МУНИЦИПАЛЬНОЕ БЮДЖЕТНОЕ ДОШКОЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
«ПОДВЯЗЬЕВСКИЙ ДЕТСКИЙ САД»
МУНИЦИПАЛЬНОГО ОБРАЗОВАНИЯ –
РЯЗАНСКИЙ МУНИЦИПАЛЬНЫЙ РАЙОН РЯЗАНСКОЙ ОБЛАСТИ
ОГРН 1056212008478 ИНН 6215014935
390502 Рязанская обл., Рязанский район, с. Подвязье,
ул. Садовая, д.8, Тел.(4912) 26-63-03, e-mail: podv-sad@mail.ru

ПРИКАЗ

от «27» июля 2020 г. №68/1-р

«Об утверждении организационно-распорядительной документации по организации обработки и защите информации в муниципальном бюджетном дошкольном образовательном учреждении «Подвязьевский детский сад» муниципального образования – Рязанский муниципальный район Рязанской области, в том числе по работе с персональными данными»

В соответствии с Федеральными законами от 27 июля 2006 г. № 149-ФЗ «Об информационных технологиях и о защите информации» и от 27 июля 2006 г. «152-ФЗ персональных данных», постановлением Правительства Российской Федерации от 21 марта 2012 г. № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами», руководствуясь Уставом муниципального бюджетного дошкольного образовательного учреждения «Подвязьевский детский сад» муниципального образования – Рязанский муниципальный район Рязанской области Утвердить:

1) Правила обработки персональных данных в муниципальном бюджетном дошкольном образовательном учреждении «Подвязьевский детский сад» муниципального образования – Рязанский муниципальный район Рязанской области согласно приложению № 1 к настоящему распоряжению;

2) Правила рассмотрения запросов субъектов персональных данных муниципального бюджетного дошкольного образовательного учреждения «Подвязьевский детский сад» муниципального образования – Рязанский муниципальный район Рязанской области согласно приложению № 2 к настоящему распоряжению;

3) Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в муниципальном бюджетном дошкольном образовательном учреждении «Подвязьевский детский сад» муниципального образования – Рязанский муниципальный район Рязанской области согласно приложению № 3 к настоящему распоряжению;

4) Перечень должностей, при замещении которых сотрудники муниципального бюджетного дошкольного образовательного учреждения «Подвязьевский детский сад» муниципального образования – Рязанский муниципальный район Рязанской области осуществляют обработку персональных данных либо имеют доступ к персональным данным согласно приложению № 5 к настоящему распоряжению;

5) Обязательство о прекращении обработки персональных данных в случае расторжения служебного контракта (трудового договора) согласно приложению № 8 к настоящему распоряжению;

6) Согласие субъекта персональных данных на обработку персональных данных согласно приложению № 6 к настоящему распоряжению;

7) Разъяснение субъекту персональных данных (немуниципальному служащему) юридических последствий отказа представить свои персональные данные согласно приложению № 7 к настоящему распоряжению;

8) Разъяснение субъекту персональных данных (муниципальному служащему) юридических последствий отказа предоставить свои персональные данные согласно приложению № 8 к настоящему распоряжению;

9) Перечень персональных данных, обрабатываемых в муниципальном бюджетном дошкольном образовательном учреждении «Подвязьевский детский сад» муниципального образования – Рязанский муниципальный район Рязанской области согласно приложению № 9 к настоящему распоряжению;

10) Порядок доступа в помещения муниципального бюджетного дошкольного образовательного учреждения «Подвязьевский детский сад» муниципального образования – Рязанский муниципальный район Рязанской области в которых ведется обработка персональных данных, согласно приложению № 10 к настоящему распоряжению;

11) Перечень информационных систем в муниципальном бюджетном дошкольном образовательном учреждении «Подвязьевский детский сад» муниципального образования – Рязанский муниципальный район Рязанской области в том числе информационных систем персональных данных согласно приложению № 11 к настоящему распоряжению;

12) Инструкцию ответственного за организацию обработки персональных данных в муниципальном бюджетном дошкольном образовательном учреждении «Подвязьевский детский сад» муниципального образования – Рязанский муниципальный район Рязанской области согласно приложению № 12 к настоящему распоряжению;

13) Инструкцию по работе ответственного за эксплуатацию объекта информатизации в муниципальном бюджетном дошкольном образовательном учреждении «Подвязьевский детский сад» муниципального образования – Рязанский муниципальный район Рязанской области согласно приложению № 13 к настоящему распоряжению;

14) Инструкцию пользователя информационной системы персональных данных в муниципальном бюджетном дошкольном образовательном учреждении «Подвязьевский детский сад» муниципального образования – Рязанский муниципальный район Рязанской области согласно приложению № 14 к настоящему распоряжению;

15) Инструкцию по работе администратора безопасности информации информационной системы персональных данных в муниципальном бюджетном дошкольном образовательном учреждении «Подвязьевский детский сад» муниципального образования – Рязанский муниципальный район Рязанской области согласно приложению № 15 к настоящему распоряжению;

16) Инструкцию по организации парольной защиты в информационных системах муниципального бюджетного дошкольного образовательного учреждения «Подвязьевский детский сад» муниципального образования – Рязанский муниципальный район Рязанской области согласно приложению № 16 к настоящему распоряжению;

17) Инструкцию по управлению доступом к персональным данным в муниципальном бюджетном дошкольном образовательном учреждении «Подвязьевский детский сад» муниципального образования – Рязанский муниципальный район Рязанской области согласно приложению № 17 к настоящему распоряжению;

18) Инструкцию по защите машинных носителей персональных данных, используемых в информационной системе персональных данных муниципального бюджетного дошкольного образовательного учреждения «Подвязьевский детский сад» муниципального образования – Рязанский муниципальный район Рязанской области согласно приложению № 18 к настоящему распоряжению;

19) Инструкцию ответственного пользователя средств криптографической защиты информации в муниципальном бюджетном дошкольном образовательном учреждении «Подвязьевский детский сад» муниципального образования – Рязанский муниципальный район Рязанской области согласно приложению № 19 к настоящему распоряжению;

20) Инструкцию пользователя средств криптографической защиты информации в муниципальном бюджетном дошкольном образовательном учреждении «Подвязьевский детский сад» муниципального образования – Рязанский муниципальный район Рязанской области согласно приложению № 20 к настоящему распоряжению;

21) Журнал поэкземплярного учета средств защиты информации, согласно приложению № 21 к настоящему распоряжению;

22) Руководство администратора информационной системы муниципального бюджетного дошкольного образовательного учреждения «Подвязьевский детский сад» муниципального образования – Рязанский муниципальный район Рязанской области согласно приложению № 22 к настоящему распоряжению;

23) Руководство пользователя информационной системы муниципального бюджетного дошкольного образовательного учреждения «Подвязьевский детский сад» муниципального образования – Рязанский муниципальный район Рязанской области, согласно приложению № 23 к настоящему распоряжению;

1. Настоящее распоряжение вступает в силу с момента принятия.
2. Контроль за исполнением настоящего распоряжения оставляю за собой.

И.о.заведующей
МБДОУ «Подвязьевский детский сад» Ерина И.В.

ПРИЛОЖЕНИЕ 1
к приказу муниципального бюджетного дошкольного образовательного учреждения «Подвязьевский детский сад» муниципального образования – Рязанский муниципальный район Рязанской области
от «27» июля 2020 г. № 68/1-р

ПРАВИЛА
обработки персональных данных в муниципальном бюджетном дошкольном образовательном учреждении «Подвязьевский детский сад» муниципального образования – Рязанский муниципальный район Рязанской области

1. Общие положения

1.1. Правила обработки персональных данных в муниципальном бюджетном дошкольном образовательном учреждении «Подвязьевский детский сад» муниципального образования – Рязанский муниципальный район Рязанской области (далее - Правила) разработаны на основании требований Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», Постановления Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», Постановления Правительства Российской Федерации от 21.03.2012 г. № 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 или муниципальными органами» и устанавливают порядок обработки персональных данных в муниципальном бюджетном дошкольном образовательном учреждении «Подвязьевский детский сад» муниципального образования – Рязанский муниципальный район Рязанской области (далее – ДОУ), процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных, а также определяющие для каждой цели обработки персональных данных содержание обрабатываемых персональных данных, категории субъектов, персональные данные которых обрабатываются, сроки их обработки и хранения, порядок уничтожения при достижении целей обработки или при наступлении иных законных оснований.

1.2. В настоящих Правилах используются следующие основные понятия:

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

- оператор - ДОУ, самостоятельно или совместно с другими лицами организующая и (или) осуществляющая обработку персональных данных, а также определяющая цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными;

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

- автоматизированная обработка персональных данных - обработка персональных данных с помощью средств вычислительной техники;

- распространение персональных данных - действия, направленные на раскрытие персональных данных неопределенному кругу лиц;

- предоставление персональных данных - действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц;

- блокирование персональных данных - временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных);

- уничтожение персональных данных - действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных;

- информационная система персональных данных - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;

- конфиденциальность персональных данных - обязанность операторов и иных лиц, получивших доступ к персональным данным, не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом;

- использование персональных данных - действия (операции) с персональными данными, совершаемые оператором в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта персональных данных или других лиц либо иным образом затрагивающих права и свободы субъекта персональных данных или других лиц;

- информационные технологии - процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов;

- информационно-телекоммуникационная сеть - технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники;

- доступ к информации - возможность получения информации и ее использования;

- под техническими средствами, позволяющими осуществлять обработку персональных данных, понимаются средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки персональных данных (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео и буквенно-цифровой информации), программные средства (оперативные системы, системы управления базами данных и т.п.), средства защиты информации, применяемые в информационных системах;

- базой данных является представленная в объективной форме совокупность самостоятельных материалов, систематизированных таким образом, чтобы эти материалы могли быть найдены и обработаны с помощью объекта информационных технологий.

Иные понятия в данных Правилах используются в значениях, определенных действующим законодательством Российской Федерации, либо их значение дается по тексту.

1.3. Обработка персональных данных должна осуществляться на законной и справедливой основе.

1.4. Обработка персональных данных должна ограничиваться достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных.

1.5. Не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой.

1.6. Обработке подлежат только персональные данные, которые отвечают целям их обработки.

1.7. Содержание и объем обрабатываемых персональных данных должны соответствовать заявленным целям их обработки. Обрабатываемые персональные данные не должны быть избыточными по отношению к заявленным целям их обработки.

1.8. При обработке персональных данных должны быть обеспечены точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных. Оператор должен принимать необходимые меры либо

обеспечивать их принятие по удалению или уточнению неполных или неточных персональных данных.

2. Цели обработки персональных данных

Целями обработки персональных данных в ДОУ являются:

– выполнение требований трудового законодательства Российской Федерации и законодательства о муниципальной службе Российской Федерации и Рязанской области в части ведения кадрового учета, заключение служебных контрактов, трудовых и иных договоров, ведение личных дел (карточек);

– осуществление документооборота;

– выполнение требований законодательства Российской Федерации и Рязанской области в части награждения государственными премиями, наградами, вынесения благодарности и др.;

– оказание муниципальных услуг;

– противодействие коррупции;

– Исполнение требований налогового законодательства по вопросам исчисления и уплаты налога на доходы физлиц и единого социального налога, пенсионного законодательства при формировании и передаче в ПФР персонифицированных данных о каждом получателе доходов, которые учитываются при начислении взносов на обязательное пенсионное страхование.

– расчет и начесление заработной платы.

3. Порядок обработки персональных данных субъектов персональных данных, осуществляемой с использованием средств автоматизации, содержание персональных данных

3.1. Безопасность персональных данных, обрабатываемых с использованием средств автоматизации, достигается путем реализации следующих мер:

- в отношении каждой категории персональных данных определяются места хранения персональных данных (материальных носителей) и устанавливается перечень лиц, осуществляющих обработку персональных данных либо имеющих к ним доступ;

- обеспечивается раздельное хранение персональных данных (материальных носителей), обработка которых осуществляется в различных целях;

- при хранении материальных носителей соблюдаются условия, обеспечивающие сохранность персональных данных и исключение несанкционированного доступа к ним.

3.2. Безопасность персональных данных, обрабатываемых с использованием средств автоматизации, достигается путем принятия необходимых правовых, организационных и технических мер или обеспечения их принятия для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

3.3. Уполномоченными должностными лицами при обработке персональных данных в информационных системах персональных данных должна быть обеспечена их безопасность с помощью системы защиты, включающей организационные меры и средства защиты информации, в том числе шифровальные (криптографические) средства.

3.4. Обмен персональными данными при их обработке в информационных системах осуществляется по каналам связи, защита которых обеспечивается путем реализации соответствующих организационных мер и путем применения программных и технических средств.

3.5. Самостоятельное подключение средств вычислительной техники, применяемых для хранения, обработки или передачи персональных данных к информационно-телекоммуникационным сетям, позволяющим осуществлять передачу информации через государственную границу Российской Федерации, в том числе к информационно-телекоммуникационной сети «Интернет», не допускается.

3.6. Доступ пользователей (операторов информационной системы) к персональным данным в информационных системах персональных данных должен требовать обязательного прохождения процедуры идентификации и аутентификации.

3.7. Должностными лицами ДОУ, ответственными за обеспечение безопасности персональных данных при их обработке в информационных системах, должно быть обеспечено:

- своевременное обнаружение фактов несанкционированного доступа к персональным данным и немедленное доведение этой информации до руководства;
- недопущение воздействия на технические средства автоматизированной обработки персональных данных, в результате которого может быть нарушено их функционирование;
- постоянный контроль за обеспечением уровня защищенности персональных данных;
- знание и соблюдение условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией;
- учет применяемых средств защиты информации, эксплуатационной и технической документации к ним, носителей персональных данных;
- при обнаружении нарушений порядка предоставления персональных данных незамедлительное приостановление предоставления персональных данных пользователям информационной системы до выявления причин нарушений и устранения этих причин;
- разбирательство и составление заключений по фактам несоблюдения условий хранения носителей персональных данных, использования средств защиты информации, которые могут привести к нарушению конфиденциальности персональных данных или другим нарушениям, приводящим к снижению уровня защищенности персональных данных, разработка и принятие мер по предотвращению возможных опасных последствий подобных нарушений.

3.8. В случае выявления нарушений порядка обработки персональных данных в информационных системах уполномоченными должностными лицами принимаются меры по установлению причин нарушений и их устранению.

4. Порядок обработки персональных данных субъектов персональных данных, осуществляемой без использования средств автоматизации

4.1. Обработка персональных данных без использования средств автоматизации уполномоченным должностным лицом осуществляется на материальных (бумажных) носителях персональных данных для целей, указанных в настоящих Правилах.

4.2. При разработке и использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них персональных данных, (далее - типовая форма) должны соблюдаться следующие условия:

- типовая форма или связанные с ней документы (инструкция по ее заполнению, карточки, реестры и журналы) должны содержать сведения о цели обработки персональных данных, осуществляемой без использования средств автоматизации, фамилию, имя, отчество и адрес субъекта персональных данных, чьи персональные данные вносятся в указанную типовую форму, сроки обработки персональных данных, перечень действий с персональными данными, которые будут совершаться в процессе их обработки;
- типовая форма должна предусматривать поле, в котором субъект персональных данных может поставить отметку о своем согласии на обработку персональных данных, осуществляемую без использования средств автоматизации, при необходимости получения согласия на обработку персональных данных;
- типовая форма должна быть составлена таким образом, чтобы каждый из субъектов, чьи персональные данные содержатся в типовой форме, при ознакомлении со своими персональными данными не имел возможности доступа к персональным данным иных лиц, содержащимся в указанной типовой форме;
- типовая форма должна исключать объединение полей, предназначенных для внесения персональных данных, цели обработки которых заведомо не совместимы.

4.3. Уничтожение персональных данных, если это допускается материальным носителем, может производиться способом, исключающим дальнейшую обработку этих персональных

данных, с сохранением возможности обработки иных данных, зафиксированных на материальном носителе.

4.4. Уточнение персональных данных при осуществлении их обработки без использования средств автоматизации производится путем изготовления нового материального носителя с уточненными персональными данными.

5. Порядок обработки персональных данных сотрудников ДОУ

5.1. Обработка персональных данных сотрудников ДОУ осуществляется с их письменного согласия, которое действует со дня замещения ими указанных должностей или устройства на работу в ДОУ на время замещения муниципальной должности в ДОУ, или работы в ДОУ.

5.2. Лица, уполномоченные на обработку персональных данных, обеспечивают защиту персональных данных от неправомерного их использования или утраты.

5.3. Обработка персональных данных сотрудников ДОУ осуществляется как с использованием средств автоматизации, так и без использования таких средств.

5.4. При обработке персональных данных сотрудников ДОУ лица, уполномоченные на обработку персональных данных, обязаны соблюдать следующие требования:

- объем и характер обрабатываемых персональных данных, способы обработки персональных данных должны соответствовать целям обработки персональных данных;
- защита персональных данных сотрудников ДОУ от неправомерного их использования или уничтожения обеспечивается в порядке, установленном нормативными правовыми актами Российской Федерации;
- передача персональных данных сотрудников ДОУ не допускается без их письменного согласия, за исключением случаев, установленных федеральными законами. В случае, если лицо, обратившееся с запросом, не обладает соответствующими полномочиями на получение персональных данных либо отсутствует письменное согласие на передачу персональных данных, лицо, уполномоченное на обработку персональных данных, вправе отказать в предоставлении персональных данных. В этом случае лицу, обратившемуся с запросом, направляется письменный мотивированный отказ в предоставлении запрашиваемой информации;
- обеспечение конфиденциальности персональных данных сотрудников ДОУ, за исключением случаев обезличивания персональных данных и в отношении общедоступных персональных данных;
- хранение персональных данных должно осуществляться в форме, позволяющей определить сотрудников ДОУ и иных лиц, являющихся субъектами персональных данных, не дольше, чем этого требуют цели их обработки. Указанные сведения подлежат уничтожению по достижении цели их обработки или в случае утраты необходимости в их достижении, если иное не установлено законодательством Российской Федерации. Факт уничтожения персональных данных оформляется соответствующим актом;
- опубликование и распространение персональных данных сотрудников ДОУ допускаются в случаях, установленных законодательством Российской Федерации.

5.5. В целях обеспечения защиты персональных данных служащие вправе:

- получать полную информацию о своих персональных данных и способе обработки этих данных (в том числе автоматизированной);
- осуществлять свободный бесплатный доступ к своим персональным данным, включая право получать копии любой записи, за исключением случаев, предусмотренных законодательством Российской Федерации;
- требовать внесения необходимых изменений, уничтожения или блокирования соответствующих персональных данных, которые являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели их обработки;
- обжаловать в порядке, установленном законодательством Российской Федерации, действия (бездействие) уполномоченных должностных лиц.

6. Процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных

К процедурам, направленным на предотвращение и выявление нарушений законодательства Российской Федерации в отношении обработки персональных данных и устранение таких последствий, относятся:

- осуществление внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных, установленным Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных», (далее - Федеральный закон 152-ФЗ) и принятым в соответствии с ним нормативным правовым актом;
- оценка вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона 152-ФЗ, соотношение указанного вреда и принимаемых оператором мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом;
- ознакомление сотрудников ДОУ, непосредственно осуществляющих обработку персональных данных, с законодательством Российской Федерации о персональных данных, в том числе с требованиями к защите персональных данных, и настоящими Правилами.

2.2. Обеспечение безопасности персональных данных достигается, в частности:

- определением угроз безопасности персональных данных при их обработке в информационных системах персональных данных;
- применением организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивают установленные Правительством Российской Федерации уровни защищенности персональных данных;
- применением прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;
- оценкой эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;
- учетом машинных носителей персональных данных;
- обнаружением фактов несанкционированного доступа к персональным данным и принятием соответствующих мер;
- установлением правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечением регистрации и учета всех действий, совершаемых с персональными данными в информационной системе персональных данных.

7. Сроки обработки и хранения персональных данных, порядок их уничтожения при достижении целей обработки или при наступлении иных законных оснований

7.1. Хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен законодательством Российской Федерации, договором, стороной которого является субъект персональных данных. Обрабатываемые персональные данные подлежат уничтожению по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено законодательством Российской Федерации.

7.2. В случае выявления неправомерной обработки персональных данных, оператор в срок, не превышающий 3 рабочих дней с даты этого выявления, обязан прекратить неправомерную обработку персональных данных или обеспечить прекращение неправомерной обработки персональных данных лицом, действующим по поручению оператора. В случае, если обеспечить правомерность обработки персональных данных невозможно, оператор в срок, не превышающий 10 рабочих дней с даты выявления неправомерной обработки персональных данных, обязан

уничтожить такие персональные данные или обеспечить их уничтожение. Об устранении допущенных нарушений или об уничтожении персональных данных оператор обязан уведомить субъекта персональных данных или его представителя, а в случае, если обращение субъекта персональных данных или его представителя либо запрос уполномоченного органа по защите прав субъектов персональных данных были направлены уполномоченным органом по защите прав субъектов персональных данных, также указанный орган.

7.3. В случае достижения цели обработки персональных данных оператор обязан прекратить обработку персональных данных или обеспечить ее прекращение (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) и уничтожить персональные данные или обеспечить их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) в срок, не превышающий 30 дней с даты достижения цели обработки персональных данных, если иное не предусмотрено договором, стороной которого является субъект персональных данных, иным соглашением между оператором и субъектом персональных данных либо если оператор не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных законодательством Российской Федерации.

7.4. В случае отзыва субъектом персональных данных согласия на обработку своих персональных данных оператор обязан прекратить обработку персональных данных и уничтожить персональные данные в срок, не превышающий 3 рабочих дней с даты поступления указанного отзыва, если иное не предусмотрено соглашением между оператором и субъектом персональных данных. Об уничтожении персональных данных оператор обязан уведомить субъекта персональных данных.

7.5. В случае отсутствия возможности уничтожения персональных данных в течение сроков, указанных выше, оператор осуществляет блокирование таких персональных данных или обеспечивает их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) и обеспечивает уничтожение персональных данных в срок не более чем 6 месяцев, если иной срок не установлен законодательством Российской Федерации.

7.6 Должностные лица ДОУ, виновные в нарушении норм и требований действующего законодательства, регулирующих обработку и защиту персональных данных, несут ответственность в соответствии с законодательством Российской Федерации.

ПРИЛОЖЕНИЕ 2
к приказу муниципального бюджетного дошкольного образовательного учреждения «Подвязьевский детский сад» муниципального образования – Рязанский муниципальный район Рязанской области
от «27» июля 2020 г. № 68/1-р

ПРАВИЛА
рассмотрения запросов субъектов персональных данных в муниципальном бюджетном дошкольном образовательном учреждении «Подвязьевский детский сад» муниципального образования – Рязанский муниципальный район Рязанской области.

I. Общие положения

1. Настоящие Правила рассмотрения запросов субъектов персональных данных или их представителей в администрации муниципального образования - Семеновское сельское поселение Рязанского муниципального района Рязанской области (далее - Правила) разработаны на основании требований Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» (далее - Федеральный закон № 152-ФЗ), Федерального закона от 02.03.2007 № 25-ФЗ «О муниципальной службе в 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 или муниципальными органами».

2. Целью Правил является определение требований к порядку рассмотрения запросов субъектов персональных данных или их представителей в муниципальном бюджетном дошкольном образовательном учреждении «Подвязьевский детский сад» муниципального образования – Рязанский муниципальный район Рязанской области (далее – ДОУ).

3. В ДОУ, являющейся оператором, обработка персональных данных субъектов персональных данных и их представителей должна осуществляться на основе принципов, определенных Федеральным законом № 152-ФЗ.

4. В настоящих Правилах термины и определения применяются в том значении, в котором они применяются в Федеральном законе № 152-ФЗ.

II. Информация, предоставляемая по запросу

5. Субъекту персональных данных по его запросу предоставляется информация, касающаяся обработки его персональных данных, в том числе содержащая:

1) подтверждение факта обработки персональных данных;

2) правовые основания и цели обработки персональных данных;

3) цели и применяемые способы обработки персональных данных;

4) наименование и место нахождения оператора, сведения о лицах (за исключением работников оператора), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании соглашения с оператором или на основании федерального закона;

5) обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;

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

7) порядок осуществления субъектом персональных данных прав, предусмотренных Федеральным законом № 152-ФЗ;

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

9) наименование организации или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению оператора, если обработка поручена или будет поручена такому лицу.

6. Сведения, указанные в пункте 5 настоящих Правил, предоставляются субъекту персональных данных или его представителю оператором при обращении либо при получении запроса субъекта персональных данных или его представителя.

Запрос может быть направлен в форме электронного документа и подписан электронной подписью в соответствии с законодательством Российской Федерации.

7. В случае, если сведения, указанные в пункте 5 настоящих Правил, а также обрабатываемые персональные данные были предоставлены для ознакомления субъекту персональных данных по его запросу, субъект персональных данных вправе обратиться повторно к оператору или направить ему повторный запрос в целях получения сведений, указанных в пункте 5 настоящих Правил, и ознакомления с такими персональными данными не ранее чем через тридцать дней после первоначального обращения или направления первоначального запроса, если более короткий срок не установлен Федеральным законом № 152-ФЗ, принятым в соответствии с ним нормативным правовым актом или договором, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных.

8. Субъект персональных данных вправе обратиться повторно к оператору или направить ему повторный запрос в целях получения сведений, указанных в пункте 5 настоящих Правил, а также в целях ознакомления с обрабатываемыми персональными данными до истечения срока, указанного в пункте 7 настоящих Правил, в случае, если такие сведения и (или) обрабатываемые персональные данные не были предоставлены ему для ознакомления в полном объеме по результатам рассмотрения первоначального обращения.

Повторный запрос должен содержать обоснование направления повторного запроса.

III. Требования к содержанию запроса

9. Сведения предоставляются субъекту персональных данных или его представителю при обращении либо при получении запроса субъекта персональных данных или его представителя.

10. Запрос может быть подан на имя заведующего ДОУ одним из следующих способов:

1) лично;

2) с использованием почтовой связи;

3) с использованием средств электронной связи, посредством направления электронного документа, подписанного электронной подписью, в соответствии с законодательством Российской Федерации.

11. Запрос должен содержать:

1) номер основного документа, удостоверяющего личность субъекта персональных данных или его представителя;

2) сведения о дате выдачи указанного документа и выдавшем его органе;

3) сведения, подтверждающие участие субъекта персональных данных в отношениях с оператором (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки персональных данных оператором, подпись субъекта персональных данных или его представителя.

4) сведения, подтверждающие участие субъекта персональных данных в отношениях с ДОУ;

5) подпись субъекта персональных данных или его представителя.

12. К запросу прилагается копия документа, удостоверяющего личность субъекта персональных данных, документ, подтверждающий полномочия заявителя при обращении представителя субъекта персональных данных (нотариально заверенная доверенность).

IV. Действия ДОУ при рассмотрении запроса

13. Рассмотрение запросов является служебной обязанностью уполномоченных должностных лиц ДОУ, в чьи обязанности входит обработка персональных данных.

14. Прием, первичная обработка, регистрация и доведение до исполнителей поступивших запросов производятся в соответствии с установленным порядком организации работы с документами в ДОУ.

15. ДОУ обязано сообщить субъекту персональных данных или его представителю информацию о наличии персональных данных, относящихся к соответствующему субъекту персональных данных, а также предоставить возможность ознакомления с этими персональными данными при обращении субъекта персональных данных или его представителя в течение 30 (тридцати) дней с даты получения запроса субъекта персональных данных или его представителя.

16. В случае отказа в предоставлении информации о наличии персональных данных о соответствующем субъекте персональных данных или персональных данных субъекту персональных данных или его представителю при их обращении либо при получении запроса субъекта персональных данных или его представителя ДОУ обязано дать в письменной форме мотивированный ответ, содержащий ссылку на положение части 8 статьи 14 Федерального закона № 152-ФЗ или иного федерального закона, являющегося основанием для такого отказа, в срок, не превышающий тридцати дней со дня обращения субъекта персональных данных или его представителя либо с даты получения запроса субъекта персональных данных или его представителя.

17. ДОУ обязано сообщать в уполномоченный орган по защите прав субъектов персональных данных по запросу этого органа необходимую информацию в течение 30 (тридцати) дней с даты получения такого запроса.

ПРИЛОЖЕНИЕ 3
к приказу муниципального бюджетного дошкольного образовательного учреждения «Подвязьевский детский сад» муниципального образования – Рязанский муниципальный район Рязанской области от «27» июля 2020 г. № 68/1-р

ПРАВИЛА
осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в муниципальном бюджетном дошкольном образовательном учреждении «Подвязьевский детский сад» муниципального образования – Рязанский муниципальный район Рязанской области.

1. Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в муниципальном бюджетном дошкольном образовательном учреждении «Подвязьевский детский сад» муниципального образования – Рязанский муниципальный район Рязанской области (далее – Правила) разработаны в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», Постановлением Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», Постановлением 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 или муниципальными органами» и другими нормативными правовыми актами.

2. Настоящими Правилами определяются процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных, основания, порядок, формы и методы проведения внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных.

3. В целях осуществления внутреннего контроля соответствия обработки персональных данных установленным требованиям организовывается проведение периодических проверок условий обработки персональных данных.

4. Проверки осуществляются комиссией, утверждаемой распоряжением заведующего муниципального бюджетного дошкольного образовательного учреждения «Подвязьевский детский сад» муниципального образования – Рязанский муниципальный район Рязанской области, возглавляемой ответственным за организацию обработки персональных данных в муниципальном бюджетном дошкольном образовательном учреждении «Подвязьевский детский сад» муниципального образования – Рязанский муниципальный район Рязанской области (далее – Администрация).

5. Проверки проводятся не реже одного раза в три года на основании утвержденного плана осуществления внутреннего контроля соответствия обработки персональных данных установленным требованиям или на основании поступившего письменного заявления о нарушениях правил обработки персональных данных (внеплановые проверки). Проведение внеплановой проверки обеспечивается в течение трех рабочих дней с момента поступления соответствующего заявления.

6. При проведении проверки соответствия обработки персональных данных требованиям к их защите проверяются:

- выполнение правил обработки персональных данных в Администрации;
- порядок и условия применения организационных и технических мер по обеспечению безопасности персональных данных при их обработке, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные уровни защищенности персональных данных;
- порядок и условия применения средств защиты информации;
- эффективность принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;

- состояние учета машинных носителей персональных данных;
- соблюдение правил доступа к персональным данным;
- наличие (отсутствие) фактов несанкционированного доступа к персональным данным и принятие необходимых мер;
- осуществление мероприятий по обеспечению целостности персональных данных.

7. Проверка должна быть завершена не позднее чем через месяц со дня принятия решения о ее проведении. О результатах проведенной проверки и мерах, необходимых для устранения выявленных нарушений ответственный за организацию обработки персональных данных в ДОУ подготавливает письменное заключение.

8. Контроль за своевременностью и правильностью проведения проверки возлагается на главу муниципального образования.

ПРИЛОЖЕНИЕ 4
к приказу муниципального бюджетного дошкольного образовательного учреждения «Подвязьевский детский сад» муниципального образования – Рязанский муниципальный район Рязанской области от «27» июля 2020 г. № 68/1-р

ПЕРЕЧЕНЬ
должностей, при замещении которых сотрудники муниципального бюджетного дошкольного образовательного учреждения «Подвязьевский детский сад» муниципального образования – Рязанский муниципальный район Рязанской области осуществляют обработку персональных данных либо имеют доступ к персональным данным

1. Заведующий муниципального бюджетного дошкольного образовательного учреждения «Подвязьевский детский сад» муниципального образования – Рязанский муниципальный район Рязанской области.
2. Заместитель заведующего по УВР муниципального бюджетного дошкольного образовательного учреждения «Подвязьевский детский сад» муниципального образования – Рязанский муниципальный район Рязанской области.

ПРИЛОЖЕНИЕ 5
к приказу муниципального бюджетного дошкольного образовательного учреждения «Подвязьевский детский сад» муниципального образования – Рязанский муниципальный район Рязанской области от «27» июля 2020 г. № 68/1-р

Обязательство
о прекращении обработки персональных данных в случае расторжения служебного контракта (трудового договора)

Я, _____ ,
(фамилия, имя, отчество)
паспорт серии _____ № _____ , выдан _____
_____
_____
_____ дата выдачи «___»_____ _____г.

работающий(ая) в должности
_____
_____
_____
_____
(должность, наименование структурного подразделения)

Настоящим добровольно принимаю на себя обязательства:

1. Прекратить обработку персональных данных субъектов персональных данных, которые мне доверены в связи с исполнением должностных обязанностей, в случае расторжения со мной служебного контракта (трудового договора).
2. После расторжения со мной служебного контракта (трудового договора) не разглашать и не передавать третьим лицам известную мне информацию, содержащую персональные данные.

_____ _____ _____
(дата) (подпись) (расшифровка подписи)

Я предупрежден (а) о том, что в случае разглашения мной сведений, касающихся персональных данных я несу ответственность, предусмотренную законодательством Российской Федерации.

_____ _____ _____
(дата) (подпись) (расшифровка подписи)

ПРИЛОЖЕНИЕ 6
к приказу муниципального бюджетного дошкольного образовательного учреждения «Подвязьевский детский сад» муниципального образования – Рязанский муниципальный район Рязанской области
от «27» июля 2020 г. № 68/1-р

Согласие
субъекта персональных данных на обработку персональных данных

Я, _____ ,
(фамилия, имя, отчество)
проживающий(ая) по адресу: _____
_____

паспорт серии _____ № _____
выдан _____
_____

дата выдачи «____» _____ г.

свободно, своей волей и в своем интересе в соответствии с требованиями Федерального закона от 27.07.06 № 152-ФЗ «О персональных данных» даю согласие уполномоченным должностным лицам **муниципального бюджетного дошкольного образовательного учреждения «Подвязьевский детский сад» муниципального образования – Рязанский муниципальный район Рязанской области**, адрес: 390502, Рязанская область, Рязанский район, с.Подвязье, ул. Садовая д.8 (далее – Оператор), на обработку* следующих персональных данных:

_____
_____
_____
_____
_____
_____
_____
_____

в целях:

_____
_____
_____

Срок действия Согласия на обработку персональных данных – с даты подписания Согласия, в течение _____.

Я предупрежден(а), что обработка моих персональных данных осуществляется с использованием бумажных носителей и средств вычислительной техники, с соблюдением принципов и правил обработки персональных данных, предусмотренных Федеральным законом «О персональных данных», а также необходимых правовых, организационных и технических мер, обеспечивающих их защиту от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

Согласие может быть досрочно отозвано путем подачи письменного заявления в адрес Оператора.

Я предупрежден(а), что в случае отзыва согласия на обработку персональных данных, Оператор вправе продолжить обработку персональных данных без согласия при наличии оснований, указанных в пп.2-11 ч.1 ст.6 и ч.2 ст.10 Федерального закона «О персональных данных».

(дата)	(подпись)	(расшифровка подписи)

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

ПРИЛОЖЕНИЕ 7
к приказу муниципального бюджетного дошкольного образовательного учреждения «Подвязьевский детский сад» муниципального образования – Рязанский муниципальный район Рязанской области
от «27» июля 2020 г. № 68/1-р

Разъяснение субъекту персональных данных (немуниципальному служащему) юридических последствий отказа предоставить свои персональные данные

Я, _____ ,
(фамилия, имя, отчество)
паспорт серии _____ № _____ , выдан _____
_____
_____
_____ дата выдачи «___»_____ _____г.

получил(а) разъяснения о юридических последствиях отказа предоставить свои персональные данные муниципальному бюджетному дошкольному образовательному учреждению «Подвязьевский детский сад» муниципального образования – Рязанский муниципальный район Рязанской области в соответствии с законодательством Российской Федерации.

В соответствии со статьей 65 Трудового кодекса Российской федерации субъект персональных данных при приеме на работу и заключении трудового договора, обязан представить определенный перечень информации о себе.

Без предоставления субъектом персональных данных обязательных для заключения трудового договора сведений, трудовой договор не может быть заключен.

На основании пункта 11 статьи 77 Трудового кодекса Российской Федерации трудовой договор прекращается вследствие нарушения установленных обязательных правил его заключения, если это нарушение исключает возможность продолжения работы.

_____ _____ _____
(дата) (подпись) (расшифровка подписи)

ПРИЛОЖЕНИЕ 8
к приказу муниципального бюджетного дошкольного образовательного учреждения «Подвязьевский детский сад» муниципального образования – Рязанский муниципальный район Рязанской области от «27» июля 2020 г. № 68/1-р

Разъяснение субъекту персональных данных (муниципальному служащему) юридических последствий отказа предоставить свои персональные данные

Я, _____ ,
(фамилия, имя, отчество)
паспорт серии _____ № _____ , выдан _____
_____
_____
_____ дата выдачи «___»_____ _____г.

получил(а) разъяснения о юридических последствиях отказа предоставить свои персональные данные муниципальному бюджетному дошкольному образовательному учреждению «Подвязьевский детский сад» муниципального образования – Рязанский муниципальный район Рязанской области в соответствии с законодательством Российской Федерации.

В соответствии со статьей 16 Федерального закона от 02.03.2007 г. N 25-ФЗ «О муниципальной службе в Российской Федерации» субъект персональных данных, поступающий на муниципальную службу, при заключении трудового договора обязан представить определенный перечень информации о себе.

Без предоставления субъектом персональных данных обязательных для заключения трудового договора сведений, трудовой договор не может быть заключен.

На основании пункта 11 статьи 77 Трудового кодекса Российской Федерации трудовой договор прекращается вследствие нарушения установленных обязательных правил его заключения, если это нарушение исключает возможность продолжения замещения муниципальным служащим должности муниципальной службы.

_____ _____ _____
(дата) (подпись) (расшифровка подписи)

ПРИЛОЖЕНИЕ 9
к приказу муниципального бюджетного дошкольного образовательного учреждения «Подвязьевский детский сад» муниципального образования – Рязанский муниципальный район Рязанской области
от «27» июля 2020 г. № 68/1-р

ПЕРЕЧЕНЬ
персональных данных, обрабатываемых в муниципальном бюджетном дошкольном образовательном учреждении «Подвязьевский детский сад» муниципального образования – Рязанский муниципальный район Рязанской области

– автобиография;
– адрес проживания;
– адрес регистрации;
– адрес электронной почты;
– банковские реквизиты;
– гражданство (подданство);
– данные документа, удостоверяющего личность;
– данные заграничного паспорта;
– данные медицинского страхового полиса;
– данные о командировках;
– данные об отпусках;
– данные трудовой книжки;
– дата выдачи документа, удостоверяющего личность;
– дата выхода на пенсию;
– дата обращения;
– дата регистрации по месту жительства;
– дата рождения;
– дата увольнения;
– должность;
– ИНН;
– информация о явках/неявках на работу;
– иные сведения, необходимые в целях оказания государственных и муниципальных услуг и осуществления функций, полномочий и обязанностей
– иные сведения, содержащиеся в обращении
– квалификация по документу об образовании;
– контактные телефоны (или иной вид связи);
– место работы;
– место рождения;
– место учебы;
– наименование органа, выдавшего документ, удостоверяющий личность;
– направление подготовки или специальность по документу об образовании;
– основание прекращения трудового договора (увольнения);
– ответ на обращение;
– отношение к воинской обязанности и воинское звание;
– период нетрудоспособности;
– пол;
– причина обращения;
– размер оклада;
– реквизиты документа об образовании;
– реквизиты листка нетрудоспособности;

– реквизиты трудового договора;
– реквизиты трудовой книжки;
– сведения о беременности;
– сведения о близких родственниках, постоянно проживающих за границей и (или) оформляющих документы для выезда на постоянное место жительства в другое государство;
– сведения о близких родственниках;
– сведения о владении иностранными языками;
– сведения о воинском учете;
– сведения о государственных и ведомственных наградах;
– сведения о донорстве (номер справки, дата сдачи крови);
– сведения о допуске к государственной тайне;
– сведения о доходах, расходах, об имуществе и обязательствах имущественного характера супруги (супруга) и несовершеннолетних детей;
– сведения о доходах, расходах, об имуществе и обязательствах имущественного характера;
– сведения о замещаемой должности;
– сведения о наградах (поощрениях);
– сведения о наличии (отсутствии) судимости;
– сведения о наличии гражданства другого государства;
– сведения о наличии инвалидности;
– сведения о пенсиях;
– сведения о повышении квалификации;
– сведения о послевузовском профессиональном образовании;
– сведения о постановке на учет в ранние сроки беременности;
– сведения о почетных званиях;
– сведения о пребывании за границей;
– сведения о приеме на работу и переводах на другие должности;
– сведения о присвоении квалификационного разряда, классного чина, дипломатического ранга, воинского звания;
– сведения о профессиональной переподготовке;
– сведения о прохождении медицинского осмотра;
– сведения о смене ФИО;
– сведения о собственности;
– сведения о составе семьи;
– сведения о социальных льготах, на которые работник имеет право в соответствии с законодательством;
– сведения о судимости;
– сведения о трудовой деятельности;
– сведения об адресах сайтов и (или) страниц сайтов в информационно-телекоммуникационной сети «Интернет»;
– сведения об аттестации;
– сведения об изменении гражданства;
– сведения об изменении ФИО близкими родственниками;
– сведения об образовании;
– сведения об увольнении;
– сведения, указанные в свидетельстве о государственной регистрации акта гражданского состояния;
– семейное положение;
– СНИЛС;
– стаж муниципальной службы;
– стаж работы;
– степень родства;
– структурное подразделение;
– суть обращения;
– табельный номер;
– ученая степень;

– ученое звание;
– ФИО;
– фотография;
– характер, вид работы;
– характеристика

ПРИЛОЖЕНИЕ 10
к приказу муниципального бюджетного дошкольного образовательного учреждения «Подвязьевский детский сад» муниципального образования – Рязанский муниципальный район Рязанской области
от «27» июля 2020 г. № 68/1-р

ПОРЯДОК
доступа в помещения муниципального бюджетного дошкольного образовательного учреждения «Подвязьевский детский сад» муниципального образования – Рязанский муниципальный район Рязанской области, в которых ведется обработка персональных данных

1. Доступ в помещения, в которых ведется обработка персональных данных, имеют следующие лица:

- заведующая муниципальным бюджетным дошкольным образовательным учреждением «Подвязьевский детский сад» муниципального образования – Рязанский муниципальный район Рязанской области;
- заместитель заведующего по учебной и воспитательной работе муниципального бюджетного дошкольного образовательного учреждения «Подвязьевский детский сад» муниципального образования – Рязанский муниципальный район Рязанской области;
- делопроизводитель муниципального бюджетного дошкольного образовательного учреждения «Подвязьевский детский сад» муниципального образования – Рязанский муниципальный район Рязанской области .

2. Лица, не имеющие доступа в помещения, где обрабатываются персональные данные, имеют право пребывать в указанных помещениях только в присутствии сотрудников, имеющих право доступа в них.

3. Персональные электронно-вычислительные машины, на которых обрабатываются персональные данные, должны размещаться так, чтобы исключить несанкционированный доступ к информации посторонних лиц.

4. Во время отсутствия в помещениях сотрудников двери должны быть закрыты на замок.

5. Ответственность за соблюдение порядка доступа в помещения, в которых ведется обработка персональных данных, возлагается на заведующую ДОУ.

ПРИЛОЖЕНИЕ 11
к приказу муниципального бюджетного дошкольного образовательного учреждения «Подвязьевский детский сад» муниципального образования – Рязанский муниципальный район Рязанской области
от «27» июля 2020 г. № 68/1-р

ПЕРЕЧЕНЬ
информационных систем в муниципальном бюджетном дошкольном образовательном учреждении «Подвязьевский детский сад» муниципального образования – Рязанский муниципальный район Рязанской области

№ п/п	Наименование	Содержание персональных данных, да/нет
1.	Электронная почта	да
2.	Официальный сайт ДОУ	да
3.	Государственная информационная система о государственных и муниципальных платежах Рязанской области	да
4.	ССТУ	да
5.	1С: Предприятие	да
6.	СБИС Электронная отчетность	да
7.	Официальный сайт для размещения информации о государственных (муниципальных) учреждениях	да
8.	Directum Система межведомственного электронного взаимодействия	да
9.	Кадровый учет	да
10.	Награждение сотрудников	нет
11.	Осуществление документооборота	да
12.	Работа с обращениями граждан	нет
13.	Сведения о доходах, расходах и обязательствах имущественного характера	да
14.	Оказание муниципальных услуг	да
15.	Федеральная информационная адресная система	да
16.	Государственная информационная система жилищно-коммунального хозяйства	нет

ПРИЛОЖЕНИЕ 12
к приказу муниципального бюджетного дошкольного образовательного учреждения «Подвязьевский детский сад» муниципального образования – Рязанский муниципальный район Рязанской области от «27» июля 2020 г. № 68/1-р

ИНСТРУКЦИЯ
ответственного за организацию обработки персональных данных в муниципальном бюджетном дошкольном образовательном учреждении «Подвязьевский детский сад» муниципального образования – Рязанский муниципальный район Рязанской области

1. Ответственный за организацию обработки персональных данных в муниципальном бюджетном дошкольном образовательном учреждении «Подвязьевский детский сад» муниципального образования – Рязанский муниципальный район Рязанской области (далее - ответственный за организацию обработки персональных данных) должен руководствоваться в своей деятельности Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», иными нормативными правовыми актами в области защиты персональных данных, настоящей должностной инструкцией.

2. Ответственный за организацию обработки персональных данных обязан:

- предоставлять субъекту персональных данных по его просьбе информацию;
- осуществлять внутренний контроль за соблюдением требований законодательства Российской Федерации при обработке персональных данных, в том числе требований к защите персональных данных;
- доводить до сведения лиц, осуществляющих обработку персональных данных либо имеющих доступ к персональным данным, положения законодательства Российской Федерации о персональных данных, локальных актов по вопросам обработки персональных данных, требования к защите персональных данных;
- организовывать прием и обработку обращений и запросов субъектов персональных данных или их представителей и (или) осуществлять контроль за приемом и обработкой таких обращений и запросов;
- хранить в тайне известные им персональные данные, информировать о фактах нарушения порядка обращения с персональными данными, о попытках несанкционированного доступа к ним;
- соблюдать правила использования персональных данных, порядок их учета и хранения, исключить доступ к ним посторонних лиц;
- обрабатывать только те персональные данные, к которым получен доступ в силу исполнения служебных обязанностей.

3. При обработке персональных данных ответственному за организацию обработки персональных данных запрещается:

- передавать персональные данные по незащищенным каналам связи (факсимильная связь, электронная почта и т.п.) без использования сертифицированных средств криптографической защиты информации;
- снимать копии с документов и других носителей информации, содержащих персональные данные, или производить выписки из них, а равно использовать различные технические средства (видео и звукозаписывающую аппаратуру) для фиксации сведений, содержащих персональные данные, без разрешения руководителя структурного подразделения ДОУ;
- выполнять на дому работы, связанные с использованием персональных данных, выносить документы и другие носители информации, содержащие персональные данные.

4. Допуск ответственного за организацию обработки персональных данных к работе с персональными данными осуществляется после изучения им требований нормативных правовых документов в части, его касающейся, и подписания обязательства о соблюдении режима конфиденциальности персональных данных.

5. Ответственный за организацию обработки персональных данных, виновный в нарушении требований законодательства о защите персональных данных, в том числе допустивший разглашение персональных данных, несет предусмотренную законодательством Российской Федерации ответственность.

ПРИЛОЖЕНИЕ 13
к приказу муниципального бюджетного дошкольного образовательного учреждения «Подвязьевский детский сад» муниципального образования – Рязанский муниципальный район Рязанской области
от «27» июля 2020 г. № 68/1-р

ИНСТРУКЦИЯ
по работе ответственного за эксплуатацию объекта информатизации в муниципальном бюджетном дошкольном образовательном учреждении «Подвязьевский детский сад» муниципального образования – Рязанский муниципальный район Рязанской области

1. Общие положения

Настоящая инструкция определяет права и обязанности администратора автоматизированных рабочих мест в муниципальном бюджетном дошкольном образовательном учреждении «Подвязьевский детский сад» муниципального образования – Рязанский муниципальный район Рязанской области (далее соответственно – АРМ, Администратор), ответственного за эксплуатацию автоматизированного рабочего места заведующего муниципальным бюджетным дошкольным образовательным учреждением «Подвязьевский детский сад» муниципального образования – Рязанский муниципальный район Рязанской области (далее – АРМ Администратора).

1.1. Администратор назначается распоряжением муниципального бюджетного дошкольного образовательного учреждения «Подвязьевский детский сад» муниципального образования – Рязанский муниципальный район Рязанской области.

1.2. Администратор отвечает за обеспечение возможности эксплуатации АРМ, в том числе АРМ Администратора.

1.3. Требования Администратора, связанные с выполнением им своих обязанностей, обязательны для исполнения всеми пользователями АРМ, в том числе АРМ Администратора.

1.4. Администратор несет персональную ответственность за качество проводимых им работ по администрированию АРМ, в том числе АРМ Администратора, состояние и поддержание уровня защищенности информации и класса защищенности, содержащейся на АРМ, в том числе АРМ Администратора.

2. Задачи Администратора

2.1. Основными задачами Администратора являются:
– обеспечение возможности эксплуатации АРМ, в том числе АРМ Администратора;
– администрирование АРМ, в том числе АРМ Администратора.
2.2. В рамках выполнения основных задач Администратор осуществляет:
– создание учётных записей пользователей АРМ, в том числе пользователей АРМ Администратора;
– контроль за событиями безопасности и действиями пользователей АРМ, в том числе пользователей АРМ Администратора;
– контроль выполнения пользователями АРМ, в том числе пользователями АРМ Администратора мероприятий по обеспечению безопасности информации АРМ, в том числе АРМ Администратора;
– методическую помощь пользователям АРМ, в том числе АРМ Администратора.

3. Обязанности Администратора

3.1. Администратор обязан:

– знать и выполнять требования нормативных документов по защите информации, регламентирующих порядок защиты информации, в том числе персональных данных (далее – ПДн), обрабатываемых на АРМ и АРМ Администратора;

– осуществлять общее руководство деятельности по обработке информации, в том числе, ПДн на АРМ и АРМ Администратора;

– участвовать в разработке организационно-распорядительной документации по вопросам обеспечения безопасности информации, содержащейся в АРМ и АРМ Администратора;

– анализировать состояние работоспособности и защищённости АРМ и АРМ Администратора

– контролировать правильность функционирования прикладного программного обеспечения АРМ и АРМ Администратора и неизменность его настроек;

– контролировать исполнение пользователями АРМ и АРМ Администратора введенного режима безопасности, а также правильность работы с элементами АРМ и АРМ Администратора;

– периодически анализировать журналы учета событий безопасности, регистрируемых прикладным программным обеспечением АРМ и АРМ Администратора, с целью контроля действий пользователей и выявления возможных нарушений;

– контролировать выполнение администратором безопасности и пользователями АРМ, в том числе АРМ Администратора, своих обязанностей;

– периодически представлять руководителю отчет о состоянии АРМ, АРМ Администратора и о нештатных ситуациях и допущенных пользователями и администратором безопасности нарушениях установленных требований по защите информации;

– в случае выявления нарушений режима безопасности информации (в том числе ПДн), а также возникновения внештатных и аварийных ситуаций, принимать необходимые меры с целью ликвидации их последствий и определению причин их появления;

– принимать участие в проведении работ по оценке АРМ, в том числе АРМ Администратора, требованиям безопасности информации.

4. Права Администратора

4.1. Администратор имеет право:

– давать пользователям АРМ и АРМ Администратора обязательные для исполнения указания и рекомендации по вопросам безопасной эксплуатации прикладного программного обеспечения АРМ и АРМ Администратора;

– проводить служебные расследования по фактам нарушений установленных требований обеспечения информационной безопасности (далее – ИБ), несанкционированного доступа (далее – НСД), утраты, порчи защищаемой информации и технических средств АРМ и АРМ Администратора;

– организовывать и участвовать в любых проверках по использованию пользователями АРМ и АРМ Администратора;

– запрещать устанавливать на АРМ нештатное программное и аппаратное обеспечение;

– запрашивать и получать материалы, необходимые для организации своей работы;

– вносить на рассмотрение предложения по улучшению состояния ИБ, обрабатываемой в АРМ и АРМ Администратора, по замене вышедших из строя элементов системы защиты информации АРМ и АРМ Администратора, а также по выведению из эксплуатации машинных носителей персональных данных, у которых закончился период эксплуатации, установленный их производителем.

5. Ответственность Администратора

5.1. Администратор несет ответственность:

– за организацию безопасной эксплуатации АРМ и АРМ Администратора;

– за выполнение установленных условий функционирования АРМ и АРМ Администратора;

– за качество выполнения обязанностей, установленных настоящей Инструкцией;

– за качество проводимых работ по контролю действий администратора безопасности и пользователей АРМ, в том числе АРМ Администратора, состояние и поддержание необходимого уровня защищенности и класса защищенности информационных и технических АРМ, в том числе АРМ Администратора;

– за качество и состояние организационно-распорядительной и эксплуатационной документации по вопросам эксплуатации АРМ, в том числе АРМ Администратора;

– за разглашение сведений ограниченного доступа (ПДн, иная защищаемая информация), ставших известными ему по роду работы.

ПРИЛОЖЕНИЕ 14
к приказу муниципального бюджетного дошкольного образовательного учреждения «Подвязьевский детский сад» муниципального образования – Рязанский муниципальный район Рязанской области
от «27» июля 2020 г. № 68/1-р

ИНСТРУКЦИЯ
пользователя информационной системы персональных данных в муниципальном бюджетном дошкольном образовательном учреждении «Подвязьевский детский сад» муниципального образования – Рязанский муниципальный район Рязанской области

1.Общие положения

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

1.2. Пользователем является каждый сотрудник муниципального бюджетного дошкольного образовательного учреждения «Подвязьевский детский сад» муниципального образования – Рязанский муниципальный район Рязанской области (далее – ДОУ), участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки информации и имеющий доступ к аппаратным средствам, программному обеспечению, данным и средствам защиты.

1.3. Пользователь несет персональную ответственность за свои действия.

1.4. Пользователь в своей работе руководствуется настоящей инструкцией, и нормативными документами ДОУ.

1.5. Методическое руководство работой пользователя осуществляется ответственным за обеспечение защиты персональных данных.

2.Должностные обязанности

Пользователь обязан:

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

2.2. Выполнять на автоматизированном рабочем месте (АРМ) только те процедуры, которые определены для него в Положении об организации работы с персональными данными в ДОУ.

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

2.4. Соблюдать требования инструкции по организации парольной защиты

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

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

2.7. Обо всех выявленных нарушениях, связанных с информационной безопасностью ДОУ, а также для получений консультаций по вопросам информационной безопасности, необходимо обращаться к Администратору безопасности персональных данных ДОУ.

2.8. Для получения консультаций по вопросам работы и настройке элементов ИСПДн необходимо обращаться к Администратору безопасности персональных данных ДОУ.

2.9. Пользователям запрещается:

- разглашать защищаемую информацию третьим лицам;
- копировать защищаемую информацию на внешние носители без разрешения своего руководителя;
- самостоятельно устанавливать, тиражировать, или модифицировать программное обеспечение и аппаратное обеспечение, изменять установленный алгоритм функционирования технических и программных средств;
- несанкционированно открывать общий доступ к папкам на своей рабочей станции;
- запрещено подключать к рабочей станции и корпоративной информационной сети личные внешние носители и мобильные устройства;
- отключать (блокировать) средства защиты информации;
- обрабатывать на АРМ информацию и выполнять другие работы, не предусмотренные перечнем прав пользователя по доступу к ИСПДн;
- сообщать (или передавать) посторонним лицам личные ключи и атрибуты доступа к ресурсам ИСПДн;
- привлекать посторонних лиц для производства ремонта или настройки АРМ, без согласования с ответственным за обеспечение защиты персональных данных.

2.10. При отсутствии визуального контроля за АРМ доступ к компьютеру должен быть немедленно заблокирован. Для этого необходимо нажать одновременно комбинацию клавиш <Ctrl><Alt><Del> и выбрать опцию «Блокировка».

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

3. Правила работы в сетях общего доступа и (или) международного обмена

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

3.2. При работе в Сети запрещается:

- осуществлять работу при отключенных средствах защиты (антивирус и других);
- передавать по Сети защищаемую информацию без использования средств шифрования;
- запрещается скачивать из Сети программное обеспечение и другие файлы;
- запрещается посещение сайтов сомнительной репутации (порно-сайты, сайты, содержащие нелегально распространяемое ПО и другие);
- запрещается нецелевое использование подключения к Сети.

4. Права и ответственность пользователей ИСПДн

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

4.2 Пользователи, виновные в несоблюдении Настоящей инструкции, несут предусмотренную законодательством Российской Федерации ответственность.

ПРИЛОЖЕНИЕ 15
к приказу муниципального бюджетного дошкольного образовательного учреждения «Подвязьевский детский сад» муниципального образования – Рязанский муниципальный район Рязанской области
от «27» июля 2020 г. № 68/1-р

ИНСТРУКЦИЯ
по работе администратора безопасности информации информационной системы персональных данных в муниципальном бюджетном дошкольном образовательном учреждении «Подвязьевский детский сад» муниципального образования – Рязанский муниципальный район Рязанской области

1. Общие положения

1.1 Администратор безопасности информации (далее - АБИ) - лицо, выполняющее функции по настройке и сопровождению всех программных и технических средств защиты информации информационной системы персональных данных, предназначенных для обработки информации, содержащей персональные данные (далее ИСПДн).

1.2 АБИ в пределах своих функциональных обязанностей обеспечивает безопасность информации, обрабатываемой, передаваемой и хранимой в ИСПДн.

1.3 АБИ назначается распоряжением заведующего муниципальным бюджетным дошкольным образовательным учреждением «Подвязьевский детский сад» муниципального образования – Рязанский муниципальный район Рязанской области.

1.4 АБИ в своей работе руководствуется положениями нормативно - правовых актов РФ, руководящими документами по безопасности информации, актами муниципального бюджетного дошкольного образовательного учреждения «Подвязьевский детский сад» муниципального образования – Рязанский муниципальный район Рязанской области и положениями настоящей Инструкции.

2. Обязанности АБИ

Основными обязанностями АБИ являются:

- управление средствами и системами защиты информации (далее - СЗИ) информационных систем персональных данных (далее – ИСПДн) и поддержание их функционирования;
- восстановление функций программных и технических систем защиты информации (далее – СЗИ) от несанкционированного доступа (далее – НСД) к информации;
- генерация ключей, личных идентификаторов, а также паролей для пользователей автоматизированных систем (далее – АС);
- формирование и управление списком необходимых реквизитов и значением атрибутов объектов и субъектов доступа;
- обеспечение правильной эксплуатации технических и программных СЗИ в ИСПДн;
- контроль целостности эксплуатируемого в ИСПДн программного обеспечения, в том числе самих СЗИ, с целью недопущения и выявления несанкционированных модификаций;
- текущий, после сбоев и периодический (не реже 1 раза в год) контроль работоспособности средств и систем защиты информации от НСД;
- контроль соблюдения пользователями ИСПДн требований инструкций и порядка работы при обработке информации в ИСПДн, по вопросам защиты информации от НСД;
- выполнение резервного копирования машинных документов, содержащих персональные данные;

• организация антивирусной защиты информации и программных средств в ИСПДн.

3. Права АБИ

АБИ имеет право:

• Останавливать обработку информации в ИСПДн в случаях подтвержденных нарушений установленной обработки данных, приводящих к нарушению функционирования СЗИ.

4. Ответственность АБИ

4.1 На АБИ возлагается персональная ответственность за качество и полноту проводимых им работ по обеспечению защиты информации в соответствии с его функциональными обязанностями.

4.2 АБИ несет ответственность по законодательству РФ за нарушение требований нормативно - методических документов по защите информации и настоящей инструкции.

ПРИЛОЖЕНИЕ 16
к приказу муниципального
бюджетного дошкольного
образовательного учреждения
«Подвязьевский детский сад»
муниципального образования –
Рязанский муниципальный район
Рязанской области от «27» июля 2020
г. № 68/1-р

ИНСТРУКЦИЯ
по организации парольной защиты
в информационных системах администрации муниципального бюджетного дошкольного образовательного учреждения «Подвязьевский детский сад» муниципального образования – Рязанский муниципальный район Рязанской области.

1. Общие положения

1.1. Данная инструкция по организации парольной защиты в автоматизированных рабочих местах и информационных системах (далее – ИС) муниципального бюджетного дошкольного образовательного учреждения «Подвязьевский детский сад» муниципального образования – Рязанский муниципальный район Рязанской области регламентирует процессы генерации, смены и прекращения действия паролей (удаления учётных записей пользователей) в ИС, а также контроль над действиями пользователей и обслуживающего персонала информационных систем при работе с паролями.

1.2. Осуществление процессов генерации, использования, смены и прекращения действия паролей в ИС и контроль за действиями исполнителей и обслуживающего персонала информационной системы при работе с паролями возлагается на администратора информационной безопасности информационных систем и информационных систем персональных данных (далее – администратор безопасности ИС).

2. Термины и определения

2.1. Информация - сведения (сообщения, данные) независимо от формы их представления (ст. 2 ФЗ РФ от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и защите информации»).

2.2. Персональные данные - любая информация, относящаяся к прямо или косвенно определенному, или определяемому физическому лицу (субъекту персональных данных) (ст. 3 ФЗ РФ от 27.07.2006 № 152-ФЗ «О персональных данных»).

2.3. Пароль - секретная комбинация цифр, знаков, слов, или осмысленное предложение, служащие для защиты информации от несанкционированного доступа к информационным ресурсам.

2.4. Компрометация пароля – раскрытие, обнаружение или утеря пароля.

3. Правила формирования паролей

3.1. Личные пароли должны генерироваться и распределяться централизованно.

3.2. Ответственность за правильность формирования и распределения паролей в ИС возлагается на администратора безопасности ИС.

3.3. Ответственность за правильность формирования и распределения паролей для доступа на автоматизированные рабочие места гражданских служащих ИС возлагается на системного администратора ИС.

3.4. При ручном назначении пароля он должен соответствовать следующим параметрам:

3.5. Длина пароля должна быть не менее 6 символов.

3.6. Пароль должен содержать комбинацию букв в верхнем и нижнем регистре, а также цифры, знаки препинания и/или специальные символы (@,#, $, %, ^, &, * и т.п.).

3.7. Пароль не должен включать в себя слова, которые содержатся в словарях (русских или иностранных), имена, фамилии и отчества людей, клички животных, имена вымышленных персонажей, различные географические наименования, даты рождения, номера телефонов и другую личную информацию.

3.8. При смене пароля новое значение должно отличаться от предыдущего не менее чем в 4 позициях.

4. Порядок смены личных паролей

4.1. Смена паролей доступа в ИС должна проводиться регулярно, не реже одного раза в 60 дней, централизованно, администратором безопасности ИС.

4.2. В случае прекращения полномочий пользователя (увольнение, переход на другую работу и т.п.) должно производиться немедленное удаление его учетных записей доступа в ИС, а также учетные данные для доступа на автоматизированное рабочее место.

4.3. Срочная (внеплановая) полная смена паролей должна производиться в случае прекращения полномочий (увольнение, переход на другую работу и т.п.) ответственного за защиту персональных данных, администратора безопасности информационных систем и других сотрудников Администрации, которым по роду работы были предоставлены полномочия по управлению системой парольной защиты.

5. Хранение пароля.

5.1. Запрещается входить в ИС под учетной записью и паролем другого пользователя.

6. Действия в случае утери и компрометации пароля.

6.1. В случае подозрения в компрометации пароля пользователя должна быть немедленно проведена внеплановая процедура смены пароля.

6.2. По факту компрометации пароля может быть проведено служебное расследование.

7. Ответственность при организации парольной защиты.

7.1. Каждый пользователь ИС несет персональную ответственность за соблюдение требований настоящей Инструкции и за все действия, совершенные от имени его учетной записи в ИС, если с его стороны не было предпринято необходимых действий для предотвращения компрометации пароля его учетной записи.

7.2. Ответственность за контроль проведения мероприятий по организации парольной защиты в ИС возлагается на администратора безопасности ИС.

7.3. За разглашение информации ограниченного доступа и нарушение порядка работы с ИС, обрабатывающей информацию ограниченного доступа, сотрудники Администрации могут быть привлечены к гражданской, уголовной, административной, дисциплинарной и иной предусмотренной законодательством Российской Федерации ответственности.

ПРИЛОЖЕНИЕ 17
к приказу муниципального
бюджетного дошкольного
образовательного учреждения
«Подвязьевский детский сад»
муниципального образования –
Рязанский муниципальный район
Рязанской области от «27» июля 2020
г. № 68/1-р

ИНСТРУКЦИЯ
по управлению доступом к персональным данным в информационных системах персональных данных муниципального бюджетного дошкольного образовательного учреждения «Подвязьевский детский сад» муниципального образования – Рязанский муниципальный район Рязанской области

1. Введение

1.1. Настоящая инструкция предназначена для обеспечения защиты персональных данных (далее – ПДн), содержащихся в информационной системе персональных данных (далее – ИСПДн) муниципального бюджетного дошкольного образовательного учреждения «Подвязьевский детский сад» муниципального образования – Рязанский муниципальный район Рязанской области (далее - ДОУ) при разграничении доступа пользователей к ресурсам и информации, содержащейся в ИСПДн.

1.2. Настоящая инструкция определяет порядок действий администратора безопасности и пользователей ИСПДн при разграничении доступа к ресурсам и информации ИСПДн.

2. Матрица доступа

2.1. Разграничение доступа к ресурсам и информации ИСПДн осуществляет и контролирует администратор безопасности путем настройки программно – технических средств и средств защиты информации (далее – СЗИ) ИСПДн на основании журнала учета выдачи паролей и матрицы доступа.

2.2. Матрица доступа к ресурсам ИСПДн ДОУ утверждается распоряжением.

2.3. Сохранность, конфиденциальность и актуальность матрицы доступа обеспечивает администратор безопасности.

3. Порядок доступа без ввода пароля

3.1. Вход в ИСПДн и действия с ресурсами ИСПДн до процедур идентификации и аутентификации разрешен администратору безопасности для восстановления ИСПДн после сбоев и аварий технических средств ИСПДн. Срок действия разрешения заканчивается в момент запуска ИСПДн после восстановления.

3.2. Доступ к ресурсам ИСПДн до момента прохождения процедур идентификации и аутентификации остальным пользователям запрещен.

4. Порядок предоставления удаленного доступа

4.1. Удаленный доступ пользователей к информационным ресурсам ИСПДн возможен только с помощью технических средств (персональный компьютер, ноутбук, планшет, сотовый телефон) являющихся собственностью ДОУ и внесенных в журнал разрешенных устройств удаленного доступа (приложение 1 к настоящей Инструкции).

4.2. Выдачу, учет, хранение, настройку программного обеспечения, установку программного обеспечения и его обновление, антивирусную защиту технических средств удаленного доступа осуществляет администратор безопасности. Все данные по конфигурации и настройкам должны быть записаны в журнал разрешенных устройств удаленного доступа.

4.3. При настройке средств удаленного доступа к ресурсам ИСПДн администратор безопасности осуществляет возможность удаленного доступа к ресурсам ИСПДн с автоматической аутентификацией средств удаленного доступа.

4.4. Указанные в пункте 4 требования подлежат исполнению только в случае, если предусмотрен доступ к ресурсам ИСПДн с использованием информационно-телекоммуникационной сети Интернет.

5. Порядок использования мобильных технических средств

5.1. К мобильным техническим средствам ДОУ отнесены все переносные технические устройства, на которые может быть записана и с помощью которых может быть осуществлена обработка информации, содержащейся в ИСПДн.

5.2. Все мобильные технические средства ДОУ должны быть учтены и идентифицированы. Учет мобильных технических средств осуществляет администратор безопасности в журнале учета разрешенных мобильных технических средств (приложение 2 к настоящей Инструкции).

5.3. При передаче мобильных технических средств на ремонт или техническое обслуживание администратор безопасности полностью очищает их от информации, имеющей отношение к ИСПДн.

5.4. Указанные в пункте 5 требования подлежат исполнению только в случае, если предусмотрен доступ к ресурсам ИСПДн с использованием мобильных технические средств.

6. Взаимодействие с внешними информационными системами (внешними пользователями)

6.1. Пользователям внешних информационных систем (внешним пользователям) доступ к ресурсам ИСПДн устанавливают в матрице доступа.

6.2. Администратор безопасности осуществляет процедуру доступа внешних пользователей к ресурсам ИСПДн в соответствии с пунктом 2 настоящей Инструкции.

7. Заключительные положения

7.1. Все пользователи ИСПДн должны быть предупреждены об ответственности за действия с получением доступа к ресурсам ИСПДн, нарушающие требования настоящей инструкции.

7.2. Пользователи ИСПДн должны быть ознакомлены с настоящей инструкцией до начала работы с ИСПДн. Обязанность ознакомления пользователей информационной системы с настоящей инструкцией лежит на администраторе безопасности.

7.3. Сотрудники ДОУ несут ответственность за ненадлежащее исполнение или неисполнение своих обязанностей, предусмотренных настоящей Инструкцией, в пределах, определенных действующим законодательством Российской Федерации.

ПРИЛОЖЕНИЕ 1
к инструкции по управлению доступом к персональным данным в информационных системах персональных данных в муниципальном бюджетном дошкольном образовательном учреждении «Подвязьевский детский сад» муниципального образования – Рязанский муниципальный район Рязанской области

муниципальное бюджетное дошкольное образовательное учреждение «Подвязьевский детский сад» муниципального образования – Рязанский муниципальный район Рязанской области

ЖУРНАЛ
учета разрешенных средств удаленного доступа

Учетный № _____
2_____ год. Листов (_____)

№	Наименование	Инв. №	Состояние	Пользователь	Дата выдачи/ роспись	Дата возврата/ роспись
1	2	3	4	5	6	7

ПРИЛОЖЕНИЕ 2
к инструкции по управлению доступом к персональным данным в информационных системах персональных данных муниципального бюджетного дошкольного образовательного учреждения «Подвязьевский детский сад» муниципального образования – Рязанский муниципальный район Рязанской области

муниципальное бюджетное дошкольное образовательное учреждение «Подвязьевский детский сад» муниципального образования – Рязанский муниципальный район Рязанской области

ЖУРНАЛ
учета разрешенных мобильных технических средств

Учетный № _____
2_____ год. Листов (_____)

№	Наименование	Инв. №	Состояние	Пользователь	Дата выдачи/ роспись	Дата возврата/ роспись
1	2	3	4	5	6	7

ПРИЛОЖЕНИЕ 18
к приказу муниципального бюджетного дошкольного образовательного учреждения «Подвязьевский детский сад» муниципального образования – Рязанский муниципальный район Рязанской области от «27» июля 2020 г. № 68/1-р

ИНСТРУКЦИЯ
по защите машинных носителей персональных данных, используемых в информационной системе персональных данных муниципального бюджетного дошкольного образовательного учреждения «Подвязьевский детский сад» муниципального образования – Рязанский муниципальный район Рязанской области

1. Введение

1.1. Настоящая инструкция определяет порядок учета, хранения, выдачи, уничтожения и ограничения использования машинных носителей информации в муниципальном бюджетном дошкольном образовательном учреждении «Подвязьевский детский сад» муниципального образования – Рязанский муниципальный район Рязанской области (далее – ДОУ).

1.2. Машинный носитель информации (далее – МНИ) – это материальный носитель, используемый для передачи и хранения защищаемой информации в электронном виде, в том числе персональных данных (далее – ПДн). МНИ делятся на съемные и несъемные носители.

1.2.1. Несъемные МНИ являются частью автоматизированного рабочего места (далее – АРМ) или сервера и в процессе эксплуатации не предполагают демонтаж.

1.2.2. К съемным носителям относятся любые технические устройства, предназначенные для запоминания информации, оперативно подключаемые к АРМ или серверу в целях записи на них информации из памяти АРМ (или сервера) или считывания с них информации в память АРМ (или сервера).

2. Учет машинных носителей информации

2.1. Все используемые в информационной системе персональных данных Администрации (далее – ИСПДн) МНИ подлежат учёту.

2.2. Учет, хранение и выдачу носителей информации осуществляет администратор безопасности. При увольнении администратора безопасности составляется акт приема-сдачи учетных документов и носителей.

2.3. Учет всех видов и типов носителей информации производится в Журнале учета машинных носителей информации (Приложение №1 к настоящей Инструкции).

2.4. На несъемную часть носителей ИСПДн наносится уникальный в пределах ДОУ учетный номер.

3. Выдача машинных носителей информации

3.1. Пользователи ИСПДн получают учтенный носитель от администратора безопасности, для выполнения работ на конкретный срок.

3.2. При получении пользователем носителя информации делается соответствующая запись в Журнале учета машинных носителей информации.

3.3. По окончании работ или установленного срока использования пользователь ИСПДн сдает носитель информации администратору безопасности, о чем делается соответствующая запись в Журнале учета машинных носителей информации.

4. Использование и передача машинных носителей информации

4.1. На МНИ записываются исключительно ПДн и программные средства обработки ПДн, содержащихся в ИСПДн.

4.2. Носители информации, допускающие повторную запись информации, проходят процедуру многократной перезаписи общедоступной информации перед повторным использованием или ремонтом с целью гарантированного уничтожения остаточной информации. Процедуру перезаписи организует и контролирует администратор безопасности.

4.3. ПДн, используемые в различных целях, записываются на разные носители.

4.4. Вынос учтенных носителей информации за пределы установленных мест обработки ПДн допустим только с письменного разрешения ответственного за организацию обработки ПДн.

4.5. Передача носителей, содержащих ПДн, которые обрабатываются в ИСПДн сторонним организациям или третьим лицам производится через администратора безопасности. Администратор безопасности производит в этом случае необходимые отметки в Журнале учета машинных носителей информации.

5. Хранение машинных носителей информации

5.1. Хранение МНИ осуществляется в условиях, препятствующих несанкционированному ознакомлению с информацией, копированию, изменению или уничтожению информации, содержащейся на машинных носителях.

5.2. МНИ хранятся в служебных помещениях, в отведенных для этих целей хранилищах, исключающих несанкционированный доступ к ним.

5.3. ЗАПРЕЩАЕТСЯ хранить носители информации на рабочих столах, оставлять их без присмотра, передавать на хранение третьим лицам.

6. Действия при утрате или порче машинных носителей информации

6.1. В случае утраты или порчи пользователем МНИ, содержащих ПДн, которые обрабатываются в ИСПДн, немедленно ставится в известность администратор безопасности. Администратор безопасности вносит соответствующую запись в Журнал учета машинных носителей информации и докладывает об инциденте ответственному за организацию обработки ПДн.

6.2. По факту утраты или порчи МНИ ответственным за организацию обработки ПДн проводится служебное расследование в установленном порядке.

6.3. Носители, пришедшие в негодность или с истекшим сроком эксплуатации, подлежат уничтожению в установленном порядке.

7. Уничтожение машинных носителей информации

7.1. Уничтожение МНИ организует администратор безопасности с предоставлением Акта уничтожения машинных носителей информации (ПРИЛОЖЕНИЕ 2 к настоящей Инструкции) ответственному за организацию обработки ПДн. Акт подписывает администратор безопасности.

7.2. Уничтожение носителей информации производится способом, гарантирующим невозможность восстановления информации, содержавшейся на носителе. Такими способами являются: механическое, электрическое, электромагнитное, химическое или термическое воздействие на носитель, применение специального программного обеспечения для уничтожения информации на носителе. Способ уничтожения выбирается администратором безопасности в зависимости от типа носителя и возможностей Администрации.

8. Ограничения и ответственность

8.1. Всем пользователям ИСПДн запрещено использовать учтенные МНИ для личных целей.

8.2. Пользователям ИСПДн запрещено передавать носители информации кому-либо, осуществлять учет, хранение и выдачу носителей информации, обрабатываемой в ИСПДн. Передача носителей информации осуществляется в порядке, предусмотренном пунктами 4.5, 4.6 настоящей Инструкции.

8.3. Любое взаимодействие (чтение, запись информации, запуск программного обеспечения) между техническими средствами ИСПДн, СЗИ и неучтенными носителями информации запрещено.

8.4. В случае выявления фактов утраты, несанкционированного и (или) нецелевого использования учтенных носителей информации, использования неучтенных (личных) носителей информации в ИСПДн назначается служебное расследование. По результату расследования и по представлению ответственного за организацию обработки ПДн, заведующий муниципальным бюджетным дошкольным образовательным учреждением «Подвязьевский детский сад» муниципального образования – Рязанский муниципальный район Рязанской области принимает решение о привлечении пользователя ИСПДн к ответственности согласно нормативным актам ДОУ и действующему законодательству.

8.5. Сотрудники ДОУ, несут ответственность за ненадлежащее исполнение или неисполнение своих обязанностей, предусмотренных настоящей Инструкцией, в пределах, определенных действующим законодательством Российской Федерации.

9. Заключительные положения

9.1. Пользователи ИСПДн должны быть предупреждены об ответственности за невыполнение требований настоящей Инструкции и ознакомлены с Инструкцией до начала работы в ИСПДн.

9.2. Обязанность ознакомления пользователей ИСПДн с настоящей Инструкцией лежит на ответственном за организацию обработки ПДн.

ПРИЛОЖЕНИЕ 1
к инструкции по защите машинных носителей персональных данных, используемых в информационной системе персональных данных муниципального бюджетного дошкольного образовательного учреждения «Подвязьевский детский сад» муниципального образования – Рязанский муниципальный район Рязанской области.

муниципальное бюджетное дошкольное образовательное учреждение «Подвязьевский детский сад» муниципального образования – Рязанский муниципальный район Рязанской области

ЖУРНАЛ
учета машинных носителей персональных данных

Учетный № _____20_____ год.

Листов (_____)

Учетный / заводской номер	Наименование (марка) носителя	Вид носителя (съемный /несъемный)	Цель обработки хранимых ПДн	Место установки (для несъемных носителей)	Ф.И.О. лица, эксплуатирующего носитель	Дата получения съемного носителя и подпись	Дата возврата съемного носителя и подпись администратора	Отметка об уничтожении носителя
1	2	3	4	5	6	7	8	9

ПРИЛОЖЕНИЕ 2
к инструкции по защите машинных носителей персональных данных, используемых в информационной системе персональных данных муниципального бюджетного дошкольного образовательного учреждения «Подвязьевский детский сад» муниципального образования – Рязанский муниципальный район Рязанской области

АКТ
уничтожения носителей персональных данных

Комиссия, назначенная приказом заведующего муниципальным бюджетным дошкольным образовательным учреждением «Подвязьевский детский сад» муниципального образования – Рязанский муниципальный район Рязанской области, в составе:

Председателя комиссии _____

и членов комиссии _____
_____

настоящим актом подтверждает, что:

1. _____
(наименование цифровых носителей ПДн их серийные номера и номера в журнале учета носителей)

_____
_____

2. _____
(наименование цифровых носителей ПДн их серийные номера и номера в журнале учета носителей)

_____
_____

3. _____
(наименование цифровых носителей ПДн их серийные номера и номера в журнале учета носителей)

_____
_____

4. _____
(наименование цифровых носителей ПДн их серийные номера и номера в журнале учета носителей)

_____
_____

уничтожены по причине их неработоспособности в кабинете №__ путем разрушения их целостности "____" _____ 20_ г.

Председатель комиссии _____

_____ (подпись) (инициалы, фамилия)

Члены комиссии ___ _____

_____ (подпись) (инициалы, фамилия)

_____

_____ (подпись) (инициалы, фамилия)

АКТ
уничтожения персональных данных муниципального бюджетного дошкольного образовательного учреждения «Подвязьевский детский сад» муниципального образования – Рязанский муниципальный район Рязанской области.

«___« _____20 г.

Председатель комиссии _____
(Ф.И.О.)

Член комиссии: _____
(Ф.И.О.)

составили настоящий акт в том, что «___» _____ 20__ г. произведено уничтожение персональных данных, находящейся на

_____
(наименование носителя персональных данных, Ф.И.О. ответственного

_____
способ уничтожения информации)

Председатель комиссии: _____
(подпись)

Член комиссии: _____
(подпись)

ПРИЛОЖЕНИЕ 19
к приказу муниципального
бюджетного дошкольного
образовательного учреждения
«Подвязьевский детский сад»
муниципального образования –
Рязанский муниципальный район
Рязанской области от «27» июля 2020
г. № 68/1-р

Инструкция
ответственного пользователя средств криптографической защиты информации в муниципальном бюджетном дошкольном образовательном учреждении «Подвязьевский детский сад» муниципального образования – Рязанский муниципальный район Рязанской области

1. Общие положения

1.1. Настоящая Инструкция ответственного пользователя средств криптографической защиты информации (далее – Инструкция) муниципального бюджетного дошкольного образовательного учреждения «Подвязьевский детский сад» муниципального образования – Рязанский муниципальный район Рязанской области (далее –ДОУ) определяет основные обязанности и права ответственного пользователя средств криптографической защиты информации.

1.2. Ответственный пользователь средств криптографической защиты информации назначается заведующим муниципального бюджетного дошкольного образовательного учреждения «Подвязьевский детский сад» муниципального образования – Рязанский муниципальный район Рязанской области и отвечает за организацию, обеспечение функционирования и безопасности средств криптографической защиты информации (далее - СКЗИ), предназначенных для защиты персональных данных при их обработке в информационных системах персональных данных (далее - ИСПДн).

1.3. Ответственный пользователь СКЗИ должен знать нормативные акты Российской Федерации и Рязанской области, методические материалы в сфере обработки персональных данных, в том числе распорядительные документы Администрации в сфере обработки персональных данных.

1.4. В своей деятельности, связанной с обработкой персональных данных, ответственный пользователь СКЗИ руководствуется настоящей Инструкцией.

2. Обязанности ответственного пользователя СКЗИ

Ответственный пользователь СКЗИ обязан:

2.1. Соблюдать требования Нормативных актов, устанавливающих порядок работы с персональными данными.

2.2. Осуществлять текущий контроль за организацией, обеспечением функционирования и безопасности СКЗИ, предназначенных для защиты персональных данных при их обработке в информационных системах персональных данных:

- контролировать соблюдение условий использования СКЗИ, предусмотренных эксплуатационной и технической документацией к ним;
- обеспечивать надежное хранение эксплуатационной и технической документации к СКЗИ, ключевых документов, носителей информации ограниченного распространения;
- вносить предложения по режиму охраны помещений, в которых установлены СКЗИ или хранятся ключевые документы к ним;

- вести Журнал поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов (далее - Журнал);

- выдавать пользователям СКЗИ экземпляры СКЗИ, эксплуатационной и технической документации к ним, ключевых документов под расписку в соответствующем Журнале;

- контролировать передачу СКЗИ, эксплуатационной и технической документации к ним, ключевых документов между пользователями СКЗИ и (или) ответственным пользователем СКЗИ под расписку в соответствующем Журнале;

- пломбировать (опечатывать) и контролировать сохранность печатей (пломб) на аппаратных средствах, с которыми осуществляется штатное функционирование СКЗИ, а также аппаратных и аппаратно-программных СКЗИ;

- контролировать получение и доставку СКЗИ, эксплуатационной и технической документации к ним;

- заблаговременно делать заказы на изготовление очередных ключевых документов и рассылку на места использования для своевременной замены действующих ключевых документов;

- контролировать уничтожение неиспользованных или выведенных из действия ключевых документов в сроки, указанные в эксплуатационной и технической документации к соответствующим СКЗИ, или, если срок уничтожения эксплуатационной и технической документацией не установлен, не позднее 10 суток после вывода их из действия (окончания срока действия) под расписку в соответствующем Журнале;

- выводить из действия носители ключевой информации (далее - НКИ), в отношении которых возникло подозрение в компрометации, а также действующие совместно с ними другие НКИ;

- принимать решение в чрезвычайных случаях, когда отсутствуют НКИ для замены скомпрометированных, об использовании скомпрометированных НКИ;

- проводить инструктаж пользователей СКЗИ по правилам работы с СКЗИ и ключевыми документами.

2.3. Требовать прекращения обработки персональных данных в случае нарушения установленного порядка работ с СКЗИ или нарушения функционирования СКЗИ.

2.4. Участвовать в анализе ситуаций, касающихся нарушения условий хранения носителей персональных данных, использования СКЗИ, которые могут привести к нарушению конфиденциальности персональных данных или другим нарушениям, приводящим к снижению уровня защищенности персональных данных.

2.5. Контролировать исполнение пользователями СКЗИ требований нормативных актов в части обеспечения защиты персональных данных с помощью СКЗИ.

2.6. Принимать все необходимые меры для обеспечения безопасности персональных данных, в случае получения от пользователей СКЗИ информации о фактах утраты, компрометации ключевой информации, в частности, обеспечить выполнение следующих мероприятий:

- в каждом случае, по факту (или предполагаемой) компрометации ключевых документов, проводится служебное расследование; результатом расследования является квалификация или не квалификация данного события как компрометация;

- о факте компрометации ключевой информации пользователями СКЗИ совместно с ответственным пользователем СКЗИ производится информирование всех заинтересованных участников информационного обмена;

- выведенные из действия скомпрометированные ключевые документы после проведения расследования уничтожаются, о чем делается соответствующая запись в Журнале;

- для своевременного восстановления связи пользователю СКЗИ выдается новый НКИ; для этого создается резервный запас НКИ, использование которых осуществляется в случаях крайней необходимости по решению ответственного пользователя СКЗИ.

2.7. Подготавливать копии НКИ, которые подлежат основному учету и хранятся в сейфе ответственного пользователя СКЗИ. Данные копии применяются с разрешения

ответственного за обработку персональных данных, если по результатам расследования не было установлено факта компрометации.

2.8. Хранить резервные НКИ отдельно от рабочих (актуальных) НКИ, с целью обеспечения невозможности их одновременной компрометации.

2.9. Своевременно информировать ответственного за обработку персональных данных о фактах утраты или недостачи СКЗИ, ключевых документов к ним, ключей от помещений, хранилищ, личных печатей и о других фактах, которые могут привести к разглашению защищаемых персональных данных.

3. Права ответственного пользователя СКЗИ

Ответственный пользователь СКЗИ имеет право:

3.1. Знакомиться с Нормативными актами, регламентирующими процессы обработки персональных данных.

3.2. Требовать от пользователей СКЗИ соблюдения требований Нормативных актов в части обеспечения защиты информации с помощью СКЗИ.

3.3. Требовать прекращения работы в ИСПДн, как в целом, так и отдельных пользователей СКЗИ, в случае выявления нарушений требований по работе с СКЗИ, предназначенными для обеспечения безопасности персональных данных, или в связи с нарушением функционирования СКЗИ.

ПРИЛОЖЕНИЕ 20
к приказу муниципального бюджетного дошкольного образовательного учреждения «Подвязьевский детский сад» муниципального образования – Рязанский муниципальный район Рязанской области от «27» июля 2020 г. № 68/1-р

Инструкция пользователя средств криптографической защиты информации в муниципальном бюджетном дошкольном образовательном учреждении «Подвязьевский детский сад» муниципального образования – Рязанский муниципальный район Рязанской области

1. Общие положения

1.1. Настоящая Инструкция пользователя средств криптографической защиты информации (далее - Инструкция) в муниципальном бюджетном дошкольном образовательном учреждении «Подвязьевский детский сад» муниципального образования – Рязанский муниципальный район Рязанской области (далее - ДОУ) определяет права и обязанности пользователя средств криптографической защиты информации, порядок обращения с криптографическими средствами защиты информации (далее - СКЗИ), а также определяет порядок восстановления связи в случае компрометации действующих ключей к СКЗИ.

1.2. Пользователем СКЗИ является сотрудник ДОУ, включенный в перечень сотрудников, допущенных к работе с СКЗИ, предназначенными для обеспечения безопасности персональных данных в информационных системах персональных данных, утвержденный заведующим ДОУ.

1.3. Пользователь СКЗИ должен знать нормативные акты Российской Федерации и Рязанской области, методические материалы в сфере обработки персональных данных, в том числе распорядительные документы ДОУ в сфере обработки персональных данных (далее - Нормативные акты).

1.4. В своей деятельности, связанной с обработкой персональных данных, пользователь СКЗИ руководствуется настоящей Инструкцией.

1.5. Пользователи СКЗИ несут персональную ответственность за обеспечение конфиденциальности ключевой информации и защиту СКЗИ от несанкционированного использования.

2. Обязанности и права пользователя СКЗИ

2.1. Пользователь СКЗИ обязан:

- соблюдать требования по обеспечению безопасности функционирования СКЗИ;
- обеспечить конфиденциальность всей информации ограниченного распространения, доступной по роду выполняемых функциональных обязанностей;
- сдать ответственному пользователю СКЗИ ДОУ (далее - Ответственный) носители ключевой информации (далее - НКИ) при увольнении или отстранении от исполнения обязанностей, связанных с использованием СКЗИ;
- сдать Ответственному НКИ по окончании срока действия сертификата ключа, а также в случае компрометации ключа;
- немедленно уведомлять руководителя структурного подразделения или Ответственного о компрометации НКИ, о фактах утраты или недостачи СКЗИ;

- в пределах своей компетенции предоставлять информацию комиссии, проводящей служебные расследования по фактам компрометации, а также выявлению причин нарушения требований безопасности функционирования СКЗИ.

2.2. Пользователю СКЗИ запрещается:

- осуществлять несанкционированное и безучетное копирование ключевых данных;
- хранить НКИ вне сейфов и помещений, гарантирующих их сохранность и конфиденциальность;
- передавать НКИ каким бы то ни было лицам, кроме Ответственного;
- во время работы оставлять НКИ без присмотра (например, на рабочем столе или в разъеме системного блока ПЭВМ);
- хранить на НКИ какую-либо информацию, кроме ключевой;
- использовать в помещениях, где применяются СКЗИ, личные технические средства, позволяющие осуществлять копирование ключевой информации;
- использовать НКИ, выведенные из действия.

2.3. Пользователь имеет право:

- вносить предложения по вопросам использования СКЗИ;
- повышать уровень квалификации по использованию СКЗИ.

3. Порядок обращения с СКЗИ

3.1. Монтаж и установка СКЗИ осуществляются органом криптографической защиты, назначенным заведующим ДОУ.

3.2. Служебные помещения, в которых размещаются СКЗИ, должны отвечать всем требованиям по оборудованию и охране, предъявляемым к помещениям, выделенным для работы с конфиденциальной информацией. Для хранения НКИ помещения обеспечиваются сейфами (металлическими шкафами и по убытии сотрудников закрываются и опечатываются личными печатями ответственных лиц.

3.3. Пользователи СКЗИ хранят инсталлирующие СКЗИ носители, эксплуатационную и техническую документацию к СКЗИ, ключевые документы в шкафах (ящиках, хранилищах) индивидуального пользования в условиях, исключающих бесконтрольный доступ к ним, а также их непреднамеренное уничтожение.

3.4. К эксплуатации СКЗИ допускаются лица, прошедшие инструктаж и изучившие правила пользования данным СКЗИ.

3.5. Все программное обеспечение ПЭВМ, предназначенной для установки СКЗИ, должно иметь соответствующие лицензии. Установка средств разработки и отладки программ на рабочую станцию, использующую СКЗИ, не допускается.

4. Восстановление связи в случае компрометации действующих ключей к СКЗИ

4.1. Под компрометацией криптографического ключа понимается утрата доверия к тому, что данный ключ обеспечивает однозначную идентификацию владельца НКИ и конфиденциальность информации, обрабатываемой с его помощью. К событиям, связанным с компрометацией действующих криптографических ключей, относятся:

- утрата (хищение) НКИ, в том числе - с последующим их обнаружением;
- увольнение (переназначение) сотрудников, имевших доступ к НКИ;
- передача секретных ключей по линии связи в открытом виде;
- нарушение правил хранения НКИ;
- вскрытие фактов утечки передаваемой информации или ее искажения (подмены, подделки);
- ошибки при совершении криптографических операций;
- несанкционированное или безучетное копирование ключевой информации;

- все случаи, когда нельзя достоверно установить, что произошло с НКИ (в том числе случаи, когда НКИ вышел из строя и доказательно не опровергнута вероятность того, что данный факт произошел в результате злоумышленных действий).

4.2. При наступлении любого из перечисленных выше событий пользователь СКЗИ или владелец НКИ должен немедленно прекратить связь с другими абонентами и сообщить о факте компрометации (или предполагаемом факте компрометации) Ответственному лично, по телефону, электронной почте или другим доступным способом. В любом случае пользователь СКЗИ или владелец НКИ обязан убедиться, что его сообщение получено и прочтено.

4.3. При подтверждении факта компрометации действующих ключей пользователь СКЗИ обязан обеспечить немедленное изъятие из обращения скомпрометированных криптографических ключей и сдачу Ответственному в течение 3 рабочих дней.

4.4. Для восстановления конфиденциальной связи после компрометации действующих ключей пользователь СКЗИ получает у Ответственного новые ключи.

ПРИЛОЖЕНИЕ 21
к приказу муниципального бюджетного дошкольного образовательного учреждения «Подвязьевский детский сад» муниципального образования – Рязанский муниципальный район Рязанской области от «27» июля 2020 г. № 68/1-р

муниципальное бюджетное дошкольное образовательное учреждение «Подвязьевский детский сад» муниципального образования – Рязанский муниципальный район Рязанской области

Журнал поэкземплярного учета средств защиты информации

Учетный № _____20_____ год.

Листов (_____)

№ п/п	Наименование СЗИ	Серийные номера СЗИ	Номера экземпляров	Отметка о получении	Владелец сертификата, срок действия	Отметка о выдаче	Отметка о подключении (установке) СКЗИ	Отметка об изъятии СЗИ	Примечание
				От кого получены \ Дата и номер сопроводительного письма		Ф.И.О. пользователя СКЗИ \ Дата и расписка в получении	Ф.И.О.\ Дата подключения \ Номера аппаратных средств, в которые установлены или к которым подключены СКЗИ	Дата изъятия (уничто-жения) \ Ф.И.О. \ Номер акта или расписка об уничтожении	
1	2	3	4	5	6	7	8	9	10

ПРИЛОЖЕНИЕ 22
к приказу муниципального бюджетного дошкольного образовательного учреждения «Подвязьевский детский сад» муниципального образования – Рязанский муниципальный район Рязанской области от «27» июля 2020 г. № 68/1-р

РУКОВОДСТВО

администратора информационной системы муниципального бюджетного дошкольного образовательного учреждения «Подвязьевский детский сад» муниципального образования – Рязанский муниципальный район Рязанской области

1. ОБЩИЕ ПОЛОЖЕНИЯ

Настоящее руководство определяет права и обязанности администратора информационной системы (далее – администратор ИС), ответственного за эксплуатацию информационной системы (далее – ИС).

1.1. Администратор ИС назначается распоряжением муниципального бюджетного дошкольного образовательного учреждения «Подвязьевский детский сад» муниципального образования – Рязанский муниципальный район Рязанской области (далее – ДОУ) и подчиняется непосредственно заведующему ДОУ.

1.2. Администратор ИС отвечает за обеспечение возможности эксплуатации ИС.

1.3. Требования администратора ИС, связанные с выполнением им своих обязанностей, обязательны для исполнения всеми пользователями ИС.

1.4. Администратор ИС несет персональную ответственность за качество проводимых им работ по администрированию ИС, состояние и поддержание уровня защищенности информации, содержащейся в ИС.

2. ЗАДАЧИ АДМИНИСТРАТОРА ИС

2.1. Основными задачами администратора ИС являются:

– обеспечение возможности эксплуатации ИС;

– администрирование ИС.

2.2. В рамках выполнения основных задач администратор ИС осуществляет:

– создание учётных записей пользователей ИС;

– контроль за событиями безопасности и действиями администратора безопасности и пользователей ИС;

– контроль выполнения пользователями ИС мероприятий по обеспечению безопасности информации ИС;

– методическую помощь пользователям ИС.

3. ОБЯЗАННОСТИ АДМИНИСТРАТОРА ИС

3.1. Администратор ИС обязан:

– знать и выполнять требования нормативных документов по защите информации, регламентирующих порядок защиты информации, обрабатываемой в ИС, в том числе содержащих персональные данные (далее – ПДн);

– осуществлять общее руководство деятельности по обработке информации в ИС, в том числе содержащих ПДн;

– участвовать в разработке организационно-распорядительной документации по вопросам обеспечения безопасности информации, содержащейся в ИС;

– анализировать состояние работоспособности и защищённости ИС;

– контролировать правильность функционирования прикладного программного обеспечения ИС и неизменность его настроек;

– контролировать исполнение пользователями ИС введенного режима безопасности, а также правильность работы с элементами ИС;

– периодически анализировать журналы учета событий безопасности, регистрируемых прикладным программным обеспечением ИС, с целью контроля действий пользователей и выявления возможных нарушений;

– контролировать выполнение администратором безопасности и пользователями ИС своих обязанностей;

– периодически представлять заведующему ДОУ отчет о состоянии ИС и о нештатных ситуациях и допущенных пользователями и администратором безопасности нарушениях установленных требований по защите информации;

– в случае выявления нарушений режима безопасности информации (в том числе ПДн), а также возникновения внештатных и аварийных ситуаций, принимать необходимые меры с целью ликвидации их последствий и определению причин их появления;

– принимать участие в проведении работ по оценке ИС требованиям безопасности информации.

4. ПРАВА АДМИНИСТРАТОРА ИС

4.1. Администратор ИС имеет право:

– давать пользователям ИС обязательные для исполнения указания и рекомендации по вопросам безопасной эксплуатации прикладного программного обеспечения ИС;

– проводить служебные расследования по фактам нарушений установленных требований обеспечения информационной безопасности (далее – ИБ), несанкционированного доступа (далее – НСД), утраты, порчи защищаемой информации и технических средств ИС;

– организовывать и участвовать в любых проверках по использованию пользователями ИС;

– запрещать устанавливать на автоматизированных рабочих местах нештатное программное и аппаратное обеспечение;

– запрашивать и получать от заведующего ДОУ материалы, необходимые для организации своей работы;

– вносить на рассмотрение заведующему ДОУ предложения по улучшению состояния ИБ, по замене вышедших из строя элементов системы защиты информации ИС, а также по выведению из эксплуатации машинных носителей персональных данных, у которых закончился период эксплуатации, установленный их производителем.

5. ОТВЕТСТВЕННОСТЬ АДМИНИСТРАТОРА ИС

5.1. Администратор ИС несет ответственность:

– за организацию безопасной эксплуатации ИС;

– за выполнение установленных условий функционирования ИС;

– за качество выполнения обязанностей, установленных настоящей Инструкцией;

– за качество проводимых работ по контролю действий администратора безопасности и пользователей ИС, состояние и поддержание необходимого уровня защиты информационных и технических ИС;

– за качество и состояние организационно-распорядительной и эксплуатационной документации по вопросам эксплуатации ИС;

– за разглашение сведений ограниченного доступа (ПДн, иная защищаемая

информация), ставших известными ему по роду работы.

ОЗНАКОМЛЕНЫ:

(должность)	*(дата, подпись)*	*(расшифровка подписи)*
(должность)	*(дата, подпись)*	*(расшифровка подписи)*
(должность)	*(дата, подпись)*	*(расшифровка подписи)*
(должность)	*(дата, подпись)*	*(расшифровка подписи)*
(должность)	*(дата, подпись)*	*(расшифровка подписи)*
(должность)	*(дата, подпись)*	*(расшифровка подписи)*
(должность)	*(дата, подпись)*	*(расшифровка подписи)*

ПРИЛОЖЕНИЕ 23
к приказу муниципального бюджетного дошкольного образовательного учреждения «Подвязьевский детский сад» муниципального образования – Рязанский муниципальный район Рязанской области от «27» июля 2020 г. № 68/1-р

РУКОВОДСТВО

пользователя информационной системы муниципального бюджетного дошкольного образовательного учреждения «Подвязьевский детский сад» муниципального образования – Рязанский муниципальный район Рязанской области

1. ОБЩИЕ ПОЛОЖЕНИЯ

Настоящее руководство определяет права и обязанности Пользователя информационной системы муниципального бюджетного дошкольного образовательного учреждения «Подвязьевский детский сад» муниципального образования – Рязанский муниципальный район Рязанской области (далее – пользователь ИС), ответственного за эксплуатацию информационной системы муниципального бюджетного дошкольного образовательного учреждения «Подвязьевский детский сад» муниципального образования – Рязанский муниципальный район Рязанской области (далее - ИС).

1.1. Пользователи ИС (в том числе внешние пользователи) назначаются муниципальным бюджетным дошкольным образовательным учреждением «Подвязьевский детский сад» муниципального образования – Рязанский муниципальный район Рязанской области (далее – ДОУ).

2. ОБЯЗАННОСТИ ПОЛЬЗОВАТЕЛЯ ИС

2.1. Пользователи ИС обязаны знать и выполнять требования законодательства РФ, законодательства Рязанской области, распоряжений и постановлений Правительства Рязанской области, нормативных актов ДОУ, устанавливающих правила обработки и защиты информации в ИС, в том числе содержащих персональные данные (далее – ПДн).

2.2. При эксплуатации ИС с целью защиты информации, в том числе ПДн, пользователь ИС обязан:

– руководствоваться требованиями организационно – распорядительной документации по организации обработки и защиты информации в ИС;

– соблюдать установленную технологию обработки и защиты информации;

– использовать для записи информации ИС только съемные носители информации, учтенные в установленном порядке;

– использовать для вывода на печать документов, содержащих информацию, находящуюся в ИС, только устройства печати, расположенные в пределах установленных контролируемых зон, сводя к минимуму возможность доступа к ним посторонних лиц.

2.3. Пользователь должен свести к минимуму возможность неконтролируемого доступа к средствам вычислительной техники (далее – СВТ) ИС посторонних лиц, а также возможность просмотра посторонними лицами ведущихся на СВТ работ. В случаях кратковременного отсутствия (перерыв, обед) при выходе в течение рабочего дня из помещения, в котором размещаются СВТ ИС, пользователь обязан блокировать ввод-вывод информации на своем рабочем месте или выключить СВТ. Защищаемые носители

информации должны быть убраны в запираемые хранилища, определенные в установленном порядке для этих целей.

2.4. Пользователь обязан докладывать администратору безопасности ИС и своему непосредственному руководителю (для сотрудников ДОУ):

– о фактах имевшегося или предполагаемого несанкционированного доступа к информации, носителям информации, СВТ ИС, помещениям, в которых располагаются СВТ ИС, и хранилищам;

– об утрате носителей информации, паролей и идентификаторов, ключей от помещений, где ведется обработка информации ИС и хранилищ;

– об обнаружении вредоносного программного обеспечения или нетипичного поведения ИС;

– о попытках получения информации лицами, не имеющими к ней допуска;

– об иных внештатных ситуациях, связанных с угрозой безопасности ИС;

2.5. Пользователю запрещается:

– подключать к СВТ ИС нештатные устройства;

– самостоятельно вносить изменения в состав, конфигурацию и размещение СВТ ИС;

– самостоятельно вносить изменения в состав, конфигурацию и настройку программного обеспечения, установленного в ИС;

– самостоятельно вносить изменения в размещение, состав и настройку средств защиты информации (далее – СЗИ) ИС;

– сообщать устно, письменно или иным способом (показ и т.п.) другим лицам идентификаторы и пароли, передавать ключи от хранилищ и помещений и другие реквизиты доступа к ИС;

– разрешать работу с СВТ ИС лицам, не допущенным в установленном порядке к обработке информации в ИС.

3. ПРАВА ПОЛЬЗОВАТЕЛЯ ИС

3.1. Пользователь ИС имеет право:

– обращаться к администратору безопасности, администратору ИС и ответственному за организацию обработки ПДн по любым вопросам, касающихся обработки и защиты информации в ИС (выполнение режимных мер, установленной технологии обработки информации, инструкций и других документов по обеспечению безопасности информации ИС);

– обращаться к администратору безопасности с просьбой об оказании консультаций и технической помощи по обеспечению безопасности обрабатываемой в ИС информации, а также по вопросам эксплуатации установленных средств защиты информации (СЗИ);

– обращаться к администратору ИС и администратору безопасности с просьбой об оказании консультаций и технической помощи по использованию установленных программных и технических средств ИС.

4. ОТВЕТСТВЕННОСТЬ ПОЛЬЗОВАТЕЛЯ ИС

4.1. Пользователь ИС несет ответственность:

– за соблюдение установленной технологии обработки информации в ИС, в том числе ПДн*;

– за соблюдение режима конфиденциальности информации;

– за правильность понимания и полноту выполнения задач, функций, прав и обязанностей, возложенных на него при работе в ИС;

– за соблюдение требований локальных актов по вопросам обработки и защиты информации в ИС, в том числе ПДн.

4.2. Пользователи ИС, несут ответственность за ненадлежащее исполнение или неисполнение своих обязанностей, предусмотренных настоящим Руководством, в пределах, определенных действующим законодательством Российской Федерации.

ОЗНАКОМЛЕНЫ:

(должность)	*(дата, подпись)*	*(расшифровка подписи)*
(должность)	*(дата, подпись)*	*(расшифровка подписи)*
(должность)	*(дата, подпись)*	*(расшифровка подписи)*
(должность)	*(дата, подпись)*	*(расшифровка подписи)*
(должность)	*(дата, подпись)*	*(расшифровка подписи)*
(должность)	*(дата, подпись)*	*(расшифровка подписи)*
(должность)	*(дата, подпись)*	*(расшифровка подписи)*
(должность)	*(дата, подпись)*	*(расшифровка подписи)*