным ресурсам МБДОУ № 47 (возможность доступа только к тем ресурсам и выполнения только тех операций с ними, которые необходимы конкретным пользователям для выполнения своих служебных обязанностей), то есть защиту от несанкционированного доступа;

– обеспечение аутентификации пользователей, участвующих в информационном обмене (подтверждение подлинности отправителя и получателя информации);

– защиту от несанкционированной модификации используемых в информационных системах МБДОУ № 47 программных средств, а также защиту системы от внедрения несанкционированных программ, включая компьютерные вирусы;

– защиту информации ограниченного пользования от утечки по техническим каналам при ее обработке, хранении и передаче по каналам связи.

4.3. Основные пути решения задач системы защиты

Поставленные основные цели защиты и решение перечисленных выше задач достигаются:

– строгим учетом всех подлежащих защите ресурсов информационных систем МБДОУ № 47 (информации, задач, документов, каналов связи, серверов, автоматизированных рабочих мест);

– журналированием действий персонала, осуществляющего обслуживание и модификацию программных и технических средств информационных систем;

– полнотой, реальной выполнимостью и непротиворечивостью требований организационно-распорядительных документов МБДОУ № 47 по вопросам обеспечения безопасности информации;

– подготовкой должностных лиц (сотрудников), ответственных за организацию и осуществление практических мероприятий по обеспечению безопасности ПДн и процессов их обработки;

– наделением каждого сотрудника (пользователя) минимально необходимыми для выполнения им своих функциональных обязанностей полномочиями по доступу к информационным ресурсам МБДОУ № 47;

– четким знанием и строгим соблюдением всеми пользователями информационных систем МБДОУ № 47 требований организационно-распорядительных документов по вопросам обеспечения безопасности информации;

– персональной ответственностью за свои действия каждого сотрудника, в рамках своих функциональных обязанностей имеющего доступ к информационным ресурсам МБДОУ № 47;

– непрерывным поддержанием необходимого уровня защищенности элементов информационной среды;

– применением физических и технических (программно-аппаратных) средств защиты ресурсов системы и непрерывной административной поддержкой их использования;

– эффективным контролем над соблюдением пользователями информационных ресурсов требований по обеспечению безопасности информации;

– юридической защитой интересов **МБДОУ № 47** при взаимодействии с внешними организациями (связанном с обменом информацией) от противоправных действий, как со стороны этих организаций, так и от несанкционированных действий обслуживающего персонала и третьих лиц.

5. Построение системы, обеспечение безопасности информации МБДОУ № 47 и ее функционирование должны осуществляться в соответствии со следующими основными принципами:

5.1. Законность

Предполагает осуществление защитных мероприятий и разработку системы безопасности информации МБДОУ № 47 в соответствии с действующим законодательством в области защиты информации, а также других законодательных актов по безопасности информации РФ, с применением всех дозволенных методов обнаружения и пресечения правонарушений при работе с информацией. Принятые меры безопасности ПДн не должны препятствовать доступу правоохранительных органов в предусмотренных законодательством случаях.

Все пользователи информационных систем должны иметь представление об ответственности за правонарушения в области защиты информации.

5.2. Системность

Системный подход к построению системы защиты информации в МБДОУ № 47 предполагает учет всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, значимых для понимания и решения проблемы обеспечения безопасности информации.

При создании системы защиты должны учитываться все слабые и наиболее уязвимые места информационных систем, а также характер, возможные объекты и направления атак на нее со стороны нарушителей (особенно высококвалифицированных злоумышленников).

Система защиты должна строиться с учетом не только всех известных каналов проникновения и несанкционированного доступа к информации, но и с учетом возможности появления принципиально новых путей реализации угроз безопасности.

5.3. Комплексность

Комплексное использование методов и средств защиты компьютерных систем предполагает согласованное применение разнородных средств при

построении целостной системы защиты, перекрывающей все существенные (значимые) каналы реализации угроз и не содержащей слабых мест на стыках отдельных ее компонентов. Защита должна строиться эшелонировано. Внешняя защита должна обеспечиваться физическими средствами, организационными и правовыми мерами.

5.4. Непрерывность защиты

Обеспечение безопасности информации - процесс, осуществляемый руководством МБДОУ № 47, администратором безопасности информации и сотрудниками всех уровней. Это не только и не столько процедура или политика, которая осуществляется в определенный отрезок времени или совокупность средств защиты, сколько процесс, который должен постоянно идти на всех уровнях внутри МБДОУ № 47 и каждый сотрудник должен принимать участие в этом процессе. Деятельность по обеспечению информационной безопасности является составной частью повседневной деятельности МБДОУ № 47. И ее эффективность зависит от участия руководства МБДОУ № 47 в обеспечении информационной безопасности информации.

Кроме того, большинству физических и технических средств защиты для эффективного выполнения своих функций необходима постоянная организационная (административная) поддержка (своевременная смена и обеспечение правильного хранения и применения имен, паролей, переопределение полномочий и т.п.). Перерывы в работе средств защиты могут быть использованы злоумышленниками для анализа применяемых методов и средств защиты, для внедрения специальных программных и аппаратных "закладок" и других средств преодоления защиты.

5.5. Своевременность

Предполагает упреждающий характер мер обеспечения безопасности информации, то есть постановку задач по комплексной защите информации и реализацию мер обеспечения безопасности информации на ранних стадиях разработки информационных систем в целом и их систем защиты, в частности.

Разработка системы защиты должна вестись параллельно с разработкой и развитием самих защищаемых информационных систем. Это позволит учесть требования безопасности при проектировании архитектуры и, в конечном счете, создать более эффективные (как по затратам ресурсов, так и по стойкости) системы, обладающие достаточным уровнем защищенности.

5.6. Преемственность и совершенствование

Предполагает постоянное совершенствование мер и средств защиты информации на основе преемственности организационных и технических решений, кадрового состава, анализа функционирования информационных систем **МБДОУ № 47** и системы их защиты с учетом изменений в методах и средствах перехвата информации, нормативных требований по защите, достигнутого отечественного и зарубежного опыта в этой области.

5.7. Разумная достаточность (экономическая целесообразность)

Предполагает соответствие уровня затрат на обеспечение безопасности информации ценности информационных ресурсов и величине возможного ущерба от их разглашения, утраты, утечки, уничтожения и искажения. Используемые меры

и средства обеспечения безопасности информационных ресурсов не должны заметно ухудшать эргономические показатели работы компонентов информационных систем. Излишние меры безопасности, помимо экономической неэффективности, приводят к утомлению и раздражению персонала.

Создать абсолютно непреодолимую систему защиты принципиально невозможно. Пока информация находится в обращении, принимаемые меры могут только снизить вероятность негативных воздействий или ущерб от них, но не исключить их полностью. При достаточном количестве времени и средств возможно преодолеть любую защиту. Поэтому имеет смысл рассматривать некоторый приемлемый уровень обеспечения безопасности. Высокоэффективная система защиты стоит дорого, использует при работе существенную часть ресурсов и может создавать ощутимые дополнительные неудобства пользователям. Важно правильно выбрать тот достаточный уровень защиты, при котором затраты, риск и размер возможного ущерба были бы приемлемыми.

5.8. Персональная ответственность

Предполагает возложение ответственности за обеспечение безопасности информации и системы их обработки на каждого сотрудника в пределах его полномочий. В соответствии с этим принципом распределение прав и обязанностей сотрудников строится таким образом, чтобы в случае любого нарушения круг виновников был четко известен или сведен к минимуму.

5.9. Минимизация полномочий

Означает предоставление пользователям минимальных прав доступа в соответствии со служебной необходимостью. Доступ к информации должен предоставляться только в том случае и объеме, если это необходимо сотруднику для выполнения его должностных обязанностей.

5.10. Исключение конфликта интересов (разделение функций)

Эффективная система обеспечения информационной безопасности предполагает четкое разделение обязанностей сотрудников и исключение ситуаций, когда сфера ответственности сотрудников допускает конфликт интересов. Сферы потенциальных конфликтов должны выявляться, минимизироваться, и находится под строгим независимым контролем. Реализация данного принципа предполагает, что не один сотрудник не должен иметь полномочий, позволяющих ему единолично осуществлять выполнение критичных операций. Наделение сотрудников полномочиями, порождающими конфликт интересов, дает ему возможность подтасовывать информацию в корыстных целях или с тем, чтобы скрыть проблемы или понесенные убытки. Для снижения риска манипулирования информацией и риска хищения, такие полномочия должны в максимально возможной степени быть разделены между различными сотрудниками или подразделениями Управления. Необходимо проводить периодические проверки обязанностей, функций и деятельности сотрудников, выполняющих ключевые функции, с тем, чтобы они не имели возможности скрывать совершение неправомерных действий. Кроме того, необходимо принимать специальные меры по недопущению сговора между сотрудниками.

5.11. Взаимодействие и сотрудничество

Предполагает создание благоприятной атмосферы в коллективе МБДОУ № 47. В такой обстановке сотрудники должны осознанно соблюдать установленные правила и оказывать содействие деятельности администратора безопасности информации.

Важным элементом эффективной системы обеспечения безопасности информации в **МБДОУ № 47** является высокая культура работы с информацией. Руководство **МБДОУ № 47** несет ответственность за строгое соблюдение этических норм и стандартов профессиональной деятельности, подчеркивающей и демонстрирующей персоналу на всех уровнях важность обеспечения информационной безопасности **МБДОУ № 47**. Все сотрудники **МБДОУ № 47** должны понимать свою роль в процессе обеспечения информационной безопасности и принимать участие в этом процессе. Несмотря на то, что высокая культура обеспечения информационной безопасности не гарантирует автоматического достижения целей, ее отсутствие создает больше возможностей для нарушения безопасности или не обнаружения фактов ее нарушения.

5.12. Гибкость системы защиты

Система обеспечения информационной безопасности должна быть способна реагировать на изменения внешней среды и условий осуществления Управлением своей деятельности. В число таких изменений входят:

– изменения организационной и штатной структуры МБДОУ № 47;

– изменение существующих или внедрение принципиально новых информационных систем;

– новые технические средства.

Свойство гибкости системы обеспечения информационной безопасности избавляет в таких ситуациях от необходимости принятия кардинальных мер по полной замене средств и методов защиты на новые, что снижает ее общую стоимость.

5.13. Открытость алгоритмов и механизмов защиты

Суть принципа открытости алгоритмов и механизмов защиты состоит в том, что защита не должна обеспечиваться только за счет секретности структурной организации и алгоритмов функционирования ее подсистем. Знание алгоритмов работы системы защиты не должно давать возможности ее преодоления (даже авторам). Это, однако, не означает, что информация об используемых системах и механизмах защиты должна быть общедоступна.

5.14. Простота применения средств защиты

Механизмы и методы защиты должны быть интуитивно понятны и просты в использовании. Применение средств и методов защиты не должно быть связано со знанием специальных языков или с выполнением действий, требующих значительных дополнительных трудозатрат при обычной работе зарегистрированных пользователей, а также не должно требовать от пользователя выполнения рутинных малопонятных ему операций.

5.15. Обоснованность и техническая реализуемость

Информационные технологии, технические и программные средства, средства и меры защиты информации должны быть реализованы на современном

уровне развития науки и техники, обоснованы с точки зрения достижения заданного уровня безопасности информации и экономической целесообразности, а также должны соответствовать установленным нормам и требованиям по безопасности информации.

5.16. Специализация и профессионализм

Предполагает привлечение к разработке средств и реализации мер защиты информации специализированных организаций, наиболее подготовленных к конкретному виду деятельности по обеспечению безопасности информационных ресурсов, имеющих опыт практической работы и государственную лицензию на право оказания услуг в этой области. Реализация административных мер и эксплуатация средств защиты должна осуществляться профессионально подготовленными специалистами Управления.

5.17. Обязательность контроля

Предполагает обязательность и своевременность выявления и пресечения попыток нарушения установленных правил, обеспечения безопасности информации, на основе используемых систем и средств защиты информации, при совершенствовании критериев и методов оценки эффективности этих систем и средств.

Контроль за деятельностью любого пользователя, каждого средства защиты и в отношении любого объекта защиты должен осуществляться на основе применения средств оперативного контроля и регистрации и должен охватывать как несанкционированные, так и санкционированные действия пользователей.

Кроме того, эффективная система обеспечения информационной безопасности требует наличия адекватной и всеобъемлющей информации о текущем состоянии процессов, связанных с движением информации и сведений о соблюдении установленных нормативных требований, а также дополнительной информации, имеющей отношение к принятию решений. Информация должна быть надежной, своевременной, доступной и правильно оформленной.

Недостатки системы обеспечения информационной безопасности, выявленные сотрудниками **МБДОУ № 47**, должны немедленно доводиться до сведения руководителя **МБДОУ № 47** и оперативно устраняться. Вопросы, которые кажутся незначительными, когда отдельные процессы рассматриваются изолированно, при рассмотрении их наряду с другими аспектами могут указать на отрицательные тенденции, грозящие перерасти в крупные недостатки, если они не будут своевременно устранены.

6. Меры обеспечения информационной безопасности

Все меры обеспечения безопасности информационных систем МБДОУ № 47 подразделяются на:

6.1. Законодательные (правовые) меры защиты

К правовым мерам защиты относятся действующие в стране законы, указы и нормативные акты, регламентирующие правила обращения с информацией, закрепляющие права и обязанности участников информационных отношений в процессе их обработки и использования, а также устанавливающие ответственность за нарушения этих правил. Правовые меры защиты носят в

основном упреждающий, профилактический характер и требуют постоянной разъяснительной работы с пользователями и обслуживающим персоналом информационных систем МБДОУ № 47.

6.2. Морально-этические меры защиты

К морально-этическим мерам относятся нормы поведения, которые традиционно сложились или складываются по мере распространения информационных технологий в обществе. Эти нормы большей частью не являются обязательными, как законодательно утвержденные нормативные акты, однако, их несоблюдение может привести к падению авторитета, престижа человека, группы лиц или МБДОУ № 47 в целом. Морально-этические нормы бывают как неписаные, так и писаные, то есть оформленные в некоторый свод (устав) правил или предписаний. Морально-этические меры защиты являются профилактическими и требуют постоянной работы по созданию здорового морального климата в коллективе.

6.3. Технологические меры защиты

К данному виду мер защиты относятся разного рода технологические решения и приемы, основанные на использовании некоторых видов избыточности (структурной, функциональной, информационной, временной и т.п.) и направленные на уменьшение возможности совершения сотрудниками ошибок и нарушений в рамках предоставленных им прав и полномочий.

6.4. Организационные (административные) меры защиты

Организационные (административные) меры защиты - это меры организационного характера, регламентирующие процессы функционирования системы обработки информации, использование ее ресурсов, деятельность обслуживающего персонала, а также порядок взаимодействия пользователей с системой таким образом, чтобы в наибольшей степени затруднить или исключить возможность реализации угроз безопасности или снизить размер потерь в случае их реализации.

6.5. Формирование политики безопасности

Главная цель административных мер, предпринимаемых на высшем управленческом уровне - сформировать политику в области обеспечения безопасности информации (отражающую подходы к защите информации) и обеспечить ее выполнение, выделяя необходимые ресурсы и контролируя состояние дел.

С практической точки зрения политику в области обеспечения безопасности информации в МБДОУ № 47 целесообразно разбить на два уровня. К верхнему уровню относятся решения руководства, затрагивающие деятельность МБДОУ № 47 в целом. Политика верхнего уровня должна четко очертить сферу влияния и ограничения при определении целей безопасности информации, определить какими ресурсами (материальными, структурными, организационными) они будут достигнуты, и найти разумный компромисс между приемлемым уровнем безопасности и функциональностью.

Политика нижнего уровня, определяет процедуры, и правила достижения целей и решения задач безопасности информации и детализирует (регламентирует) эти правила:

– каковы роли и обязанности должностных лиц, отвечающие за проведение политики безопасности информации;

– кто имеет права доступа к информации, кто и при каких условиях может читать и модифицировать информации и т.д.

Политика нижнего уровня должна:

– предусматривать регламент информационных отношений, исключающих возможность произвольных, монопольных или несанкционированных действий в отношении информационных ресурсов;

– определять коалиционные и иерархические принципы и методы разделения секретов и разграничения доступа к информации;

– выбирать программно-технические (аппаратные) средства противодействия НСД, аутентификации, авторизации, идентификации и других защитных механизмов, обеспечивающих гарантии реализации прав и ответственности субъектов информационных отношений.

6.6. Регламентация доступа в помещения

Компоненты информационных систем должны размещаться в помещениях, находящихся под охраной или наблюдением, исключающим возможность бесконтрольного проникновения в помещения посторонних лиц и обеспечивающим физическую сохранность находящихся в помещении защищаемых ресурсов (документов, АРМ и т.п.). Уборка таких помещений должна производиться в присутствии ответственного сотрудника, за которым закреплены данные компоненты, с соблюдением мер, исключающих доступ посторонних лиц к защищаемым информационным ресурсам.

Все посторонние лица допускаются в помещения с компонентами информационной системы только в присутствии сотрудников Управления.

По окончании рабочего дня, помещения, в которых размещаются компоненты информационных систем МБДОУ № 47, должны запираться на ключ, по возможности опечатываться.

В случае оснащения помещений средствами охранной сигнализации, а также автоматизированной системой приема и регистрации сигналов от этих средств, прием-сдача таких помещений под охрану осуществляется на основании специально разрабатываемой инструкции.

6.7. Регламентация допуска сотрудников к использованию информационных ресурсов

В рамках разрешительной системы (матрицы) доступа устанавливается: кто, кому, какую информацию и для какого вида доступа может предоставить и при каких условиях.

Допуск пользователей к работе с информационными системами и доступ к их ресурсам должен быть строго регламентирован. Любые изменения состава и полномочий пользователей подсистем должны производиться установленным порядком.

Уровень полномочий каждого пользователя определяется индивидуально, соблюдая следующие требования:

– каждый сотрудник пользуется только предписанными ему правами по отношению к информации, с которыми ему необходима работа в соответствии с должностными обязанностями. Расширение прав доступа и предоставление доступа к дополнительным информационных ресурсам, в обязательном порядке, должно согласовываться с администратором безопасности информации;

– руководитель МБДОУ № 47 имеет права на просмотр информации своих подчиненных только в установленных пределах в соответствии со своими должностными обязанностями.

Все сотрудники МБДОУ № 47 и обслуживающий персонал, должны нести персональную ответственность за нарушения установленного порядка обработки информации, правил хранения, использования и передачи находящихся в их распоряжении защищаемых ресурсов системы. Каждый сотрудник (при приеме на работу) должен подписывать обязательство о соблюдении и ответственности за нарушение установленных требований по сохранению информации МБДОУ № 47.

Обработка ПДн в компонентах информационных систем **МБДОУ № 47** должна производиться в соответствии с утвержденными технологическими инструкциями.

6.8. Регламентация процессов обслуживания и осуществления модификации аппаратных и программных ресурсов

В целях поддержания режима информационной безопасности аппаратно-программная конфигурация автоматизированных рабочих мест сотрудников Управления, с которых возможен доступ к ресурсам информационной системы, должна соответствовать кругу возложенных на данных пользователей функциональных обязанностей.

В компонентах информационной системы и на рабочих местах пользователей должны устанавливаться и использоваться лицензионные программные средства.

6.9. Обеспечение и контроль физической целостности (неизменности конфигурации) аппаратных ресурсов

Оборудование информационных систем, используемое для доступа и хранения информации, к которому доступ обслуживающего персонала в процессе эксплуатации не требуется, после наладочных, ремонтных и иных работ, связанных с доступом к его компонентам должно закрываться.

6.10. Подбор и подготовка персонала, обучение пользователей

Пользователи информационных систем МБДОУ № 47, а также руководящий и обслуживающий персонал должны быть ознакомлены со своим уровнем полномочий, а также организационно-распорядительной, нормативной, технической и эксплуатационной документацией, определяющей требования и порядок обработки информации в МБДОУ № 47.

Обеспечение безопасности информации возможно только после выработки у пользователей определенной культуры работы, т.е. норм, обязательных для исполнения всеми, кто работает с информационными ресурсами Управления. К таким нормам можно отнести запрещение любых умышленных или неумышленных действий, которые нарушают нормальную работу компонентов информационных систем, вызывают дополнительные затраты ресурсов, нарушают

целостность хранимой и обрабатываемой информации, нарушают интересы законных пользователей, владельцев или собственников.

Все пользователи информационных систем должны быть ознакомлены с организационно - распорядительными документами по обеспечению безопасности информации (ПДн) МБДОУ № 47, в части, их касающейся, должны знать и неукоснительно выполнять инструкции и знать общие обязанности по обеспечению безопасности информации. Доведение требований указанных документов до лиц, допущенных к обработке защищаемой информации, должно осуществляться под роспись.

6.11. Ответственность за нарушения установленного порядка пользования ресурсами информационной системы

Мера ответственности персонала за действия, совершенные в нарушение установленных правил обеспечения безопасной работы с информацией, должна определяться нанесенным ущербом, наличием злого умысла и другими факторами по усмотрению руководства МБДОУ № 47.

Для реализации принципа персональной ответственности пользователей за свои действия необходимы:

– индивидуальная идентификация пользователей и инициированных ими процессов, т.е. установление за ними идентификатора (login, Username), на базе которого будет осуществляться разграничение доступа в соответствии с принципом обоснованности доступа;

– проверка подлинности пользователей (аутентификация) на основе паролей;

– реакция на попытки несанкционированного доступа (сигнализация, блокировка и т.д.).

6.12. Средства обеспечения безопасности информации

Для обеспечения информационной безопасности используются следующие средства защиты:

Физические средства защиты

Физические меры защиты основаны на применении разного рода механических, электронных или электронно-механических устройств и сооружений, специально предназначенных для создания физических препятствий на возможных путях проникновения и доступа потенциальных нарушителей к компонентам системы и защищаемой информации, а также технических средств визуального наблюдения, связи и охранной сигнализации.

Для обеспечения физической безопасности компонентов информационных систем необходимо осуществлять ряд организационных и технических мероприятий, включающих: проверку оборудования, предназначенного для обработки информации, на:

– наличие специально внедренных закладных устройств;

– введение дополнительных ограничений по доступу в помещения, предназначенные для хранения и обработки информации;

– оборудование систем информатизации устройствами защиты от сбоев электропитания и помех в линиях связи.

Технические средства защиты

Технические (аппаратно-программные) меры защиты основаны на использовании различных электронных устройств и специальных программ и выполняющих (самостоятельно или в комплексе с другими средствами) функции защиты (идентификацию и аутентификацию пользователей, разграничение доступа к ресурсам, регистрацию событий, криптографическое закрытие информации и т.д.).

С учетом всех требований и принципов обеспечения безопасности информации по всем направлениям защиты в состав системы защиты должны быть включены следующие средства:

– средства разграничения доступа к данным;

– средства регистрации доступа к компонентам информационной системы и контроля за использованием информации;

– средства реагирования на нарушения режима информационной безопасности.

На технические средства защиты возлагается решение следующих основных задач:

– идентификация и аутентификация пользователей при помощи имен или специальных аппаратных средств;

– регламентация и управление доступом пользователей в помещения, к физическим и логическим устройствам;

– защита от проникновения компьютерных вирусов и разрушительного воздействия вредоносных программ;

– регистрация всех действий пользователя в защищенном журнале, наличие нескольких уровней регистрации;

– защита данных системы защиты на файловом сервере от доступа пользователей, в чьи должностные обязанности не входит работа с информации, находящейся на нем.

Средства идентификации и аутентификации пользователей

В целях предотвращения работы с ресурсами информационных систем посторонних лиц необходимо обеспечить возможность распознавания каждого легального пользователя (или групп пользователей). Для идентификации могут применяться различного рода устройства: магнитные карточки, ключи, ключевые вставки, дискеты и т.п.

Аутентификация (подтверждение подлинности) пользователей также может осуществляться:

– путем проверки наличия у пользователей каких-либо специальных устройств (магнитных карточек, ключей, ключевых вставок и т.д.);

– путем проверки знания ими паролей;

– путем проверки уникальных физических характеристик и параметров самих пользователей при помощи специальных биометрических устройств.

Средства разграничения доступа

Зоны ответственности и задачи конкретных технических средств защиты устанавливаются исходя из их возможностей и эксплуатационных характеристик, описанных в документации на данные средства.

Технические средства разграничения доступа должны по возможности быть составной частью единой системы контроля доступа:

– на контролируемую территорию;

– в отдельные помещения;

– к компонентам информационной среды и элементам системы защиты ПДн (физический доступ);

– к информационным ресурсам (документам, носителям информации, файлам, наборам данных, архивам, справкам и т.д.);

– к активным ресурсам (прикладным программам, задачам и т.п.);

– к операционной системе, системным программам и программам защиты.

Средства обеспечения и контроля целостности

Средства обеспечения целостности включают в свой состав средства резервного копирования, программы антивирусной защиты, программы восстановления целостности операционной среды и баз данных.

Средства контроля целостности информационных ресурсов систем предназначены для своевременного обнаружения модификации или искажения ресурсов системы. Они позволяют обеспечить правильность функционирования системы защиты и целостность хранимой и обрабатываемой информации.

Контроль целостности информации и средств защиты, с целью обеспечения неизменности информационной среды, определяемой предусмотренной технологией обработки, и защиты от несанкционированной модификации информации должен обеспечиваться:

– средствами разграничения доступа (в помещения, к документам, к носителям информации, к серверам, логическим устройствам и т.п.);

– средствами электронной подписи;

– средствами подсчета контрольных сумм (для используемого программного обеспечения).

Средства оперативного контроля и регистрации событий безопасности

Средства объективного контроля должны обеспечивать обнаружение и регистрацию всех событий (действий пользователей, попыток НСД и т.п.), которые могут повлечь за собой нарушение безопасности и привести к возникновению кризисных ситуаций. Анализ собранной средствами регистрации информации позволяет выявить факты совершения нарушений, их характер, подсказать метод его расследования и способы поиска нарушителя и исправления ситуации. Средства контроля и регистрации должны предоставлять возможности:

– ведения и анализа журналов регистрации событий безопасности (системных журналов);

– получения твердой копии (печати) журнала регистрации событий безопасности;

– упорядочения журналов, а также установления ограничений на срок их хранения;

– оперативного оповещения администратора безопасности информации о нарушениях.

При регистрации событий безопасности в журнале должна фиксироваться следующая информация:

– дата и время события;

– идентификатор субъекта, осуществляющего регистрируемое действие;

– действие (тип доступа).

6.13. Контроль эффективности системы защиты

Контроль эффективности защиты информации осуществляется с целью своевременного выявления и предотвращения утечки информации за счет несанкционированного доступа, а также предупреждения возможных специальных воздействий, направленных на уничтожение информации, разрушение средств информатизации. Контроль может проводиться привлекаемыми для этой цели организациями, имеющими лицензию на этот вид деятельности.

Оценка эффективности мер защиты информации проводится с использованием технических и программных средств контроля на предмет соответствия установленным требованиям.

Приложение № 2
к приказук приказу №26
от 24.03.2026 г .

ИНСТРУКЦИЯ
по работе пользователя в государственных, региональных и автоматизированных информационных системах, используемых в МБДОУ № 47

1. Настоящая Инструкция устанавливает порядок работы пользователя в государственных, региональных и автоматизированных информационных системах, используемых в МБДОУ № 47 (далее – ИС) и требования к действиям пользователя ИСПДн, направленным на обеспечение безопасности персональных данных (далее - ПДн) МБДОУ № 47.

Основной целью Инструкции является установление правил выполнения пользователем ИС следующих действий:

- доступа к защищаемой информации;
- работы с защищаемой информацией;
- работы с автоматизированными рабочими местами (АРМ) ИС;
- при возникновении внештатных ситуаций.

2. Порядок работы с ИСПДн

Каждый пользователь ИС имеет прямой доступ к ее элементам, в частности к своему АРМ, базе данных защищаемой информации.

Каждый пользователь перед началом работы в ИС должен пройти инструктаж по нормам безопасности информации.

Работа пользователя ИСПДн на АРМ с соблюдением норм безопасности ПДн заключается в следующем:

- при включении своего компьютера пользователь должен ввести название своей учетной записи и пароль в диалоговом окне операционной системы;
- для получения доступа к защищаемой информации в базе данных пользователь должен ввести учетную запись и пароль в диалоговое окно той программы, в которой он обрабатывает информацию или использовать ЕСИА (вариант авторизации в ИС используется в зависимости от требований безопасности конкретной ИС);
- в процессе обработки информации пользователь должен соблюдать конфиденциальность информации, к которой в данный момент он имеет доступ, т.е. не зачитывать их, не давать просматривать информацию с экрана монитора или распечаток другим лицам, никому не передавать файлы, содержащие защищаемую информацию по внутренней сети организации и по каналу Интернет, не копировать файлы, содержащие защищаемую информацию на неучтенные носители;
- описанные выше действия, кроме копирования на неучтенные носители, пользователь может совершать только по служебной необходимости, с пользователями, имеющими санкционированный доступ к защищаемой информации с соблюдением мер предосторожности;

– при прерывании обработки защищаемой информации в течение рабочего дня пользователь должен или отключится от базы данных защищаемой информации, или заблокировать рабочий стол компьютера. Для этого необходимо нажать одновременно комбинацию клавиш <Ctrl><Alt><Del> и выбрать опцию <Блокировка>;

– по окончанию обработки защищаемой информации, пользователь должен отключиться от базы данных ПДн, выключить свой компьютер, убрать со своего рабочего места все распечатки, содержащие защищаемую информацию, в место, не доступное посторонним;

– при возникновении внештатных ситуаций, таких как компрометация пароля доступа к базе защищаемой информации, возникновения необычных процессов работы компьютера, внезапном отключении компьютера, возникновении вирусного заражения, нарушающего работу компьютера, странном поведении коллег, пытающихся выведать какую-либо информацию и других подозрительных ситуаций, пользователь обязан незамедлительно сообщить о данном факте администратору информационной безопасности, который в случае необходимости созывает группу реагирования на инциденты информационной безопасности, которая оценивает инцидент и реагирует на него наиболее целесообразным и результативным способом.

3. Пользователь имеет право:

– в любой момент обратиться к администратору информационной безопасности с интересующим его вопросом по работе в ИС или за разъяснением реализации норм безопасности информации;

– доступа к такому объему информации и выполнения тех действий с ней, которые необходимы для выполнения своих должностных обязанностей;

– доступа ко всем внутренним документам и законодательным актам, регламентирующим работу с информацией и обеспечение ее безопасности.

4. Ответственность пользователей ИС

Каждый пользователь должен понимать, что за не соблюдение п.2. настоящей Инструкции влечет нарушение норм безопасности информации и вызывает потенциальную или реализуемую ее утечку.

За несоблюдение настоящей Инструкции пользователь может быть привлечен к административному наказанию в соответствии с действующим законодательством.

Приложение № 3
к приказук приказу №26
от 24.03.2026 г .

ИНСТРУКЦИЯ
по организации антивирусной защиты

1. Инструкция устанавливает требования антивирусной безопасности для информационных систем персональных данных (ИС) МБДОУ № 47 в целом и их элементов в частности.

2. Общие требования

Антивирусные средства защиты должны быть лицензионными и иметь сертификат соответствия требованиям безопасности, выданный Федеральной службой по техническому и экспортной контролю (ФСТЭК) России.

Закупка средств антивирусной защиты должна быть централизованной. Все элементы ИС рекомендуется оснащать одним антивирусным программным продуктом.

Параметры антивирусной политики задаются администратором информационной безопасности.

Реализация параметров антивирусной политики осуществляется системным администратором.

Антивирусные средства защиты должны функционировать исправно и непрерывно. При сбоях в работе требуется немедленное вмешательство системного администратора для устранения неполадок.

При выборе антивирусных средств необходимо так же учитывать его быстродействие, для того чтобы не перегружать системные процессы автоматизированного рабочего места (АРМ) и не создавать затруднений для работы пользователей ИС.

3. Параметры антивирусной политики

Основными параметрами антивирусной политики являются периодичность обновления антивирусных баз, периодичность проверки наличия/отсутствия вирусных заражений и параметры проверки «на лету» при работе в Интернете.

Обновление антивирусных баз должно осуществлять по мере выхода новых баз. Для этого необходимо настроить каждое АРМ ИС на обновление из сети Интернет.

Периодичность проверки наличия/отсутствия вирусных заражений настраивается в консоли управления антивирусным средством и применяется на каждом АРМ ИС. Данный параметр устанавливается на один раз в неделю (в любой день) на обеденный перерыв. Проверке должны подвергаться все разделы жесткого диска АРМ. На АРМ ИС такие настройки делаются непосредственно на месте системным администратором.

Параметры проверки «на лету» при работе в Интернете должны включать в себя все возможные объекты реагирования. На АРМ ИС такие настройки делаются непосредственно на месте системным администратором.

4. Порядок работы со средствами антивирусного контроля

На каждое АРМ ИС системным администратором устанавливается и настраивается антивирусное средство защиты.

Каждый пользователь АРМ ИС не должен препятствовать обновлению антивирусных баз или проверке наличия/отсутствия вирусных заражений, а также реагировать на предупреждения антивирусного средства защиты при работе в сети Интернет, если при проверке «на лету» обнаружено вредоносное программное обеспечение или вирус.

Каждый пользователь ИС в обеденный перерыв определенного дня недели, заранее оговоренного с системным администратором, должен оставлять свое АРМ во включенном состоянии, для еженедельной проверки на наличие/отсутствие вирусных заражений.

Каждый пользователь при работе со съемными носителями (дискеты, диски, USB-носители, съемные жесткие диски, карты памяти, в том числе в составе мобильного телефона) должен перед использованием носителя проверить его на наличие вирусов или вредоносного программного обеспечения. Для этого необходимо:

– подключить/вставить в системный блок своего компьютера или ноутбука носитель;

– двойным щелчком левой клавиши мыши открыть ярлык «Мой компьютер»;

– в открывшемся окне проводника найти носитель;

– одни щелчком правой клавиши мыши вызвать «выплывающее» меню и выбрать в нем проверку на вирусы. Обычно данный пункт меню имеет эмблему и название антивирусного средства, установленного на АРМ;

– дождаться окончания проверки и при отрицательном результате начать работу с носителем;

– при положительном результате проверки, при условии невозможности «вылечить» зараженный файл, пользователь должен обратится к системному администратору или администратору информационной безопасности, но не начинать работу с носителем.

Системный администратор или администратор информационной безопасности, при обращении к ним пользователей ИС с зараженными носителями должны еще раз проверить носитель, выяснить причину невозможности «вылечить» зараженный файл (например, устаревшая антивирусная база) и по возможности удалить этот файл.

Проверке на заражение также подлежат файлы, полученные по электронной почте. В данном случае достаточно одним щелчком правой клавишей мыши на файле вызвать меню и выбрать в нем проверку на вирусы. В случае если файл заражен, обратится к отправителю с просьбой повторно отправить не зараженный файл. Работа с зараженными файлами категорически запрещена.

При подозрении на вирусное заражение АРМ, пользователь должен незамедлительно сообщить об этом администратору информационной безопасности и системному администратору. Работу на компьютере необходимо приостановить, базу данных с ПДн закрыть.

Признаками вирусного заражения являются:

– работоспособность компьютера значительно снижается;

– компьютер «подвисает»;

– появляются различного рода диалоговые окна Интернет-характера;

– самопроизвольно открываются/закрываются используемые в работе проводниковые окна, файлы, программы;

– появление на экране монитора баннера рекламного или эротического характера.

5. Последствия вирусных заражений

Антивирусная безопасность ИС является неотъемлемой составной частью системы защиты информации.

Вирусное заражение одного АРМ ИС может вызвать заражение сегмента или всей локально-вычислительной системы. Такое заражение выводит из строя все АРМ. Серьезные вирусные заражения не «лечатся», и при возникновении такого заражения пользователь не имеет возможности сохранить последние данные, с которыми он работал, файлы, расположенные на жестком диске его компьютера, и восстановление работоспособности возможно только путем переустановки операционной системы. В этом случае пользователь теряет рабочее время и данные со своего компьютера.

Приложение № 4
к приказук приказу №26
от 24.03.2026 г .

ИНСТРУКЦИЯ
по применению парольной политики

1. Настоящая Инструкция устанавливает порядок работы пользователей информационных систем (далее - ИС) МБДОУ № 47 со своими учетными записями и паролями доступа и правила парольной политики, направленной на обеспечение безопасности защищаемой информации.

Основной целью Инструкции является установление правил парольной политики для пользователей ИС.

2. Общие требования

Пароли для всех учетных записей пользователей ИС должны выбираться с учетом следующих требований:

- длина пароля должна быть не менее 12 символов;
- в числе символов пароля обязательно должны присутствовать буквы и цифры;
- при смене пароля новое значение должно отличаться от предыдущего не менее чем в 4 позициях;
- пароль не должен включать в себя легко вычисляемые (угадываемые) сочетания символов (имена, фамилии, отчества, наименования АРМ, организации и т.д.), а также общепринятые сокращения (ЭВМ, ЛВС, USER, ADM, ADMIN и т.п.);
- пароль должен легко запоминаться, для этого используется некоторые приемы, например: для задания пароля используется четверостишье: «ваше благородие, госпожа удача, для кого вы добрая, для кого иначе», далее для пароля берут первые буквы «вбгудквддки» и в конце добавляется число символов – 11, таким образом, получаем пароль – вбгудквддки11;
- минимальное время применения пароля - не менее 2 дней;
- максимальное время применения пароля - не более чем 60 дней;
- пароль не должен повторяться;
- пользователь не может неправильно ввести пароль учетной записи более 3 раз, в этом случае должна происходить блокировка учетной записи пользователя, до момента снятия блокировки системным администратором, обслуживающим программы обработки персональных данных.

Смена пароля учетной записи пользователя должна проводиться регулярно и не реже одного раза в два месяца.

В случае прекращения полномочий учетной записи пользователя (увольнение, переход на другую работу, в другой отдел или помещение, а также и другие обстоятельства) учетная запись должна быть заблокирована и пароль должен быть заменен сразу после окончания последнего сеанса работы данного пользователя в ИС. Удалять учетную запись не рекомендуется, с целью возможной необходимости просмотра «лог-файлов» по данной учетной записи.

3. Требования к владельцам паролей

Пользователи обязаны хранить свой личный пароль в тайне от других и не передавать любым способом пароль никому.

Хранение пользователем значений своих паролей на бумажном носителе допускается только в запираемых ящиках столов, сейфах или других труднодоступных местах. Хранение бумажных носителей паролей в доступных местах (под клавиатурой, на мониторе и т.д.) категорически запрещено.

В случае компрометации личного пароля пользователь ИС должен немедленно предпринять меры, указанные в п.4 настоящей Инструкции.

4. Компрометация паролей

Пользователь при компрометации или подозрении на компрометацию своего пароля, утере личного идентификатора обязан без промедления сообщить об этом администратору информационной безопасности в устной форме.

Администратор информационной безопасности должен провести следующие мероприятия:

– взять объяснительную в письменном виде с пользователя, обнаружившего компрометацию пароля. Объяснительная пишется на имя руководителя и должна содержать ФИО, должность пользователя, описание обстоятельств, при которых была обнаружена компрометация, утеря личного идентификатора или описание причин подозрения на компрометацию, последние действия, проведенные в автоматизированной системе, личную подпись пользователя;

– запросить у системного администратора внеочередную смену пароля пользователя или при утере личного идентификатора блокировку учетной записи пользователя, для предотвращения использования злоумышленником данной учетной записи;

– запросить у системного администратора журнал операций в автоматизированной системе по пользователю ИС и проанализировать его;

– в случае выявления действий, не указанных пользователем в объяснительной, проводится служебное расследование по выяснению причин компрометации пароля с целью выработки новых или совершенствования принятых технических и организационных мер по устранению такой угрозы в будущем, а также выяснению величины нанесенного ущерба безопасности информации;

– в случае не обнаружения никаких признаков использования пароля или идентификатора пользователя в несанкционированных целях, составляется Акт об отсутствии нарушений при использовании пароля. К Акту подшивается объяснительная пользователя;

– акты и документы по служебным расследованиям хранятся у администратора информационной безопасности в течение двух лет, затем подлежат уничтожению.

5. Проверка соблюдения парольной политики

Администратором информационной безопасности, в соответствии с Планом мероприятий по обеспечению защиты информации, проводится периодическая проверка выполнения пользователями ИС парольной политики.

Проверка проводится на местах. Количество проверяемых пользователей и периодичность проверки определяется администратором информационной безопасности самостоятельно.

В ходе проверки проверяется знание пользователями парольной политики и места хранения бумажных носителей паролей, а также периодичность смены пароля, если эта функция не выполняется в автоматическом режиме.

Результаты проверки фиксируются в Акте проверки.

В случае выявления нарушений к пользователю могут быть применены меры наказания, на усмотрение руководителя.

Приложение № 5
к приказук приказу №26
от 24.03.2026 г .

ПЕРЕЧЕНЬ
информационных систем в управлении образования администрации города Коврова для обработки персональных данных и сопутствующей информации, не составляющей государственную тайну

1. Государственная информационная система Владимирской области «Региональный сегмент единой федеральной межведомственной системы учета контингента обучающихся по основным образовательным программам и дополнительным общеобразовательным программам» (в том числе модули системы: АИС «Электронная школа», АИС «Питание», АИС «Электронный детский сад», АИС «Электронное учреждение дополнительного образования», АИС «Навигатор дополнительного образования», АИС «Электронное и дистанционное обучение»). Предназначена для обработки персональных данных и сопутствующей информации, не составляющей государственную тайну, об участниках образовательных отношений.
2. ФГИС Моя школа
3. ФИС ФРДО

Приложение № 6
к приказук приказу №26
от 24.03.2026 г .

ПОЛОЖЕНИЕ
по защите информации в государственной информационной системе «Региональный сегмент единой федеральной межведомственной системы учета контингента обучающихся по основным образовательным программам и дополнительным общеобразовательным программам»

1. Положение по защите информации в государственной информационной системе «Региональный сегмент единой федеральной межведомственной системы учета контингента обучающихся по основным образовательным программам и дополнительным общеобразовательным программам» (далее – Положение) МБДОУ № 47 (далее – МБДОУ № 47) разработано в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» и Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и защите информации», законами, указами, постановлениями, другими нормативными документами действующего законодательства Российской Федерации.

Настоящее Положение определяет нормы защиты информации и персональных данных (ПДн) и ответственность за нарушения установленных норм.

2. Целью настоящего Положения является обеспечение безопасности ПДн и сопутствующей информации, не составляющей государственную тайну, о родившихся и зарегистрированных по месту жительства обучающихся, в том числе сведения обо всех этапах обучения детей.

3. Настоящий документ обязаны знать и выполнять установленные им нормы все сотрудники МБДОУ № 47, имеющие отношение к государственной информационной системе «Региональный сегмент единой федеральной межведомственной системы учета контингента обучающихся по основным образовательным программам и дополнительным общеобразовательным программам» (далее – ГИС РС «Контингент»).

3. Состав защищаемой информации приведен в Перечне защищаемой информации (пункт 1 приложения к Положению).

4. Обработка ПДн и информации

Управление выполняет проверку полноты и актуальности занесенных в ГИС РС «Контингент» данных по бумажным отчетам, предоставляемым образовательными организациями, подведомственными Управлению (школы, детские сады, учреждения дополнительного образования) (далее - ОО). В случае ошибок осуществляют контроль за дополнением ГИС РС «Контингент» со стороны ОО.

5. Доступ к ПДн и информации

Доступ к защищаемой информации имеют сотрудники МБДОУ № 47 в соответствии с Матрицей доступа к защищаемой информации, утвержденной руководителем МБДОУ № 47.

Сотрудники МБДОУ № 47 имеют только права чтения защищаемой информации.

6. Передача ПДн и информации

Защищаемая информация консолидируется на серверах в БД в ГАОУ ДПО ВО ВИРО по защищенному каналу, построенному на базе криптографического комплекса ViPNet Client for Windows 4.5

7. Основные нормы безопасности ПДн при распределении полномочий доступа

Каждый сотрудник МБДОУ № 47, имеющий отношение к ПДн, должен быть наделен минимальными полномочиями обработки ПДн, необходимыми для выполнения своих обязанностей.

Каждый сотрудник МБДОУ № 47, имеющий отношение к ПДн, обязан знать и выполнять установленные нормы безопасности ПДн.

8. Нормы безопасности при обработке ПДн

При обработке ПДн на бумажных носителях необходимо соблюдать следующие меры безопасности:

– бумажные носители, находящиеся в работе, не должны оставаться без присмотра сотрудника, работающего с ними;

– передача бумажных носителей между подразделениями Управления возможна только тем сотрудникам, которые имеют санкционированный доступ к ним, в соответствии со списками таких сотрудников;

– хранение бумажных носителей должно осуществляться в местах, не доступных посторонним лицам, а также сотрудникам МБДОУ № 47, не имеющим санкционированного доступа к ним;

– в отношении каждого вида бумажных носителей должны быть определены сроки хранения и методы уничтожения;

– при передаче бумажных носителей на долгосрочное хранение в архив, к ним применяются нормы безопасности, установленные владельцем архива.

При обработке ПДн в ГИС РС «Контингент» необходимо соблюдать следующие меры безопасности:

– каждый сотрудник МБДОУ № 47, обрабатывающий ПДн в ГИС РС «Контингент», должен иметь свою учетную запись и пароль к ней;

– сотрудникам запрещается передавать пароли на учетные записи между собой и кому-либо вообще;

– каждый сотрудник при обнаружении компрометации своего пароля должен незамедлительно сообщить об этом администратору информационной безопасности;

– вход в модули ГИС РС «Контингент» осуществляется с использованием Единой системы идентификации и аутентификации (далее – ЕСИА);

– каждое автоматизированное рабочее место ГИС РС «Контингент» должно быть оснащено сертифицированными средствами защиты в программном или программно-аппаратном исполнении;

- защита ГИС РС «Контингент» должна быть комплексной и охватывать все возможные каналы утечки ПДн (угрозы техногенного характера, стихийные бедствия, несанкционированный доступ разного рода, воздействия из внешний сетей и т.д.);

- необходимо соблюдение организационных мероприятий при защите ГИС РС «Контингент» в целом и отдельных элементов. К организационным мероприятиям относятся: контроль со стороны сотрудников, работающих в ГИС РС «Контингент», за нахождением в кабинете посторонних лиц, а также сотрудников, не имеющих санкционированного доступа к ПДн, просмотр ПДн с экрана монитора, доступ к автоматизированному рабочему месту, работа с ПДн;

– при обработке критичных ПДн, необходима аттестация ГИС РС «Контингент».

9. Нормы безопасности при передаче ПДн

Передача ПДн по телефону, факсу запрещена.

Ответы на письменные запросы других организаций и учреждений в пределах их компетенции и предоставленных полномочий даются в письменной форме на бланке Управления и в том объеме, который позволяет не разглашать излишний объем персональных сведений о носителях ПДн.

Предоставление ПДн в другие организации без письменного запроса или при превышении их компетенции, действий вне рамок законодательных актов, запрещено.

При передаче по открытым каналам связи (например, Интернет, в том числе и по электронной почте) должны использоваться сертифицированные криптографические средства защиты.

10. Сотрудники Управления, имеющие доступ к ПДн несут персональную ответственность за сохранение конфиденциальности, целостности вверенных им ПДн и исполнение настоящего Положения.

Лица, виновные в нарушении установленных норм, несут дисциплинарную, гражданско-правовую, административную или уголовную ответственность в соответствии с законодательными актами.

Контроль за исполнением Положения осуществляет ответственный за организацию обработки ПДн.

Приложение к Положению
по защите информации в государственной информационной системе «Региональный сегмент единой федеральной межведомственной системы учета контингента обучающихся по основным образовательным программам и дополнительным общеобразовательным программам»

1. Перечень защищаемой информации в государственной информационной системе «Региональный сегмент единой федеральной межведомственной системы учета контингента обучающихся по основным образовательным программам и дополнительным общеобразовательным программам»

Перечень персональных данных и сопутствующей информации, обрабатываемых с использованием средств автоматизации в государственной информационной системе «Региональный сегмент единой федеральной межведомственной системы учета контингента обучающихся по основным образовательным программам и дополнительным общеобразовательным программам»:

Название автоматизированной системы	Перечень защищаемой информации	Категория субъекта
АИС «Электронная школа» (модуль «БАРС Образование»), в том числе модуль АИС «Питание»	ФИО Дата и место рождения Логин Пароль Специализация Сведения о месте работы Дата приема на работу Должность Дата вступления в должность Пол Семейное положение Сведения о документе, удостоверяющем личность (серия, номер, кем выдан, дата выдачи) Гражданство Телефон Email Адрес регистрации и места проживания ИНН СНИЛС Образование Повышение квалификации и курсовая подготовка Сведения о квалификации Научная степень Сведения о категории, в том числе педагогической с указанием даты установления	Сотрудники образовательных организаций

Название автоматизированной системы	Перечень защищаемой информации	Категория субъекта
	Сведения о стаже работы (общий стаж работы, педагогический стаж) Сведения об отпуске по уходу за ребенком Совместительство Занятость Обеспеченность жильем Награды и достижения	
	ФИО Дата и место рождения Логин Пароль Сведения об учебном заведении Класс Дата зачисления Пол Сведения о документе, удостоверяющем личность (серия, номер, кем выдан, дата выдачи) Гражданство СНИЛС Телефон Email Номер личного дела Адрес регистрации и места проживания Статус семьи Социальный статус Льготная категория Информация об организации питания История обучения, успеваемость, форма обучения, потребность в адаптированных образовательных программах, вид программы Награды и достижения Результаты экзаменов Сведения о постановке на виды учета Сведения о состоянии здоровья, физическая подготовка Сведения об ограничении возможностей, инвалидности Планируемое место продолжения учебы	Ученики образовательных организаций
	ФИО Дата рождения Логин Пароль Тип родства СНИЛС Сведения о документе, удостоверяющем личность (серия, номер, кем выдан, дата выдачи) Гражданство Льготная категория ФИО ребенка Дата рождения ребенка	Родители (законные представители) учеников образовательных организаций

Название автоматизированной системы	Перечень защищаемой информации	Категория субъекта
	Email Телефон Место работы Статус	
АИС «Электронный детский сад» (модуль «БАРС Образование»)	ФИО дата и место рождения сведения о месте работы дата приема на работу должность пол сведения о документе, удостоверяющем личность (серия, номер, кем выдан, дата выдачи) гражданство телефон адрес образование сведения о квалификации общий стаж работы педагогический стаж СНИЛС Награды и достижения	Сотрудники образовательных организаций
	ФИО дата и место рождения сведения о дошкольном учреждении возрастная группа дата зачисления пол сведения о свидетельстве о рождении (серия, номер, дата выдачи, номер актовой записи, дата создания актовой записи, место государственной регистрации) СНИЛС место рождения гражданство адрес регистрации по месту жительства адрес фактического проживания статус семьи сведения об ограничении возможностей в здоровье количество детей в семье сведения о получении компенсации за присмотр и уход льготная категория группа здоровья наличие потребности в АОП, вид АОП	Воспитанники образовательных организаций
	ФИО тип представителя дата и место рождения телефон Email СНИЛС	Родители (законные представители) воспитанников образовательных организаций

Название автоматизированной системы	Перечень защищаемой информации	Категория субъекта
	Сведения о документе, удостоверяющем личность (серия, номер, кем выдан, дата выдачи) гражданство адрес регистрации адрес фактического проживания дополнительные данные по родителям (законным представителям): смерть, место смерти, дата смерти, реквизиты документа, удостоверяющего смерть	
АИС «Электронное учреждение дополнительного образования» (модуль «БАРС Образование»)	ФИО Дата и место рождения Логин Пароль Сведения об учебном заведении Дата приема на работу Должность Пол Сведения о документе, удостоверяющем личность (серия, номер, кем выдан, дата выдачи) Гражданство Телефон E-mail СНИЛС Адрес регистрации Адрес фактического проживания Образование Сведения о квалификации Научная степень Совместительство Занятость Награды и достижения	Сотрудники образовательных организаций
	ФИО Дата рождения Логин Пароль Пол Сведения об учебном заведении Наименование группы Дата начала обучения в группе Сведения о документе, удостоверяющем личность (серия, номер, кем выдан, дата выдачи) Место рождения Телефон E-mail СНИЛС Адрес регистрации и места проживания История обучения, достижения Сведения об ограничении возможностей	Обучающиеся образовательных организаций
	Сведения о сертификате ПФДО	

Название автоматизированной системы	Перечень защищаемой информации	Категория субъекта
	ФИО Дата рождения СНИЛС Логин Пароль Тип законного представителя /родства Сведения о документе, удостоверяющем личность (серия, номер, кем выдан, дата выдачи) ФИО ребенка Дата рождения ребенка Логин ребенка E-mail Телефон Место работы Статус	Родитель (законный представитель) обучающегося
АИС «Навигатор дополнительного образования»	ФИО Должность	Сотрудники образовательных организаций
	ФИО Дата рождения Логин Пароль Пол Сведения о документе, удостоверяющем личность (серия, номер, кем выдан, дата выдачи) Сведения об учебном заведении Номер сертификата ПФДО Наименование программы Наименование группы Дата начала и окончания обучения в группе Адрес регистрации по месту жительства Адрес регистрации по месту пребывания	Обучающиеся образовательных организаций
	ФИО Дата рождения Пол E-mail Телефон Сведения о документе, удостоверяющем личность (серия, номер, кем выдан, дата выдачи)	Родители (законные представители) обучающихся
АИС «Электронное и дистанционное обучение»	ФИО Логин Пароль Город/страна проживания Сведения об учебном заведении Наименование курса Дата создание курса Роль в сообществе	Сотрудники образовательных организаций

Название автоматизированной системы	Перечень защищаемой информации	Категория субъекта
	ФИО Логин Пароль Город/страна проживания Сведения об учебном заведении Наименование курса Дата создание курса Роль в сообществе Оценка (при наличии)	Обучающиеся образовательных организаций
ИС «Муниципальный сегмент ГИС РС «Контингент»	I. Общие сведения о контингенте обучающихся: 1. ФИО; 2. Дата рождения (формат dd.mm.yyyy); 3. Место рождения 4. Пол 5. СНИЛС 6. Гражданство 7. Реквизиты свидетельства о рождении 7.1 Серия и номер 7.2 Дата выдачи 7.3 Кем выдан 7.4. Номер актовой записи 8. Реквизиты документа, удостоверяющего личность (далее – ДУЛ) 8.1 Тип ДУЛ 8.2 Серия и номер 8.3 Дата и место выдачи 8.4 Кем выдан 9. Адрес регистрации по месту жительства 10. Адрес регистрации по месту пребывания 11. Адрес фактического места жительства 12. Информация о трудной жизненной ситуации II. Информация о здоровье 1. Группа состояния здоровья 2. Медицинская группа для занятия физической культурой 3. Инвалидность: 3.1 Группа инвалидности 3.2 Срок действия группы инвалидности 3.3. Причины инвалидности 4. Наличие потребности в адаптированной программе обучения 5. Наличие потребности в длительном лечении 6. Физическая подготовка III. Информация об образовании 1. Организация образования субъекта Российской Федерации; 2. Заявление о приеме: 2.1. Учебный класс; 2.2. Дата регистрации заявления о приеме; 3. Зачисление: 3.1. Учебный год; 3.2. Учебный класс;	Учащийся

Название автоматизированной системы	Перечень защищаемой информации	Категория субъекта
	3.3. Дата зачисления; 3.4. Реквизиты распорядительного акта о зачислении; 4. Образовательная программа: 4.1. Уровень; 4.2. Адаптированность; 5. Обучение: 5.1. Перевод (зачисление) в учебные классы: 5.1.1. Учебный год; 5.1.2. Учебный класс; 5.2. Годовая успеваемость: 5.2.1. Предмет; 5.2.2. Учебный год; 5.2.3. Оценка (при наличии); 5.3. Форма получения образования и форма обучения; 5.4. Смена; 6. Портфолио: 6.1. Участие в мероприятиях (олимпиадах, конкурсах, соревнованиях и т.д.): 6.1.1. Название мероприятия; 6.1.2. Статус мероприятия; 6.1.3. Дата участия; 6.1.4. Результаты участия; 6.1.5. Присвоены разряды, звания; 6.2. Прочие достижения; 7. Результаты обучения по основным общеобразовательным программам: 7.1. Государственная итоговая аттестация (ГИА) в форме основного государственного экзамена (ОГЭ): 7.1.1. Предмет; 7.1.2. Баллы; 7.2. Государственная итоговая аттестация (ГИА) в форме государственного выпускного экзамена (ГВЭ): 7.2.1. Предмет; 7.2.2. Баллы; 7.3. Реквизиты аттестата об образовании; 7.4. Итоговая успеваемость: 7.4.1. Предмет; 7.4.2. Оценка; 8. Результаты обучения по программе среднего общего образования: 8.1. Государственная итоговая аттестация (ГИА) в форме единого государственного экзамена (ЕГЭ): 8.1.1. Предмет; 8.1.2. Баллы; 8.2. Государственная итоговая аттестация (ГИА) в форме государственного выпускного экзамена (ГВЭ):	

Название автоматизированной системы	Перечень защищаемой информации	Категория субъекта
	8.2.1. Предмет; 8.2.2. Баллы; 8.3. Реквизиты аттестата об образовании; 8.4. Итоговая успеваемость: 8.4.1. Предмет; 8.4.2. Оценка; 9. Окончание (отчисление, выбытие) организации образования субъекта Российской Федерации: 9.1. Дата окончания (отчисления, выбытия); 9.2. Основание окончания (отчисления, выбытия); 9.3. Реквизиты документа об окончании (отчисления, выбытия). 10. Льготная категория 11. Сведения о сертификате ПФДО	
	Родители (или иные законные представители): 1 Мать: 1.1 ФИО; 1.2 Дата рождения (формат dd.mm.yyyy); 1.3 СНИЛС; 1.4 Гражданство 1.5 Реквизиты документа, удостоверяющего личность; 2 Отец: 2.1 ФИО; 2.2 Дата рождения (формат dd.mm.yyyy); 2.3 СНИЛС; 2.4 Гражданство 2.5 Реквизиты ДУЛ 3 Законный представитель, не являющийся родителем: 3.1 Тип законного представителя: 3.2 ФИО; 3.3 Дата рождения; 3.4 СНИЛС; 3.5 Гражданство 3.6 Реквизиты документа, удостоверяющего личность 3.7 Документ, удостоверяющий положение законного представителя по отношению к ребенку. 3.6.1 Тип документа, удостоверяющий положение законного представителя по отношению к ребенку 3.6.2 Серия документа, удостоверяющий положение законного представителя по отношению к ребенку 3.6.3 Номер документа, удостоверяющий положение законного представителя по отношению к ребенку	Родитель (законный представитель)

2. Правила обработки защищаемой информации в государственной информационной системе «Региональный сегмент единой федеральной межведомственной системы учета контингента обучающихся по основным образовательным программам и дополнительным общеобразовательным программам»

2.1.Настоящие Правила обработки защищаемой информации в государственной информационной системе «Региональный сегмент единой федеральной межведомственной системы учета контингента обучающихся по основным образовательным программам и дополнительным общеобразовательным программам» (далее - Правила), содержащей в том числе персональные данные (ПДн), разработаны с учетом Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» и постановления Правительства РФ от 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных ФЗ «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами».

2.2.Настоящие Правила устанавливают процедуры, направленные на выявление и предотвращение нарушений законодательства РФ в сфере конфиденциальной информации и ПДн в МБДОУ № 47 (далее по тексту – МБДОУ № 47).

2.3. Настоящие Правила определяют содержание обрабатываемых ПДн и сопутствующей информации, категории субъектов ПДн, срок их обработки и хранения, порядок уничтожения в государственной информационной системе «Региональный сегмент единой федеральной межведомственной системы учета контингента обучающихся по основным образовательным программам и дополнительным общеобразовательным программам».

2.4. Исходные данные

Параметры	**Обучающиеся субъекты, родившиеся и зарегистрированные по месту жительства**
Цель обработки	Выполнение деятельности МБДОУ № 47
Содержание ПДн и сопутствующей информации	См. Перечень защищаемой информации
Срок обработки ПДн	Постоянно
Срок хранения ПДн	Не хранятся в МБДОУ № 47
Порядок уничтожения ПДн	Электронные носители – путем форматирования и физического повреждения без возможности восстановления данных.

2.5. Правила обработки информации

2.5.1. В отношении каждой категории субъектов должны быть определены отдельные места хранения носителей ПДн.

2.5.2. Любой сотрудник, работающий с ПДн, должен получать только минимально необходимый уровень доступа к ПДн.

2.5.3. Все сотрудники, работающие с ПДн должны пройти инструктаж, знать и соблюдать требования МБДОУ № 47 по обеспечения безопасности ПДн.

2.5.4. Обработка ПДн с использованием средств автоматизации должна проводиться с учетом:

– соблюдения Политики МБДОУ № 47 в отношении обработки ПДн;

– соблюдения Положения по защите информации;

– антивирусной политики, приведенной в Инструкции по организации антивирусной защиты государственной информационной системы (далее - ГИС);

– парольной политики, приведенной в Инструкции по применению парольной политики в ГИС;

– правил работы со съемными носителями, приведенными в Инструкции по работе со съемными носителями.

3. Перечень помещений, в которых обрабатывается защищаемая информация государственной информационной системы «Региональный сегмент единой федеральной межведомственной системы учета контингента обучающихся по основным образовательным программам и дополнительным общеобразовательным программам», и доступ к ним

3.1. МБДОУ № 47 (далее по тексту – МБДОУ № 47) расположено по адресу: г. Ковров, ул. Гастелло дом 11 / главный корпус
ул. Киркижа дом 22 / корпус № 2

3.2. Для размещения элементов государственной информационной системы Владимирской области «Региональный сегмент единой федеральной межведомственной системы учета контингента обучающихся по основным образовательным программам и дополнительным общеобразовательным программам» используется кабинет № …. на ……. этаже ……. здания.

4. Разрешительная система (матрица) доступа к защищаемой информации, обрабатываемой на автоматизированном рабочем месте МБДОУ № 47, предназначенного для подключения к защищенной сети передачи данных системы образования Владимирской области

4.1. Разрешительная система (матрица) доступа предназначена для разграничения доступа к защищаемым ресурсам государственной информационной системы Владимирской области «Региональный сегмент единой федеральной межведомственной системы учета контингента обучающихся по основным образовательным программам и дополнительным общеобразовательным программам» МБДОУ № 47 (далее по тексту – МБДОУ № 47).

4.2. Пользователи ГИС:

№	ФИО	Должность	Подразделение	Наименование рабочих станций, к работе на которых допущен пользователь	Группа, в которую входит сотрудник
1.				АРМ «……»	Пользователь ГИС Администратор информационной безопасности
2.					Пользователь ГИС
3.					Пользователь ГИС
4.					Пользователь ГИС
5.					Пользователь ГИС
6.					Системный администратор

4.3. Информационные объекты доступа:

№	Наименование средства (системы ресурса)		Носители информации
1.	АИС «Электронная школа» (модуль БАРС Образование), в том числе модуль АИС «Питание»	Microsoft Office 2021	НМНИ АРМ «BARS», НМНИ и вычислительные ресурсы ГАОУ ДПО ВИРО
2.	АИС «Электронный детский сад» (модуль БАРС Образование)		
3.	АИС «Электронное учреждение дополнительного образования» (модуль БАРС Образование)		
4.	АИС «Навигатор дополнительного образования»		
5.	АИС «Электронное и дистанционное обучение»		
6.	ИС «Муниципальный сегмент ГИС РС «Контингент»		

4.4. Технические объекты доступа:

№	Наименование средства (системы ресурса)	Назначение средства	Носители информации
1.	НМНИ	Хранение информации в электронном виде	НМНИ АРМ «BARS» НМНИ ГАОУ ДПО ВИРО

4.5. Субъекты доступа:

№	Наименование группы	Описание группы (задачи группы)	Уровень доступа к ПДн	Разрешенные действия с защищаемой информацией	Рабочие станции группы
1.	Системные администраторы	Администрирование рабочих станций, серверов и прикладного программного обеспечения ГИС	-	-	АРМ «BARS»

№	Наименование группы	Описание группы (задачи группы)	Уровень доступа к ПДн	Разрешенные действия с защищаемой информацией	Рабочие станции группы
2.	Пользователи ГИС	Обработка и хранение защищаемой информации	Пользователь	Чтение, запись, модификация, удаление, передача	АРМ «BARS»
3.	Администраторы информационной безопасности	Контроль выполнения организационных требований по безопасности, а также правильного использования средств защиты	-	-	АРМ «BARS»

4.6. Матрица доступа на сетевом уровне ГИС представлена одним АРМ.

4.7. Разрешительная система на уровне приложений:

№	Группы доступа	Наименование ресурса					
		АС[1]	АС[2]	АС[3]	АС[4]	АС[5]	АС[6]
1.	Системные администраторы	+	+	+	+	+	+
2.	Пользователи ГИС	+	+	+	+	+	+
3.	Администраторы информационной безопасности	-	-	-	-	-	-

4.8. Перечень должностей, замещение которых предусматривает осуществление обработки защищаемой информации либо осуществление доступа к ней

- Старший воспитатель Титова О.Н.
- Зам зав по АХР Пирог О.А
- Делопроизводитель Склярова Л.В.

[1] АИС «Электронная школа» (модуль БАРС Образование), в том числе модуль АИС «Питание»
[2] АИС «Электронный детский сад» (модуль БАРС Образование)
[3] АИС «Электронное учреждение дополнительного образования» (модуль БАРС Образование)
[4] АИС «Навигатор дополнительного образования»
[5] АИС «Электронное и дистанционное обучение»
[6] ИС «Муниципальный сегмент ГИС РС «Контингент»

Приложение № 7
к приказук приказу №26
от 24.03.2026 г .

МЕТОДИКА и АКТ
определения класса защищенности государственной информационной системы «Региональный сегмент единой федеральной межведомственной системы учета контингента обучающихся по основным образовательным программам и дополнительным общеобразовательным программам»

1. Методика определения класса защищенности государственной информационной системы «Региональный сегмент единой федеральной межведомственной системы учета контингента обучающихся по основным образовательным программам и дополнительным общеобразовательным программам» (далее - Методика) МБДОУ № 47 (далее по тексту – МБДОУ № 47) предназначена для построения методики определения класса защищенности государственной информационной системы «Региональный сегмент единой федеральной межведомственной системы учета контингента обучающихся по основным образовательным программам и дополнительным общеобразовательным программам» (далее – ГИС).

Настоящая Методика разработана на основании и в соответствии с Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» и Приказом ФСТЭК России от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

Целью настоящей Методики является определение уровня защищенности ГИС.

Настоящий документ обязаны знать и использовать в работе члены комиссии по проведению мероприятий по защите информации, назначенной приказом начальника Управления.

2. Определение класса защищенности информационной системы.

Класс защищенности информационной системы (первый класс (К1), второй класс (К2), третий класс (К3)) определяется в зависимости от уровня значимости информации (УЗ), обрабатываемой в этой информационной системе, и масштаба информационной системы (федеральный, региональный, объектовый).

Класс защищенности (К) = [уровень значимости информации; масштаб системы].

Уровень значимости информации определяется степенью возможного ущерба для обладателя информации (заказчика) и (или) оператора от нарушения конфиденциальности (неправомерные доступ, копирование, предоставление или распространение), целостности (неправомерные уничтожение или модифицирование) или доступности (неправомерное блокирование) информации.

УЗ = [(конфиденциальность, степень ущерба) (целостность, степень ущерба) (доступность, степень ущерба)],

где степень возможного ущерба определяется обладателем информации (заказчиком) и (или) оператором самостоятельно экспертным или иными методами и может быть:

высокой, если в результате нарушения одного из свойств безопасности информации (конфиденциальности, целостности, доступности) возможны существенные негативные последствия в социальной, политической, международной, экономической, финансовой или иных областях деятельности и (или) информационная система и (или) оператор (обладатель информации) не могут выполнять возложенные на них функции;

средней, если в результате нарушения одного из свойств безопасности информации (конфиденциальности, целостности, доступности) возможны умеренные негативные последствия в социальной, политической, международной, экономической, финансовой или иных областях деятельности и (или) информационная система и (или) оператор (обладатель информации) не могут выполнять хотя бы одну из возложенных на них функций;

низкой, если в результате нарушения одного из свойств безопасности информации (конфиденциальности, целостности, доступности) возможны незначительные негативные последствия в социальной, политической, международной, экономической, финансовой или иных областях деятельности и (или) информационная система и (или) оператор (обладатель информации) могут выполнять возложенные на них функции с недостаточной эффективностью или выполнение функций возможно только с привлечением дополнительных сил и средств.

Информация имеет высокий уровень значимости (**УЗ 1**), если хотя бы для одного из свойств безопасности информации (конфиденциальности, целостности, доступности) определена высокая степень ущерба. Информация имеет средний уровень значимости (**УЗ 2**), если хотя бы для одного из свойств безопасности информации (конфиденциальности, целостности, доступности) определена средняя степень ущерба и нет ни одного свойства, для которого определена высокая степень ущерба. Информация имеет низкий уровень значимости (**УЗ 3**), если для всех свойств безопасности информации (конфиденциальности, целостности, доступности) определены низкие степени ущерба.

При обработке в информационной системе двух и более видов информации (служебная тайна, налоговая тайна и иные установленные законодательством Российской Федерации виды информации ограниченного доступа) уровень значимости информации (УЗ) определятся отдельно для каждого вида информации. Итоговый уровень значимости информации, обрабатываемой в информационной системе, устанавливается по наивысшим значениям степени возможного ущерба, определенным для конфиденциальности, целостности, доступности информации каждого вида информации.

Информационная система имеет федеральный масштаб, если она функционирует на территории Российской Федерации (в пределах федерального

округа) и имеет сегменты в субъектах Российской Федерации, муниципальных образованиях и (или) организациях.

Информационная система имеет региональный масштаб, если она функционирует на территории субъекта Российской Федерации и имеет сегменты в одном или нескольких муниципальных образованиях и (или) подведомственных и иных организациях.

Информационная система имеет объектовый масштаб, если она функционирует на объектах одного федерального органа государственной власти, органа государственной власти субъекта Российской Федерации, муниципального образования и (или) организации и не имеет сегментов в территориальных органах, представительствах, филиалах, подведомственных и иных организациях.

Класс защищенности информационной системы определяется в соответствии с таблицей:

Уровень значимости	**Масштаб ИС**		
	Федеральный	**Региональный**	**Объектовый**
УЗ 1	К1	К1	К1
УЗ 2	К1	К2	К2
УЗ 3	К2	К3	К3

3. Исходные данные

ГИС состоит из 1 АРМ, расположенного в кабинете № 25 на первом этаже второго здания, по адресу: Владимирская обл., г.Ковров, ул. Киркижа дом 21

Доступ в сеть Интернет – FTTx, роутер подключен к сетевому оборудованию ЛВС МБДОУ № 47.

Целью МБДОУ № 47 является ведение систем в рамках возложенных полномочий

Сотрудники МБДОУ № 47 имеют права чтения, защищаемой информации.

ГИС «Контингент» размещена на серверах ГАОУ ДПО ВО ВИРО. МБДОУ № 47 получает доступ к серверам по защищенному каналу, построенному на базе комплекса «ViPNet Client». В МБДОУ № 47 на АРМ установлена клиентская часть комплекса «ViPNet Client for Windows 4.5»

4. Доступ к ПДн и ИСПДн

Доступ к ГИС и защищаемой информации имеют ограниченный круг сотрудников управления образования.

Приложение № 8
к приказук приказу №26
от 24.03.2026 г

Бланки уведомлений уполномоченных органов

Исх. № ___ от __.__.20__

В _____

(указать уполномоченный орган)

Уведомление об исполнении требования

Настоящим уведомлением сообщаем Вам, что по вашему требованию от __.__.201_ № ___*(указать реквизиты письма)* персональные данные субъекта *(указать реквизиты субъекта)* уточнены/заблокированы/уничтожены *(указать нужное)*.

Директор/Заведующий И.О. Фамилия

Исх. № ___ от __.__.20__

В _____

(указать уполномоченный орган)

Уведомление об устранении допущенных нарушений

Настоящим уведомлением сообщаем Вам, что допущенные нарушения при обработке персональных данных, а именно_____*(указать допущенные нарушения)*, устранены.

Директор/Заведующий И.О. Фамилия

Приложение № 9
к приказук приказу №26
от 24.03.2026 г

Бланки уведомлений субъектов персональных данных

Исх. № ___ от __.__.20__

Запрос

Уважаемый(ая) _____*(ФИО),* в связи с _____ у нас возникла необходимость получения следующей информации, составляющей Ваши персональные данные _____

(перечислить информацию). Просим Вас предоставить указанные сведения в течение _____ рабочих дней с момента получения настоящего запроса.

В случае невозможности предоставить указанные сведения просим в указанный срок дать письменное согласие на получение нами необходимой информации из следующих источников _____, следующими способами _____.

По результатам обработки указанной информации нами планируется принятие следующих решений, которые будут доведены до Вашего сведения _____.

Против принятого решения Вы имеете право заявить свои письменные возражения в _____ срок.

Директор/Заведующий И.О. Фамилия

Исх. № ___ от __.__.20__

Уведомление о блокировании

Уважаемый(ая)_____*(ФИО)*, в связи с _____сообщаем Вам, что Ваши персональные данные _____*(указать перечень персональных данных)* заблокированы на срок _____.

Директор/Заведующий И.О. Фамилия

Исх. № ___ от __.__.201_

Уведомление об уточнении

Уважаемый(ая)_____*(ФИО)*, в связи с _____ сообщаем Вам, что Ваши персональные данные уточнены в соответствии со сведениями: _____.

Директор/Заведующий И.О. Фамилия

Исх. № ___ от __.__.20__

Уведомление

Уважаемый(ая) _____*(ФИО)*, нами производиться обработка сведений, составляющих Ваши персональные данные: _____*(указать перечень персональных данных)*.

Цели обработки: _____.

Способы обработки: _____.

Сведения о лицах (кроме сотрудников МБДОУ № 47), которые имеют доступ к вашим персональным данным или которым могут быть раскрыты персональные данные на основании договора с нами или на основании федерального закона:

Ф.И.О.	Основание доступа	Вид доступа	Примечания

По результатам обработки указанной информации нами планируется принятие следующих решений, которые будут доведены до Вашего сведения _____.

Против принятого решения Вы имеете право заявить свои письменные возражения в _____ срок.

Директор/Заведующий И.О. Фамилия

Исх. № ___ от __.__.20__

Уведомление об уничтожении

Уважаемый(ая) _____*(ФИО)*, в связи с _____ сообщаем Вам, что Ваши персональные данные _____*(указать перечень персональных данных)* уничтожены.

Директор/Заведующий И.О. Фамилия

Исх. № ___ от __.__.20__

Уведомление об устранении допущенных нарушений

Уважаемый(ая)_____*(ФИО)*, в связи с _____ сообщаем Вам, что все допущенные нарушения при обработке Ваших персональных данных устранены.

Директор/Заведующий И.О. Фамилия

Приложение № 10.
к приказук приказу №26
от 24.03.2026 г

Бланки заявлений субъектов персональных данных

Рег. № ___ от __.__.20__

В МБДОУ № 47

от_____
(ф.и.о. заявителя)

_____

_____

_____
(наименование и реквизиты документа,
удостоверяющего личность заявителя,
сведения о дате выдачи и выдавшем органе)

Заявление

МБДОУ № 47 осуществляет обработку моих персональных данных на основании:

_____
(указать сведения, подтверждающие факт обработки персональных данных оператором)

Прошу предоставить мне следующую информацию, касающуюся обработки моих персональных данных:

1) подтверждение факта обработки персональных данных МБДОУ № 47;

2) правовые основания и цели обработки персональных данных;

3) цели и применяемые способы обработки персональных данных;

4) наименование и место нахождения МБДОУ № 47, сведения о лицах (за исключением работников МБДОУ № 47), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с оператором или на основании Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»;

5) обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения;

6) сроки обработки персональных данных, в том числе сроки их хранения;

7) порядок осуществления субъектом персональных данных прав, предусмотренных Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных»;

8) информацию об осуществленной или о предполагаемой трансграничной передаче данных;

9) наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению МБДОУ № 47, если обработка поручена или будет поручена такому лицу;

10) иные сведения, предусмотренные Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» или другими федеральными законами.

_____(_____)

«___» _____

Рег. № ___ от __.__.20__

В МБДОУ № 47
от_____
(ф.и.о. заявителя)
_____
_____
_____
(наименование и реквизиты документа,
удостоверяющего личность заявителя,
сведения о дате выдачи и выдавшем органе)

Заявление

МБДОУ № 47 осуществляет обработку моих персональных данных на основании:

_____

(указать сведения, подтверждающие факт обработки персональных данных оператором)

Прошу уничтожить обрабатываемые Вами мои персональные данные: _____;

(указать уничтожаемые персональные данные)

в связи с тем, что _____

_____.

(указать причину уничтожения персональных данных (данные являются неполными, устаревшими, неточными, незаконно полученными, не являются необходимыми для заявленной цели обработки)

_____(_____)

«___» _____

Рег. № ___ от __.__.20__

В МБДОУ № 47
от_____
(ф.и.о. заявителя)
_____
_____
_____
(наименование и реквизиты документа,
удостоверяющего личность заявителя

Заявление

МБДОУ № 47 осуществляет обработку моих персональных данных на основании:

_____

(указать сведения, подтверждающие факт обработки персональных данных оператором)

Прошу уточнить обрабатываемые Вами мои персональные данные в соответствии со сведениями: _____

_____;

(указать уточненные персональные данные заявителя)

в связи с тем, что _____

_____.

(указать причину уточнения персональных данных (данные являются неполными, устаревшими, неточными и т.п.))

_____(_____)

«___» _____

Рег. № ___ от __.__.20__

В МБДОУ № 47

от_____
(ф.и.о. заявителя)

_____

_____

_____
(наименование и реквизиты документа,
удостоверяющего личность заявителя,
сведения о дате выдачи и выдавшем органе)

Заявление

МБДОУ № 47 осуществляет обработку моих персональных данных на основании:

_____.

(указать сведения, подтверждающие факт обработки персональных данных оператором)

Прошу заблокировать обрабатываемые Вами мои персональные данные:

_____

(указать блокируемые персональные данные)

на срок:_____;

(указать срок блокирования)

в связи с тем, что _____

_____.

(*указать причину уничтожения персональных данных (данные являются неполными, устаревшими, неточными, незаконно полученными, не являются необходимыми для заявленной цели обработки)*

_____(_____)

«___» _____

Приложение № 11
к приказук приказу №26
от 24.03.2026 г

ОБЯЗАТЕЛЬСТВО
о неразглашении информации, содержащей персональные данные

Я, _____,
проживающий по адресу:_____
_____
паспорт серия _____ №_____, выданный (кем и когда)
_____
_____
предупрежден(а) о том, что на период исполнения мною должностных обязанностей по трудовому договору, заключенному между мною и МБДОУ № 47 (далее – МБДОУ № 47), и предусматривающих работу с персональным данным обучающихся субъектов, родившиеся и зарегистрированные по месту жительства (далее - субъектов) мне будет предоставлен доступ к указанной информации.

Настоящим добровольно принимаю на себя обязательства:

– не передавать (в любом виде) и не разглашать третьим лицам и работникам Управления, не имеющим на это право в силу выполняемых ими должностных обязанностей или в соответствии с решением руководителя, информацию, содержащую персональные данные субъектов, которая мне доверена (будет доверена) или станет известной в связи с исполнением должностных обязанностей;

– в случае попытки третьих лиц или работников МБДОУ № 47, не имеющих на это право, получить от меня информацию, содержащую персональные данные, немедленно сообщать об этом факте своему непосредственному или (в случае отсутствия непосредственного) вышестоящему руководителю;

– не использовать информацию, содержащую персональные данные, с целью получения выгоды;

– выполнять требования закона и иных нормативных правовых актов Российской Федерации, а также внутренних документов МБДОУ № 47, регламентирующих вопросы защиты интересов субъектов персональных данных, порядка обработки и защиты персональных данных;

– после прекращения моих прав на допуск к информации, содержащей персональные данные (переход на должность, не предусматривающую доступ к персональным данным или прекращения трудового договора), не обрабатывать, не разглашать и не передавать третьим лицам и неуполномоченным на это работникам МБДОУ № 47, известную мне информацию, содержащую персональные данные.

Я предупрежден (а) о том, что в случае нарушения данного обязательства буду привлечен (а) к дисциплинарной ответственности и/или иной ответственности в соответствии с действующим законодательством Российской Федерации.

_____ /_____
«___» _____ _____ г.

Приложение № 12.
к приказук приказу №26
от 24.03.2026 г

ИНСТРУКЦИЯ
о порядке действий во внештатных ситуациях и восстановлению после сбоя

1. Настоящая Инструкция о порядке действий во внештатных ситуациях и восстановлению после сбоя (далее – Инструкция) устанавливает порядок действий во внештатных ситуациях сотрудников МБДОУ № 47.

Целью настоящей Инструкции является определение основных мер, методов и средств сохранения (поддержания) работоспособности информационных систем, используемых в МБДОУ № 47 (далее - ИС) при возникновении различных внештатных ситуаций, а также способов и средств восстановления информации и процессов ее обработки в случае нарушения работоспособности ИС и их основных компонентов.

2. Общие требования

Источники информации о возникновении внештатной ситуации:

– пользователи, обнаружившие подозрительные изменения в работе или конфигурации системы или средств ее защиты в своей зоне ответственности;

– средства защиты, обнаружившие кризисную ситуацию;

– системные журналы, в которых имеются записи, свидетельствующие о возникновении или возможности возникновения кризисной ситуации.

Все пользователи, работа которых может быть нарушена в результате возникновения угрожающей или серьезной внештатной ситуации, должны немедленно устно оповещаться администратором информационной безопасности. Дальнейшие действия по устранению причин нарушения работоспособности ИС, возобновлению обработки и восстановлению поврежденных (утраченных) ресурсов определяются функциональными обязанностями персонала и пользователей системы.

Каждая внештатная ситуация должна анализироваться администратором информационной безопасности. По результатам этого анализа должны вырабатываться предложения по изменению полномочий пользователей, атрибутов доступа к ресурсам, созданию дополнительных резервов, изменению конфигурации системы или параметров настройки средств защиты и т.п., при необходимости должно проводится расследование причин ее возникновения, оценка причиненного ущерба, определение виновных и принятие соответствующих мер.

Серьезная и угрожающая внештатная ситуация могут требовать оперативной замены и ремонта вышедшего из строя оборудования, а также восстановления поврежденных программ и наборов данных из резервных копий.

Оперативное восстановление программ (используя эталонные копии) и данных (используя страховые копии) в случае их уничтожения или порчи в серьезной или угрожающей кризисной ситуации обеспечивается резервным

(страховым) копированием и внешним (по отношению к основным компонентам системы) хранением копий. Внешнее хранение подразумевает нахождение копий в выделенных хранилищах (сейфах), находящихся в специально отведенных помещениях.

Резервному копированию подлежат все программы и данные, обеспечивающие работоспособность и выполнение задач системы (системное и прикладное программное обеспечение, базы данных и другие наборы данных), а также архивы, журналы транзакций, системные журналы и т.д.

Все программные средства, используемые в системе должны иметь эталонные (дистрибутивные) копии.

Необходимые действия персонала по созданию, хранению и использованию резервных копий программ и данных должны быть отражены в функциональных обязанностях соответствующих категорий персонала – системные администраторы и администратор информационной безопасности.

3. Меры обеспечения непрерывной работы и восстановления

Технические меры:

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

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

Для выполнения требований по эксплуатации (температура, относительная влажность воздуха) программно-аппаратных средств ИС в помещениях, где они установлены, должны применяться системы вентиляции и кондиционирования воздуха.

Для предотвращения потерь информации при кратковременном отключении электроэнергии все ключевые элементы ИС, 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 ИС при сбое в работе оборудования и их автоматической замены без простоев должны использоваться методы кластеризации. Могут использоваться следующие методы кластеризации: для наиболее критичных компонентов ИС 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-0) 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.).

Организационные меры:

Резервное копирование и хранение данных должно осуществлять на периодической основе:

– для защищаемой информации – не реже раза в неделю;
– для технологической информации – не реже раза в месяц;
– эталонные копии программного обеспечения (операционные системы, штатное и специальное программное обеспечение, программные средства защиты), с которых осуществляется их установка на элементы ИС – не реже раза в месяц, и каждый раз при внесении изменений в эталонные копии (выход новых версий).

Данные о проведение процедуры резервного копирования, должны отражаться в Журнале учета процедур резервного копирования, который ведет администратор информационной безопасности.

Носители, на которые произведено резервное копирование, должны быть пронумерованы: номером носителя, датой проведения резервного копирования.

Носители должны храниться в несгораемом шкафу или помещении, оборудованном системой пожаротушения.

Носители должны храниться не менее года, для возможности восстановления данных.

4. Действия персонала при возникновении внештатных ситуаций

Сотрудник обнаруживший сбой в работе ИС в результате внештатной ситуации должен незамедлительно поставить в известность администратора информационной безопасности.

В кратчайшие сроки, не превышающие одного рабочего дня администратором информационной безопасности совместно с системным администратором предпринимаются меры по восстановлению работоспособности. Предпринимаемые меры по возможности согласуются с вышестоящим руководством. По необходимости, иерархия может быть нарушена, с целью получения высококвалифицированной консультации в кратчайшие сроки.

Приложение № 13
к приказук приказу №26
от 24.03.2026 г

ИНСТРУКЦИЯ
по работе с носителями персональных данных в МБДОУ № 47

1. Инструкция по работе с носителями персональных данных в МБДОУ № 47 (далее - Инструкция) устанавливает требования при работе с носителями персональных данных (ПДн) в МБДОУ № 47 (далее - МБДОУ № 47).

Виды носителей ПДн:

– бумажные носители;

– накопители на жестких магнитных дисках (НЖМД) рабочих станций информационной системы персональных данных (ИСПДн);

– съемные носители ПДн (USB, диски, дискеты, переносные носители на жестких магнитных дисках, карты памяти, в том числе в составе сотовых телефонов и т.д.).

2. Общие требования

Носители ПДн подлежат учету, который ведет системный администратор, выполняющий функции администратора информационной безопасности (далее – системный администратор) в Журнале учета носителей ПДн с пометкой - для ПДн.

При постановке на учет машинного носителя его маркировка производится на нерабочей поверхности, посредством наклеивания на поверхность самоклеящейся бумаги с учетным номером (для флэш-накопителей), нанесения стойким красящим веществом (для жестких дисков, дискет и CD-DVD дисков).

Учетные номера присваиваются машинным носителям начиная с 01 и записываются в виде «хх МН», где хх - присвоенный учетный номер, «МН» - пометка о типе учетного номера (в данном случае - машинный носитель).

Если маркировка жесткого диска невозможна (системный блок опечатан при проведении аттестации, системный блок опечатан и находится на гарантии, жесткий диск находится в ноутбуке и т.п.), маркировка наносится на системный блок компьютера до прекращения действия обстоятельств, препятствующих маркировке.

Бумажные носители используются в работе до минования необходимости и подлежат хранению в течение сроков, определенных для разных видов документов.

Перечень мест хранения материальных носителей утверждается приказом начальника Управления.

НЖМД и съемные носители подлежат эксплуатации до выхода из строя или минования необходимости, затем производится либо затирание данных без возможности восстановления (для возможности дальнейшего использования носителя), либо уничтожение.

В отношении всех носителей ПДн необходимо соблюдать общие принципы безопасности:

– ограничение доступа к носителю ПДн;

– каждый пользователь носителя ПДн несет персональную ответственность за его сохранность.

По окончанию использования носителей ПДн они подлежат уничтожению. Порядок уничтожения определен Положением о комиссии по уничтожению.

Уничтожение всех видов носителей ПДн фиксируется в Журнале учета носителей ПДн. По факту уничтожения или вывода из эксплуатации носителя ПДн составляется акт.

3. Работа с НЖМД

НЖМД предназначены для постоянного или временного хранения баз данных ПДн а также проведения операций с ними.

Непосредственный физический доступ к носителям ПДн имеет только системный администратор. При выходе из строя носителя ПДн пользователь ИСПДн вызывает системного администратора, который проверяет его неработоспособность, производит замену носителя.

Вышедшие из строя носители ПДн подлежат уничтожению.

4. Работа со съемными носителями ПДн

Съемные носители могут быть использованы для:

- передачи ПДн в вышестоящие организации;
- переноса ПДн между сотрудниками Управления;
- постоянного или временного хранения ПДн.

Выдача съемных носителей производится системным администратором.

После получения съемного носителя лицо, его получившее, несет полную ответственность за данный носитель, за его сохранность и за сохранность и не разглашение ПДн, которые будут на нем храниться.

Перед началом работы со съемным носителем необходимо провести проверку на вирусы антивирусными средствами. В случае обнаружения вирусов необходимо провести «лечение» зараженных файлов и запустить проверку на наличие/отсутствие вирусов на своем рабочем месте.

Не допускается оставлять съемный носитель без присмотра лица, его получившего. При повреждении съемного носителя и невозможности его дальнейшего использования он сдается системному администратору.

По окончании необходимости использования съемного носителя штатными средствами операционной системы производится затирание всех имеющихся на нем данных, носитель сдается системному администратору под подпись в журнале выданных носителей, его получавшим, в отдельных случаях – его представителем.

Полученный съемный носитель проверяется системным администратором на наличие данных и отсутствие повреждений носителя, то есть возможность его дальнейшего использования.

Об утере съемного носителя лицо, получившее его, незамедлительно сообщает системному администратору. По данному факту системным администратором и ответственным за организацию обработки ПДн проводится служебное расследование или разбирательство с целью выявления возможного ущерба. Документы по служебным расследованиям хранятся у ответственного за организацию обработки ПДн.

Приложение № 14
к приказук приказу №26
от 24.03.2026 г

ПОРЯДОК
ознакомления работников МБДОУ № 47, непосредственно осуществляющих обработку персональных данных или осуществляющих доступ к ним, с положениями законодательства Российской Федерации о персональных данных

1. Порядок ознакомления работников МБДОУ № 47 с положениями законодательства РФ о персональных данных (далее - Порядок) разработан в целях исполнения пункта 6 части 1 статьи 18.1 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» по ознакомлению работников оператора, непосредственно осуществляющих обработку персональных данных или осуществляющих доступ к ним, с положениями законодательства РФ о персональных данных, в том числе требованиями к защите персональных данных, документами, определяющими политику оператора в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных, и (или) обучению указанных работников.

2. МБДОУ № 47 проводит ознакомление работников, непосредственно осуществляющих обработку персональных данных или осуществляющих доступ к ним, с положениями законодательства РФ о персональных данных, в том числе требованиями к защите персональных данных, документами, определяющими политику оператора в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных, и (или) обучение указанных работников:

2.1. при оформлении трудовых отношений;

2.2. при первоначальном допуске к обработке персональных данных в информационной системе персональных данных;

2.3. при назначении на новую должность, связанную с обработкой персональных данных или доступом к ним;

2.4. после внесения изменений в действующее законодательство Российской Федерации о персональных данных, локальные акты управления образования по вопросам обработки персональных данных, включая настоящий Порядок.

3. Ознакомление работников МБДОУ № 47, непосредственно осуществляющих обработку персональных данных или осуществляющих доступ к ним, с положениями законодательства РФ о персональных данных, в том числе требованиями к защите персональных данных, документами, определяющими политику оператора в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных, и (или) обучение указанных работников, осуществляется под подпись работника:

3.1. в случаях, указанных в пунктах 2.1 - 2.3 настоящего Порядка, фиксируется в листе ознакомления работника МБДОУ № 47, непосредственно осуществляющего обработку персональных данных или осуществляющих доступ к

ним, с положениями законодательства Российской Федерации о персональных данных (в том числе с требованиями к защите персональных данных), локальными актами по вопросам обработки персональных данных (далее – Лист ознакомления) по форме согласно приложению к данному Порядку (первичное ознакомление работников).

3.2. в случае, указанном в пункте 2.4 настоящего Порядка, фиксируется в Журнале инструктажа по защите информации и персональных данных по форме, утвержденной приложением к приказу МБДОУ № 47 «Об утверждении документов по защите информации».

Приложение
к Порядку ознакомления работников МБДОУ № 47 с положениями законодательства РФ о персональных данных

ЛИСТ ОЗНАКОМЛЕНИЯ
работника МБДОУ № 47, непосредственно осуществляющего обработку персональных данных или осуществляющих доступ к ним, с положениями законодательства Российской Федерации о персональных данных (в том числе с требованиями к защите персональных данных), локальными актами по вопросам обработки персональных данных

Я, _____,
(фамилия, имя, отчество)
_____
_____,
(должность)
ознакомлен(а) с положениями законодательства Российской Федерации о персональных данных (в том числе с требованиями к защите персональных данных), локальными актами по вопросам обработки персональных данных.

Мною изучены положения Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», Федерального закона «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ, Трудового кодекса Российской Федерации, постановления Правительства Российской Федерации от 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными и муниципальными органами», постановления Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», постановления Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», а также приказов МБДОУ № 47 по вопросам защиты информации, обработки и защиты персональных данных в МБДОУ № 47.

Я уведомлен(а) о том, что персональные данные являются конфиденциальной информацией и я обязан(а) не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, ставшие известными мне в связи с исполнением должностных обязанностей.

Ответственность и права, предусмотренные Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» и другими федеральными законами, мне разъяснены.

«___»_____20__ г. _____ _____
(дата) *(подпись)* *(расшифровка)*

Приложение № 15
к приказук приказу №26
от 24.03.2026 г

ЖУРНАЛ

инструктажа по защите информации и персональных данных

Срок хранения:

Начат «___»_____20__г.

Окончен «___»_____20__г.

На _____ листах

№ п/п	Дата инструктажа	Ответственный за организацию обработки ПДн	Тема инструктажа/ нормативный документ	Слушатели (ФИО, подпись)

Приложение № 16
к приказук приказу №26
от 24.03.2026 г

ЖУРНАЛ

учета средств защиты информации и эксплуатационной документации

Срок хранения:

Начат «___»_____20__г.

Окончен «___»_____20__г.

На _____ листах

Название СЗИ	Серийный номер	Номер СЗЗ	Сертификат соответствия	Кем установлен	Подпись ответственного	Отметка об установке		Отметка об изъятии	
						Дата установки	Подпись установившего	Дата изъятия	Подпись изъявшего

Приложение № 17
к приказук приказу №26
от 24.03.2026 г

ЖУРНАЛ

учета мероприятий по контролю над соблюдением режима защиты информации

Срок хранения:

Начат «___»_____20__г.

Окончен «___»_____20__г.

На _____ листах

№	Мероприятие	Дата проведения	Результаты проверки	Подпись исполнителя

Приложение № 18
к приказук приказу №26
от 24.03.2026 г

ЖУРНАЛ

учета обращений субъектов персональных данных

Срок хранения:

Начат «___»_____20__г.

Окончен «___»_____20__г.

На _____ листах

№	Дата	Сведения о запрашивающем лице	Цель обращения	Подпись запрашивающего	Подпись ответственного сотрудника	Краткое содержание ответа на обращение	Реквизиты ответа на обращение

Приложение № 19
к приказук приказу №26
от 24.03.2026 г ….

ЖУРНАЛ

учета процедур резервного копирования

Срок хранения:

Начат «___»_____20__г.

Окончен «___»_____20__г.

На _____ листах

№	Что подлежит резервному копированию	Дата проведения процедуры	Место создания (номер носителя) резервной копии	Подпись ответственного

Приложение № 20
к приказук приказу №26
от 24.03.2026 г

ЖУРНАЛ

учета носителей персональных данных
МБДОУ № 47

Срок хранения:

Начат «___»_____20__г.

Окончен «___»_____20__г.

На _____ листах

Учетный №	Место хранения	Дата	Вид носителя	Подпись ответственного	Отметка о выдаче		Отметка о возврате	
					Дата выдачи	Подпись получившего	Дата возврата	Подпись сдавшего
								-
						ч		
						ч		
						ч		
