МИНИСТЕРСТВО ОБРАЗОВАНИЯ И МОЛОДЕЖНОЙ ПОЛИТИКИ РЯЗАНСКОЙ ОБЛАСТИ

П Р И К А З

от «16» ноября 2018 г. г. Рязань № 1467

О защите персональных данных министерства образования и молодежной политики Рязанской области

В целях обеспечения безопасности персональных данных министерства образования и молодежной политики Рязанской области, в соответствии с Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных», Федеральным законом от 27 июля 2004 г. № 79-ФЗ «О государственной гражданской службе Российской Федерации», Федеральным законом от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Трудовым кодексом Российской Федерации, руководствуясь Положением о министерстве образования и молодежной политики Рязанской области, утвержденным постановлением Правительства Рязанской области от 11 июня 2008 г. № 99,

ПРИКАЗЫВАЮ:

1. Утвердить Положение о политике информационной безопасности в информационных системах персональных данных министерства образования и молодежной политики Рязанской области согласно приложению № 1.
2. Утвердить Положение об обработке персональных данных в информационных системах персональных данных министерства образования и молодежной политики Рязанской области согласно приложению № 2.
3. Утвердить Положение об обработке персональных данных работников министерства образования и молодежной политики Рязанской области согласно приложению № 3.
5. Утвердить форму обязательства о неразглашении персональных данных согласно приложению № 4.
6. Утвердить форму согласия на обработку персональных данных согласно приложению № 5.
7. Утвердить форму согласия лиц, не являющихся работниками министерства образования и молодежной политики Рязанской области, на обработку персональных данных согласно приложению № 6.
8. Ответственному за организацию обработки персональных данных в министерстве образования и молодежной политики Рязанской области С.В. Круцику ознакомить работников министерства образования и молодежной политики Рязанской области с настоящим приказом.
9. Признать утратившими силу приказы министерства образования Рязанской области:

от 17 декабря 2012 г. № 2419 «О защите персональных данных министерства образования Рязанской области»;

от 03 сентября 2015 г. № 8421;
от 12 августа 2014 г. № 757;
от 20 марта 2017 г. № 298.

10. Контроль за исполнением настоящего приказа возложить на заместителя министра образования и молодежной политики Рязанской области П.О. Симакова.

И.о. министра О.С. Васина

Приложение № 1
к приказу министерства образования
и молодежной политики
Рязанской области
от «16» ноября 2018 г. № 1467

ПОЛОЖЕНИЕ
о политике информационной безопасности в информационных системах персональных данных министерства образования и молодежной политики Рязанской области

1 Общие положения

1.1 Настоящее Положение о политике информационной безопасности в информационных системах персональных данных министерства образования и молодежной политики Рязанской области (далее – Положение) определяет основные цели и задачи, а также общую стратегию построения системы защиты персональных данных министерства образования и молодежной политики Рязанской области (далее – Министерство). Политика информационной безопасности в информационных системах персональных данных Министерства (далее – Политика) определяет основные требования и базовые подходы к их реализации, для достижения требуемого уровня безопасности информации.

Политика разработана в соответствии с системным подходом к обеспечению информационной безопасности. Системный подход предполагает проведение комплекса мероприятий, включающих исследование угроз информационной безопасности и разработку системы защиты персональных данных, с позиции комплексного применения технических и организационных мер и средств защиты.

Под информационной безопасностью персональных данных понимается защищенность персональных данных в обрабатывающей их инфраструктуре от любых случайных или злонамеренных воздействий, результатом которых может явиться нанесение ущерба самой информации, ее владельцам (субъектам персональных данных) или инфраструктуре. Задачи информационной безопасности сводятся к минимизации ущерба от возможной реализации угроз безопасности персональных данных, а также к прогнозированию и предотвращению таких воздействий.

Политика служит основой для разработки комплекса организационных и технических мер по обеспечению информационной безопасности Министерства, а также нормативных и методических документов, обеспечивающих ее реализацию, и не предполагает подмены функций государственных органов власти Российской Федерации, отвечающих за обеспечение безопасности информационных технологий и защиту информации. Политика является методологической основой для:

- принятия управленческих решений и разработки практических мер по воплощению политики безопасности персональных данных и выработки комплекса согласованных мер нормативно-правового, технологического и организационно-технического характера, направленных на выявление, отражение и ликвидацию последствий реализации различных видов угроз персональных данных;
- координации деятельности структурных подразделений Министерства при проведении работ по развитию и эксплуатации информационной системы персональных данных с соблюдением требований обеспечения безопасности персональных данных;
- разработки предложений по совершенствованию правового, нормативного, методического, технического и организационного обеспечения безопасности персональных данных Министерства.

Политика разработана на основании:

- Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (далее – Федеральный закон № 152-ФЗ);
- постановления Правительства РФ от 01 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- приказ Федеральной службы безопасности Российской Федерации от 10 июля 2014 г. № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности».

В Политике определены требования к персоналу, работающему в информационных системах персональных данных Министерства, степень ответственности персонала, структура и необходимый уровень защищенности, статус и должностные обязанности работников, ответственных за обеспечение безопасности персональных данных в информационных системах персональных данных.

1.2 Целью настоящей Политики является обеспечение безопасности персональных данных Министерства от всех видов угроз, внешних и внутренних, умышленных и непреднамеренных, минимизация ущерба от возможной реализации угроз безопасности персональных данных.

1.3 Безопасность персональных данных достигается путем исключения несанкционированного, в том числе случайного доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий.

1.4 Персональные данные и связанные с ними ресурсы должны быть доступны для авторизованных пользователей. Должно осуществляться своевременное обнаружение и реагирование на угрозы безопасности персональных данных.

1.5 Основные понятия, обозначения и сокращения, используемые в настоящем Положении.

1.5.1 Основные понятия:

Аутентификация отправителя данных – подтверждение того, что отправитель полученных данных соответствует заявленному.

Безопасность персональных данных – состояние защищенности персональных данных, характеризуемое способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность персональных данных при их обработке в информационных системах персональных данных.

Блокирование персональных данных – временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных).

Вирус (компьютерный, программный) – исполняемый программный код или интерпретируемый набор инструкций, обладающий свойствами несанкционированного распространения и самовоспроизведения. Созданные дубликаты компьютерного вируса не всегда совпадают с оригиналом, но сохраняют способность к дальнейшему распространению и самовоспроизведению.

Вредоносная программа – программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на персональные данные или ресурсы информационной системы персональных данных.

Защищаемая информация – информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

Идентификация – присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

Информативный сигнал – электрические сигналы, акустические, электромагнитные и другие физические поля, по параметрам которых может быть раскрыта конфиденциальная информация (персональные данные) обрабатываемая в информационной системе персональных данных.

Информационная система персональных данных – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

Информационные технологии – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

Источник угрозы безопасности информации – субъект доступа, материальный объект или физическое явление, являющиеся причиной возникновения угрозы безопасности информации.

Конфиденциальность персональных данных – обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространение без согласия субъекта персональных данных или наличия иного законного основания.

Межсетевой экран – локальное (однокомпонентное) или функционально-распределенное программное (программно-аппаратное) средство (комплекс), реализующее контроль за информацией, поступающей в информационную систему персональных данных и (или) выходящей из информационной системы.

Нарушитель безопасности пер- сональных данных – физическое лицо, случайно или преднамеренно совершающее действия, следствием которых является нарушение безопасности персональных данных при их обработке техническими средствами в информационных системах персональных данных.

Несанкционированный доступ (несанкционированные действия) – доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых информационными системами персональных данных.

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

Обезличивание персональных данных – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.

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

Оператор (персональных данных) – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующее и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

Перехват (информации) – неправомерное получение информации с использованием технического средства, осуществляющего обнаружение, прием и обработку информативных сигналов.

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

Правила разграничения доступа – совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.

Программная закладка – код программы, преднамеренно внесенный в программу с целью осуществить утечку, изменить, блокировать, уничтожить информацию или уничтожить и модифицировать программное обеспечение информационной системы персональных данных и (или) блокировать аппаратные средства.

Программное (программно-математическое) воздействие – несанкционированное воздействие на ресурсы автоматизированной информационной системы, осуществляемое с использованием вредоносных программ.

Распространение персональных данных – действия, направленные на раскрытие персональных данных неопределённому кругу лиц.

Средства вычислительной техники – совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

Субъект доступа (субъект) – лицо или процесс, действия которого регламентируются правилами разграничения доступа.

Технические средства информационной системы персональных данных – 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 (операционные системы, системы управления базами данных и т.п.), средства защиты информации).

Трансграничная передача персональных данных – передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

Угрозы безопасности персональных данных – совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий при их обработке в информационной системе персональных данных.

Уничтожение персональных данных – действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных.

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

Целостность информации – способность средства вычислительной техники или автоматизированной системы обеспечивать неизменность информации в условиях случайного и/или преднамеренного искажения (разрушения).

1.5.2 Обозначения и сокращения:

ВП	– вредоносная программа
ЗИР	– защищаемый информационный ресурс
ИС	– информационная система
ИСПДн	– информационная система персональных данных
МЭ	– межсетевой экран

НСД	– несанкционированный доступ
ОС	– операционная система
ПДн	– персональные данные
ПМВ	– программно-математические воздействия
ПО	– программное обеспечение
СЗИ	– средство защиты информации
СЗПДн	– система защиты персональных данных
СКЗИ	– средство криптографической защиты информации
БД	– база данных
ТКУИ	– технические каналы утечки информации
ТС	– технические средства
УБПДн	– угрозы безопасности персональных данных
ЭВМ	– электронно-вычислительная машина

2 Область действия

2.1 Требования настоящей Политики распространяются на всех работников Министерства (штатных, временных, работающих по контракту и т.п.), а также всех прочих лиц (подрядчики, аудиторы и т.п.).

3 Система защиты персональных данных

3.1 Система защиты персональных данных (СЗПДн), строится на основании:

- Отчёта по результатам обследования системы защиты персональных данных Министерства (далее – Отчёт по результатам обследования);
- Перечня персональных данных, подлежащих защите;
- Акта классификации информационной системы персональных данных Министерства (далее – Акт классификации);
- Модели угроз безопасности персональных данных при их обработке в информационных системах персональных данных Министерства (далее – Модель угроз);
- Частного технического задания на разработку системы защиты персональных данных Министерства;
- Проекта системы защиты персональных данных информационных систем персональных данных Министерства;
- Руководящих документов ФСТЭК и ФСБ России.

3.2 На основании этих документов определяется необходимый уровень защищенности ПДн ИСПДн Министерства. На основании анализа актуальных

угроз безопасности ПДн описанного в Отчете по результатам обследования и Модели угроз, делается заключение о необходимости использования технических средств и организационных мероприятий для обеспечения безопасности ПДн.

Под актуальными угрозами безопасности персональных данных понимается совокупность условий и факторов, создающих актуальную опасность несанкционированного, в том числе случайного, доступа к персональным данным при их обработке в информационной системе, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия.

Угрозы 1-го типа актуальны для информационной системы, если для нее в том числе актуальны угрозы, связанные с наличием недокументированных (недекларированных) возможностей в системном программном обеспечении, используемом в информационной системе.

Угрозы 2-го типа актуальны для информационной системы, если для нее в том числе актуальны угрозы, связанные с наличием недокументированных (недекларированных) возможностей в прикладном программном обеспечении, используемом в информационной системе.

Угрозы 3-го типа актуальны для информационной системы, если для нее актуальны угрозы, не связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении, используемом в информационной системе.

При обработке персональных данных в информационных системах устанавливаются 4 уровня защищенности персональных данных.

Необходимость обеспечения 1-го уровня защищенности персональных данных при их обработке в информационной системе устанавливается при наличии хотя бы одного из следующих условий:

а) для информационной системы актуальны угрозы 1-го типа и информационная система обрабатывает либо специальные категории персональных данных, либо биометрические персональные данные, либо иные категории персональных данных;

б) для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает специальные категории персональных данных более чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора.

Необходимость обеспечения 2-го уровня защищенности персональных данных при их обработке в информационной системе устанавливается при наличии хотя бы одного из следующих условий:

а) для информационной системы актуальны угрозы 1-го типа и информационная система обрабатывает общедоступные персональные данные;

б) для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает специальные категории персональных данных сотрудников оператора или специальные категории персональных данных менее чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора;

в) для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает биометрические персональные данные;

г) для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает общедоступные персональные данные более чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора;

д) для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает иные категории персональных данных более чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора;

е) для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает специальные категории персональных данных более чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора.

Необходимость обеспечения 3-го уровня защищенности персональных данных при их обработке в информационной системе устанавливается при наличии хотя бы одного из следующих условий:

а) для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает общедоступные персональные данные сотрудников оператора или общедоступные персональные данные менее чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора;

б) для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает иные категории персональных данных сотрудников оператора или иные категории персональных данных менее чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора;

в) для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает специальные категории персональных данных сотрудников оператора или специальные категории персональных данных менее чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора;

г) для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает биометрические персональные данные;

д) для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает иные категории персональных данных более чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора.

Необходимость обеспечения 4-го уровня защищенности персональных данных при их обработке в информационной системе устанавливается при наличии хотя бы одного из следующих условий:

а) для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает общедоступные персональные данные;

б) для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает иные категории персональных данных сотрудников оператора или иные категории персональных данных менее чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора.

Для обеспечения 4-го уровня защищенности персональных данных при их обработке в информационных системах необходимо выполнение следующих требований:

а) организация режима обеспече- ния безопасности помещений, в которых размещена информационная система, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения;

б) обеспечение сохранности носителей персональных данных;

в) утверждение руководителем оператора документа, определяющего перечень лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей;

г) использование средств защиты информации, прошедших процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации, в случае, когда применение таких средств необходимо для нейтрализации актуальных угроз.

Для обеспечения 3-го уровня защищенности персональных данных при их обработке в информационных системах помимо выполнения требований, предусмотренных пунктом 13 настоящего документа, необходимо, чтобы было назначено должностное лицо (работник), ответственный за обеспечение безопасности персональных данных в информационной системе.

Для обеспечения 2-го уровня защищенности персональных данных при их обработке в информационных системах помимо выполнения требований, предусмотренных пунктом 14 настоящего документа, необходимо, чтобы доступ к содержанию электронного журнала сообщений был возможен исключительно для должностных лиц (работников) оператора или уполномоченного лица, которым сведения, содержащиеся в указанном журнале, необходимы для выполнения служебных (трудовых) обязанностей.

Для обеспечения 1-го уровня защищенности персональных данных при их обработке в информационных системах помимо требований, предусмотренных для обеспечения 2-го уровня защищенности персональных данных, необходимо выполнение следующих требований:

а) автоматическая регистрация в электронном журнале безопасности изменения полномочий сотрудника оператора по доступу к персональным данным, содержащимся в информационной системе;

б) создание структурного подразделения, ответственного за обеспечение безопасности персональных данных в информационной системе, либо возложение на одно из структурных подразделений функций по обеспечению такой безопасности.

3.3 В зависимости от уровня защищенности ИСПДн и актуальных угроз, СЗПДн может включать следующие технические средства:

а) СЗИ от НСД:

– средства управления логическим доступом;

– средства регистрации и учета (самостоятельные или встроенные в другие СЗИ, обеспечивающие фиксацию важных с точки зрения обеспечения безопасности информации событий, происходящих в ИС);

– средства обеспечения целостности (самостоятельные или встроенные в другие СЗИ, обеспечивающие контроль целостности информационных ресурсов и программного обеспечения (далее – ПО);

– средства межсетевого взаимодействия;

– средства защиты от программно-математических воздействий (средства защиты от вредоносного ПО);

– средства защиты каналов связи;

– средства криптографической защиты информации (СКЗИ);

– средства инструментального анализа защищенности;

– средства обнаружения вторжений;

б) средства защиты от утечки конфиденциальной информации по техническим каналам:

– средства защиты от утечки видовой информации.

3.4 В список должны быть включены функции защиты, обеспечиваемые штатными средствами обработки ПДн, операционными системами (ОС), прикладным ПО и специальными комплексами, реализующими средства защиты.

4 Основные принципы построения системы комплексной защиты информации

4.1 Построение системы обеспечения безопасности ПДн ИСПДн Министерства и ее функционирование должны осуществляться в соответствии со следующими основными принципами:

– законность;
– системность;
– комплексность;
– непрерывность;
– своевременность;
– преемственность и непрерывность совершенствования;
– персональная ответственность;
– минимизация полномочий;
– взаимодействие и сотрудничество;
– гибкость системы защиты;
– простота применения средств защиты;
– научная обоснованность и техническая реализуемость;
– специализация и профессионализм;
– обязательность контроля.

4.1.1 Законность.

4.1.1.1 Данный принцип предполагает осуществление защитных мероприятий и разработку СЗПДн Министерства в соответствии с действующим законодательством в области защиты ПДн и других нормативных актов по безопасности информации, утвержденных органами государственной власти и управления в пределах их компетенции. Работники и обслуживающий персонал ПДн ИСПДн Министерства должны быть осведомлены о порядке работы с защищаемой информацией и об ответственности за защиту ПДн.

4.1.2 Системность.

4.1.2.1 Системный подход к построению СЗПДн Министерства предполагает учет всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, существенно значимых для понимания и решения проблемы обеспечения безопасности ПДн ИСПДн Министерства. При создании системы защиты должны учитываться все слабые и наиболее уязвимые места системы обработки ПДн, а также характер, возможные объекты и направления атак на систему со стороны нарушителей (особенно высококвалифицированных злоумышленников), пути проникновения в распределенные системы и НСД к информации. Система защиты должна строиться с учетом не только всех известных каналов проникновения и НСД к информации, но и с учетом возможности появления принципиально новых путей реализации угроз безопасности.

4.1.3 Комплексность.

4.1.3.1 Комплексное использование методов и средств защиты предполагает согласованное применение разнородных средств при построении целостной системы защиты, перекрывающей все существенные (значимые) каналы реализации угроз и не содержащей слабых мест на стыках отдельных ее компонентов. Защита должна строиться эшелонировано. Для каждого канала утечки информации и для каждой угрозы безопасности должно существовать несколько защитных рубежей. Создание защитных рубежей осуществляется с учетом того, чтобы для их преодоления потенциальному злоумышленнику требовались профессиональные навыки в нескольких невзаимосвязанных областях.

4.1.4 Непрерывность защиты ПДн.

4.1.4.1 Защита ПДн – не разовое мероприятие и не простая совокупность проведенных мероприятий и установленных средств защиты, а непрерывный целенаправленный процесс, предполагающий принятие соответствующих мер на всех этапах жизненного цикла ИСПДн. ИСПДн должны находиться в защищенном состоянии на протяжении всего времени их функционирования. В соответствии с этим принципом должны приниматься меры по недопущению перехода ИСПДн в незащищенное состояние. Большинству физических и технических средств защиты для эффективного выполнения своих функций необходима постоянная техническая и организационная (административная) поддержка (своевременная смена и обеспечение правильного хранения и применения имен, паролей, ключей шифрования, переопределение полномочий и т.п.). Перерывы в работе средств защиты могут быть использованы злоумышленниками для анализа применяемых методов и средств защиты, для внедрения специальных программных и аппаратных «закладок» и других средств преодоления системы защиты после восстановления ее функционирования.

4.1.5 Своевременность.

4.1.5.1 Данный принцип предполагает упреждающий характер мер обеспечения безопасности ПДн, то есть постановку задач по комплексной защите ИСПДн и реализацию мер обеспечения безопасности ПДн на ранних стадиях разработки ИСПДн в целом, и ее системы защиты информации, в частности. Разработка системы защиты должна вестись параллельно с разработкой и развитием самой защищаемой системы. Это позволит учесть требования безопасности при

проектировании архитектуры и, в ко- нечном счете, создать более эффективные (как по затратам ресурсов, так и по стойкости) защищенные системы.

4.1.6 Преемственность и совершенствование.

4.1.6.1 Предполагают постоянное совершенствование мер и средств защиты информации на основе преемственности организационных и технических решений, кадрового состава, анализа функционирования ИСПДн и ее системы защиты с учетом изменений в методах и средствах перехвата информации, нормативных требований по защите, достигнутого отечественного и зарубежного опыта в этой области.

4.1.7 Персональная ответственность.

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

4.1.8 Принцип минимизации полномочий.

4.1.8.1 Означает предоставление пользователям минимальных прав доступа в соответствии с производственной необходимостью, на основе принципа «все, что не разрешено, запрещено». Доступ к ПДн должен предоставляться только в том случае и объеме, если это необходимо работнику для выполнения его должностных обязанностей.

4.1.9 Взаимодействие и сотрудничество.

4.1.9.1 Предполагает создание благоприятной атмосферы в коллективах подразделений, обеспечивающих деятельность ИСПДн Министерства, для снижения вероятности возникновения негативных действий связанных с человеческим фактором. В такой обстановке работники должны осознанно соблюдать установленные правила и оказывать содействие в деятельности ответственного за организацию обработки персональных данных, администратора ИСПДн, администратора информационной безопасности ИСПДн (далее - Администратор ИБ ИСПДн).

4.1.10 Гибкость системы защиты ПДн.

4.1.10.1 Принятые меры и установленные средства защиты, особенно в начальный период их эксплуатации, могут обеспечивать как чрезмерный, так и недостаточный уровень защиты. Для обеспечения возможности варьирования уровнем защищенности, средства защиты должны обладать определенной гибкостью. Особенно важным это свойство является в тех случаях, когда установку средств защиты необходимо осуществлять на работающую систему, не нарушая процесса ее нормального функционирования.

4.1.11 Простота применения средств защиты.

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

ролей и имен и т.д.). Должна достигать- ся автоматизация максимального числа действий пользователей и администраторов ИСПДн.

4.1.12 Научная обоснованность и техническая реализуемость.

4.1.12.1 Информационные технологии, технические и программные средства, средства и меры защиты информации должны быть реализованы на современном уровне развития науки и техники, научно обоснованы с точки зрения достижения заданного уровня безопасности информации и должны соответствовать установленным нормам и требованиям по безопасности ПДн. СЗПДн должна быть ориентирована на решения, возможные риски для которых и меры противодействия этим рискам прошли всестороннюю теоретическую и практическую проверку.

4.1.13 Специализация и профессионализм.

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

4.1.14 Обязательность контроля.

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

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

5 Требования к подсистемам СЗПДн

5.1 СЗПДн включает в себя следующие подсистемы:

- управления доступом,
- регистрации и учёта;
- обеспечения целостности;
- защиты от программно-математических воздействий;
- защиты каналов связи;
- межсетевого экранирования;
- обнаружения вторжений;
- криптографической защиты;
- инструментального анализа защищенности.

5.2 СЗПДн имеют различный функционал в зависимости от класса ИСПДн, определенного в Акте классификации.

5.2.1 Подсистема управления доступом.

5.2.1.1 Подсистема управления доступом предназначена для реализации следующих функций:

– Идентификация и проверка подлинности субъектов доступа при входе в систему по паролю условно-постоянного действия длинной не менее шести буквенно-цифровых символов.

5.2.1.2 Подсистема управления доступом может быть реализована с помощью штатных средств обработки ПДн (операционных систем, приложений и СУБД). Так же может быть внедрено специальное техническое средство или их комплекс, осуществляющие дополнительные меры по аутентификации и контролю. Например, применение единых хранилищ учетных записей пользователей и регистрационной информации, использование биометрических и технических (с помощью электронных пропусков) мер аутентификации и других.

5.2.2 Подсистема регистрации и учёта.

5.2.2.1 Подсистема регистрации и учёта предназначена для реализации следующих функций:

– Регистрация входа (выхода) субъектов доступа в систему (из системы), либо регистрация загрузки и инициализации операционной системы и ее программного останова. Регистрация выхода из системы или останова не проводится в моменты аппаратурного отключения ИСПДн. В параметрах регистрации указываются дата и время входа (выхода) или загрузки (останова) системы, результат попытки входа (успешная или неуспешная), идентификатор (код или фамилия) субъекта, предъявленный при попытке доступа, код или пароль, предъявленный при неуспешной попытке.

– Учет всех защищаемых носителей информации с помощью их маркировки и занесением учетных данных в Журнал учета с отметкой об их выдаче (приеме).

5.2.3 Подсистема обеспечения целостности.

5.2.3.1 Подсистема целостности предназначена для реализации следующих функций:

– Обеспечение целостности программных средств системы защиты персональных данных, обрабатываемой информации, а также неизменность программной среды. При этом целостность системы защиты персональных данных проверяется при загрузке системы по контрольным суммам компонентов системы защиты, а целостность программной среды обеспечивается использованием трансляторов с языков высокого уровня и отсутствием средств модификации объектного кода программ в процессе обработки и (или) хранения персональных данных.

– Физическая охрана технических средств информационной системы (устройств и носителей информации), предусматривающая контроль доступа в помещения посторонних лиц, наличие надежных препятствий для несанкционированного проникновения в помещения и хранилище носителей информации.

– Периодическое тестирование функций системы защиты персональных данных при изменении программной среды и пользователей информационной системы с помощью тест – программ, имитирующих попытки несанкционированного доступа.

– Наличие средств восстановления системы защиты персональных данных, предусматривающие ведение двух копий программных компонентов средств

защиты информации, их периодическое обновление и контроль работоспособности.

5.2.4 Подсистема защиты от программно-математических воздействий.

5.2.4.1 Подсистема защиты от программно-математических воздействий (подсистема антивирусной защиты) предназначена для реализации следующих функций:

– Автоматическая проверка на наличие вредоносных программ (далее – ВП) или последствий программно-математических воздействий (далее – ПМВ) при импорте в ИСПДн всех программных модулей (прикладных программ), которые могут содержать ВП, по их типовым шаблонам и с помощью эвристического анализа.

– Реализация механизмов автоматического блокирования обнаруженных ВП путем их удаления из программных модулей или уничтожения.

– Проверка на предмет наличия ВП в средствах защиты от ПМВ (при первом запуске средства защиты от ПМВ и с устанавливаемой периодичностью).

– Факт выявления ПМВ должен инициировать автоматическую проверку на предмет наличия ВП.

– Реализация механизма отката для устанавливаемого числа операций удаления ВП из оперативной или постоянной памяти, из программных модулей и прикладных программ или программных средств, содержащих ВП.

– На всех технических средствах ИСПДн должен проводиться непрерывный согласованный по единому сценарию автоматический мониторинг информационного обмена в ИСПДн с целью выявления проявлений ПМВ.

– Проверка целостности модулей средства защиты от ПМВ, необходимых для его корректного функционирования, при его загрузке с использованием контрольных сумм.

– Реализация механизмов проверки целостности пакетов обновлений средства защиты от ПМВ с использованием контрольных сумм.

– Восстановление средств защиты от ПМВ, предусматривающая ведение двух копий программных средств защиты, его периодическое обновление и контроль работоспособности.

5.2.5 Подсистема защиты каналов связи.

5.2.5.1 Подсистема защиты каналов связи предназначена для реализации следующих функций:

– Обмен персональными данными, при их обработке в информационных системах, по каналам связи, защита которых обеспечивается путем реализации соответствующих организационных мер и (или) применения технических средств.

– Выделение канала связи, обеспечивающего защиту передаваемой информации.

– Аутентификация взаимодействующих информационных систем и проверка подлинности пользователей и целостности передаваемых данных.

– Предотвращение возможности отрицания пользователем факта отправки персональных данных другому пользователю.

– Предотвращение возможности отрицания пользователем факта получения персональных данных от другого пользователя.

5.2.6 Подсистема межсетевого экранирования.

5.2.6.1 Подсистема межсетевого экранирования предназначена для реализации следующих функций:

- Фильтрация на сетевом уровне для каждого сетевого пакета независимо (решение о фильтрации принимается на основе сетевых адресов отправителя и получателя или на основе других эквивалентных атрибутов).
- Фильтрация пакетов служебных протоколов, служащих для диагностики и управления работой сетевых устройств.
- Идентификация и аутентификация администратора межсетевого экрана при его локальных запросах на доступ по идентификатору (коду) и паролю условно – постоянного действия.
- Регистрация входа (выхода) администратора межсетевого экрана в систему (из системы) либо загрузки и инициализации системы и ее программного останова (регистрация входа из системы не проводится в моменты аппаратурного отключения межсетевого экрана).
- Контроль целостности своей программной и информационной части.
- Восстановление свойств межсетевого экрана после сбоев и отказов оборудования.
- Регламентное тестирование реализации правил фильтрации, процесса идентификации и аутентификации администратора межсетевого экрана, процесса регистрации действий администратора межсетевого экрана, процесса контроля за целостностью программной и информационной части, процедуры восстановления.

5.2.6.2 Подсистема реализуется внедрением программно-аппаратных комплексов межсетевого экранирования на границе ЛСВ, классом не ниже 4.

5.2.7 Подсистема обнаружения вторжений.

5.2.7.1 Подсистема обнаружения вторжений предназначена для реализации следующих функций:

- Обнаружение вторжений должно обеспечиваться путем использования в составе ИСПДн программных или программно-аппаратных средств (систем) обнаружения вторжений, использующие сигнатурные методы анализа, а также методы выявления аномалий.
- Подсистема обнаружения вторжений проводится для информационных систем, подключённых к сетям международного информационного обмена, путём использования в составе информационной системы программных или программно-аппаратных средств (систем) обнаружения вторжений.

5.2.8 Подсистема инструментального анализа защищенности.

5.2.8.1 Подсистема инструментального анализа защищённости предназначена для реализации следующих функций:

- Анализ защищенности проводится путем использования в составе ИСПДн программных или программно-аппаратных средств анализа защищенности.
- Для ИСПДн средствами анализа защищенности должна быть обеспечена возможность выявления уязвимостей, связанных с ошибками в конфигурации ПО ИСПДн, которые могут быть использованы нарушителем для реализации атаки на систему.

5.2.9 Подсистема криптографи- ческой защиты.

5.2.9.1 Подсистема криптографической защиты предназначена для реализации следующих функций:

– Приняты меры по исключению несанкционированного доступа в помещения, в которых размещены технические средства с установленным СКЗИ, посторонних лиц, по роду своей деятельности не являющихся персоналом, допущенным к работе в этих помещениях. В случае необходимости присутствия посторонних лиц в указанных помещениях обеспечен контроль за их действиями и обеспечена невозможность негативных действий с их стороны на СКЗИ, технические средства, на которых эксплуатируется СКЗИ и защищаемую информацию.
Обеспечена невозможность доступа к ключевым носителям лиц, не назначенных для работы с конкретным ключевым носителем.

– Ключи на ключевых носителях, срок действия которых истек, уничтожаются путем переформатирования ключевых носителей средствами ПО СКЗИ, после чего ключевые носители могут использоваться для записи на них новой ключевой информации. Об уничтожении ключей делается соответствующая запись в Журнале.

6 Пользователи ИСПДн

6.1 В ИСПДн Министерства можно выделить следующие группы пользователей, участвующих в обработке и хранении ПДн:

– Администратора ИСПДн;
– Администратора ИБ ИСПДн;
– Ответственного за организацию обработки ПДн;
– Операторов (пользователей) обработки ИСПДн.

6.1.1 Администратор ИСПДн.

6.1.1.1 Администратор ИСПДн, работник Министерства, ответственный за настройку, внедрение и сопровождение ИСПДн, обеспечивает функционирование подсистемы управления доступом ИСПДн и уполномочен осуществлять предоставление и разграничение доступа конечного пользователя (Оператора АРМ) к элементам, хранящим персональные данные.

6.1.1.2 Администратор ИСПДн обладает следующим уровнем доступа и знаний:

обладает полной информацией о системном и прикладном программном обеспечении ИСПДн;

обладает полной информацией о технических средствах и конфигурации ИСПДн;

имеет доступ ко всем техническим средствам обработки информации и данным ИСПДн;

обладает правами конфигурирования и административной настройки технических средств ИСПДн.

6.1.2 Администратор ИБ ИСПДн.

6.1.2.1 Администратор ИБ ИСПДн, работник Министерства, ответственный за функционирование СЗПДн, включая обслуживание и настройку административной, серверной и клиентской компонент.

6.1.2.2 Администратор ИБ ИСПДн обладает следующим уровнем доступа и знаний:

- обладает правами Администратора ИСПДн;
- обладает полной информацией об ИСПДн;
- имеет доступ к средствам защиты информации и протоколирования и к части ключевых элементов ИСПДн;
- не имеет прав доступа к конфигурированию технических средств сети за исключением контрольных (инспекционных).

6.1.2.3 Администратор ИБ ИСПДн уполномочен:

- реализовывать политики безопасности в части настройки СКЗИ, межсетевых экранов и систем обнаружения атак, в соответствии с которыми пользователь (Оператор АРМ) получает возможность работать с элементами ИСПДн;
- осуществлять аудит средств защиты;
- устанавливать доверительные отношения своей защищенной сети с сетями других Учреждений.

6.1.3 Операторы (пользователи) обработки ИСПДн.

6.1.3.1 Оператор обработки ИСПДн, работник Министерства, осуществляющий обработку ПДн. Обработка ПДн включает: возможность просмотра ПДн, ручной ввод ПДн в систему ИСПДн, формирование справок и отчетов по информации, полученной из ИСПД. Оператор не имеет полномочий для управления подсистемами обработки данных и СЗПДн.

6.1.3.2 Оператор ИСПДн обладает следующим уровнем доступа и знаний:

- обладает всеми необходимыми атрибутами (например, паролем), обеспечивающими доступ к некоторому подмножеству ПДн;
- располагает конфиденциальными данными, к которым имеет доступ.

7 Требования к персоналу по обеспечению защиты ПДн

7.1 Все работники Министерства, являющиеся пользователями ИСПДн, должны четко знать и строго выполнять установленные правила и обязанности по доступу к персональным данным и соблюдению режима безопасности ПДн.

7.2 При вступлении в должность нового работника ответственный за организацию обработки ПДн обязан организовать его ознакомление с должностной инструкцией и необходимыми документами, регламентирующими требования по защите ПДн, а также обучение навыкам выполнения процедур, необходимых для санкционированного использования ИСПДн.

7.3 Работник должен быть ознакомлен со сведениями настоящей Политики, принятых процедур работы с элементами ИСПДн и СЗПДн.

7.4 Работники Министерства, использующие технические средства аутентификации, должны обеспечивать сохранность идентификаторов (электронных ключей) и не допускать несанкционированного доступа к ним, а так же возможность их утери или использования третьими лицами. Пользователи несут персональную ответственность за сохранность идентификаторов.

7.5 Работники Министерства должны следовать установленным процедурам поддержания режима безопасности ПДн при выборе и использовании паролей (если не используются технические средства аутентификации).

7.6 Работники Министерства должны обеспечивать надлежащую защиту оборудования, оставляемого без присмотра, особенно в тех случаях, когда в помещение имеют доступ посторонние лица. Все пользователи должны знать требования по безопасности ПДн и процедуры защиты оборудования, оставленного без присмотра, а также свои обязанности по обеспечению такой защиты.

7.7 Работникам запрещается устанавливать постороннее программное обеспечение, подключать личные мобильные устройства и носители информации, а так же записывать на них защищаемую информацию.

7.8 Работникам запрещается разглашать защищаемую информацию, которая стала им известна при работе с информационной системой Министерства, третьим лицам.

7.9 При работе с ПДн в ИСПДн работники Министерства обязаны обеспечить отсутствие возможности просмотра ПДн третьими лицами с мониторов АРМ или терминалов.

7.10 При завершении работы с ИСПДн работники обязаны защитить АРМ или терминалы с помощью блокировки ключом или эквивалентного средства контроля, например, доступом по паролю, если не используются более сильные средства защиты.

7.11 Работники Министерства должны быть проинформированы об угрозах нарушения режима безопасности ПДн и ответственности за его нарушение. Они должны быть ознакомлены с утвержденной формальной процедурой наложения дисциплинарных взысканий на работников, которые нарушили принятые политику и процедуры безопасности ПДн.

7.12 Работники обязаны без промедления сообщать обо всех наблюдаемых или подозрительных случаях работы ИСПДн, могущих повлечь за собой угрозы безопасности ПДн, а также о выявленных ими событиях, затрагивающих безопасность ПДн, руководству подразделения и лицу, отвечающему за немедленное реагирование на угрозы безопасности ПДн.

8 Должностные обязанности пользователей ИСПДн

8.1 Должностные обязанности пользователей ИСПДн описаны в следующих документах:

- Инструкция администратора ИСПДн;
- Инструкция администратора ИБ ИСПДн;
- Инструкция пользователя ИСПДн;

9 Ответственность пользователей ИСПДн

9.1 В соответствии со статьей 24 Федерального закона № 152-ФЗ лица, виновные в нарушении требований данного Федерального закона, несут предусмотренную законодательством Российской Федерации ответственность. Моральный вред, причиненный субъекту персональных данных вследствие наруше-

ния его прав, нарушения правил обра- ботки персональных данных, установленных Федеральным законом № 152-ФЗ, а также требований к защите персональных данных, установленных в соответствии с настоящим Федеральным законом, подлежат возмещению в соответствии с законодательством Российской Федерации. Возмещение морального вреда осуществляется независимо от возмещения имущественного вреда и понесенных субъектом персональных данных убытков.

9.2 Действующее законодательство РФ позволяет предъявлять требования по обеспечению безопасной работы с защищаемой информацией и предусматривает ответственность за нарушение установленных правил эксплуатации ЭВМ и систем, неправомерный доступ к информации, если эти действия привели к уничтожению, блокированию, модификации информации или нарушению работы ЭВМ или сетей (статьи 272, 273 и 274 УК РФ).

9.3 Администратор ИСПДн и администратор ИБ ИСПДн несут ответственность за все действия, совершенные от имени их учетных записей или системных учетных записей, если не доказан факт несанкционированного использования учетных записей.

9.4 При нарушениях работниками Министерства – пользователей ИСПДн правил, связанных с безопасностью ПДн, они несут ответственность, установленную действующим законодательством Российской Федерации.

Приложение № 2
к приказу министерства образования
и молодежной политики
Рязанской области
от «16» ноября 2018 г. № 1467

ПОЛОЖЕНИЕ
об обработке персональных данных в информационных системах персональных данных министерства образования и молодежной политики Рязанской области

1 Общие положения

1.1 Настоящее Положение об обработке персональных данных (далее – Положение) определяет порядок получения, хранения, обработки, комбинирования, передачи и любого другого использования персональных данных, обрабатываемых в информационных системах персональных данных министерства образования и молодежной политики Рязанской области (далее – Министерство, Оператор или Работодатель) в соответствии с законодательством Российской Федерации.

1.2 Настоящее Положение разработано в соответствии с:

– Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;

– Федеральным законом от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

1.3 Для целей настоящего Положения используются следующие основные понятия:

– персональные данные (ПДн) – любая информация, относящаяся к прямо или косвенно к определённому или определяемому физическому лицу (субъекту персональных данных);

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

– распространение персональных данных - действия, направленные на передачу персональных данных определенному кругу лиц (передача персональных данных) или на ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных данных в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к персональным данным каким-либо иным способом;

– использование персональных данных – действия с персональными данными, совершаемые работниками Министерства 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;

– автоматизированная обработка – обработка данных, выполняемая средствами

вычислительной техники;

– блокирование персональных данных – временное прекращение сбора, систематизации, накопления, использования, распространения персональных данных, в том числе их передачи;

– уничтожение персональных данных – действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных;

– обезличивание персональных данных – действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных;

– информационная система персональных данных – система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств;

– защита персональных данных – деятельность уполномоченных лиц по обеспечению с помощью локального регулирования порядка обработки персональных данных и организационно-технических мер конфиденциальности информации о конкретном субъекте персональных данных.

1.4 Персональные данные, обрабатываемые в информационных системах персональных данных Министерства (далее – ИСПДн), относятся к конфиденциальной информации, порядок работы с которыми регламентирован Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных» и осуществляется с соблюдением строго определенных правил и условий.

2 Получение, обработка и защита персональных данных

2.1 Порядок получения персональных данных.

2.1.1 Все персональные данные следует получать лично у субъекта ПДн. Если персональные данные возможно получить только у третьей стороны, то субъект ПДн должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие. Министерство должно сообщить субъекту ПДн о целях, предполагаемых источниках и способах получения персональных данных, характере подлежащих получению персональных данных и последствиях отказа субъекта ПДн дать письменное согласие на их получение.

2.1.2 Министерство вправе обрабатывать персональные данные субъектов ПДн только с их письменного разрешения.

2.1.3 Письменное согласие субъекта ПДн на обработку своих персональных данных должно включать в себя персональные данные, указанные в перечне ПДн, подлежащих защите в ИСПДн.

2.1.4 Министерство не имеет права получать и обрабатывать персональные данные субъекта ПДн о его политических, религиозных и иных убеждениях, частной жизни, членстве в общественных объединениях или его профсоюзной деятельности.

2.1.5 Работники Министерства имеют право получать только те ПДн, которые необходимы им для выполнения своих служебных обязанностей.

2.1.6 Работники Министерства, получающие персональные данные субъекта ПДн, обязаны соблюдать режим конфиденциальности.

2.2 Порядок обработки персональных данных.

2.2.1 Обработка персональных данных может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия работникам в трудоустройстве, обучении и продвижении по службе, обеспечения личной безопасности работников, контроля количества и качества выполняемой работы и обеспечения

сохранности имущества Работодателя, работников и третьих лиц.

2.2.2 При определении объема и содержания, обрабатываемых персональных данных, Министерство должно руководствоваться Конституцией Российской Федерации, Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных» и иными федеральными законами в области защиты персональных данных.

2.2.3 При принятии решений, затрагивающих интересы субъекта ПДн, Министерство не имеет права основываться на персональных данных субъекта ПДн, полученных исключительно в результате их автоматизированной обработки или электронно.

2.2.4 Съемные электронные носители, на которые копируется база данных ИСПДн, для переноса ее в ноутбуки выездных бригад, должны быть промаркированы и учтены в Журнале регистрации, учета и выдачи сменных носителей ПДн.

2.3 Порядок защиты персональных данных.

2.3.1 Защита персональных данных субъекта ПДн от неправомерного их использования или утраты должна быть обеспечена Министерством за счет его средств в порядке, установленном федеральными законами Российской Федерации в области защиты персональных данных.

2.3.2 Министерство обязано при обработке персональных данных субъектов персональных данных принимать необходимые организационные и технические меры для защиты персональных данных от несанкционированного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных, а также от иных неправомерных действий.

2.3.3 Соблюдать порядок получения, учета и хранения персональных данных субъектов ПДн.

2.3.4 Применять технические средства охраны и сигнализации.

2.3.5 Взять со всех работников, связанных с получением, обработкой и защитой персональных данных субъектов ПДн, Обязательство о неразглашении персональных данных.

2.3.6 Привлекать к дисциплинарной ответственности работников, виновных в нарушении норм, регулирующих получение, обработку и защиту персональных данных субъекта ПДн.

2.3.7 Запретить допуск к персональным данным субъектов ПДн работников Министерства, не включенных в Перечень лиц, допущенных к обработке персональных данных, обрабатываемых в ИСПДн.

2.3.8 Защита доступа к электронной базе данных, содержащей персональные данные субъектов ПДн, должна обеспечиваться путем использования сертифицированных программных и программно-аппаратных средств защиты информации, предотвращающих несанкционированный доступ третьих лиц к персональным данным субъектов ПДн.

2.3.9 Копировать и делать выписки персональных данных субъектов ПДн разрешается исключительно в служебных целях.

2.3.10 Субъекты ПДн не должны отказываться от прав на сохранение и защиту своих персональных данных.

2.3.11 Министерство, субъекты ПДн и их представители должны совместно вырабатывать меры защиты персональных данных субъектов ПДн.

3 Хранение персональных данных

3.1 Сведения о субъектах ПДн в Министерстве на бумажных носителях должных храниться в специально оборудованных шкафах и сейфах, которые запираются и опечатываются. Ключи от шкафов и сейфов, в которых хранятся сведения о субъектах ПДн, находятся у ответственного должностного лица.

3.2 Обязанности по хранению сведений о субъектах ПДн, заполнению, хранению и выдаче документов, содержащих персональные данные, в ИСПДн возлагаются на ответственного за организацию обработки персональных данных.

3.3 Съемные электронные носители, на которых хранятся резервные копии персональных данных субъектов ПДн, должны быть промаркированы и учтены в журнале регистрации, учета и выдачи внешних носителей для хранения резервных копий ПДн.

3.4 В процессе хранения персональных данных субъектов ПДн необходимо обеспечивать контроль за достоверностью и полнотой персональных данных, их регулярное обновление и внесение по мере необходимости соответствующих изменений.

4 Передача персональных данных

4.1 При передаче персональных данных работника Министерство должно соблюдать следующие требования:

4.1.1 Не сообщать персональные данные работника третьей стороне без письменного согласия работника, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровья работника, а также в случаях, установленных Трудовым кодексом Российской Федерации или другими федеральными законами.

4.1.1.1 Учитывая, что Трудовой кодекс Российской Федерации не определяет критерии ситуаций, представляющих угрозу жизни и здоровью работника, Министерство в каждом конкретном случае делает самостоятельную оценку серьезности, неминуемости, степени такой угрозы.

4.1.1.2 Если же лицо, обратившееся с запросом, не уполномочено федеральным законом на получение персональных данных работника, либо отсутствует письменное согласие работника на предоставление его персональных данных, либо, по мнению Работодателя, отсутствует угроза жизни и здоровью работника, Работодатель обязан отказать в предоставлении персональных данных, лицу, обратившемуся с запросом, выдается письменное уведомление об отказе в предоставлении персональных данных.

4.1.1.3 Письменное согласие работника на передачу Работодателем своих персональных данных третьей стороне должно включать в себя:

- фамилию, имя, отчество, адрес субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;
- наименование (фамилию, имя, отчество) и адрес Оператора, получающего согласие субъекта персональных данных;
- цель обработки персональных данных;
- перечень персональных данных, на обработку которых дается согласие субъекта персональных данных;
- перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых Оператором способов обработки персональных данных;
- срок, в течение которого действует согласие, а также порядок его отзыва.

4.1.2 Не сообщать персональные данные работника в коммерческих целях без его письменного согласия.

4.1.3 Предупреждать лиц, получающих персональные данные работника, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждения того, что это правило соблюдено.

4.1.4 Осуществлять передачу данных работника в пределах Организации в соответствии с настоящим Положением.

4.1.5 Разрешать доступ к персональным данным работника только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те персональные данные работника, которые необходимы для выполнения конкретных функций.

4.1.6 Не запрашивать информацию о состоянии здоровья работника, за исключением тех сведений, которые относятся к вопросу о возможности выполнения работником трудовой функции, (например, допустимо обращение за информацией о состоянии здоровья беременной

женщины при решении вопроса ее перевода на другую работу).

4.1.7 Передавать персональные данные работника представителю работника в порядке, установленном Трудовым кодексом, иными федеральными законами и настоящим Положением, и ограничивать эту информацию только теми персональными данными, которые необходимы для выполнения указанными представителями их функций.

4.2 Данные требования установлены статьей 88 Трудового кодекса Российской Федерации и не подлежат изменению, исключению, так как являются обязательными для сторон трудовых отношений.

5 Уничтожение персональных данных

5.1 При необходимости уничтожения персональных данных Министерство должно руководствоваться следующими требованиями:

5.1.1 Уничтожение персональных данных в ИСПДн осуществляется комиссией по проведению мероприятий по защите персональных данных.

5.1.2 Бумажные носители персональных данных должны уничтожаться при помощи специального оборудования (измельчителя бумаги).

5.1.3 Персональные данные, представленные в электронном виде, должны уничтожаться специализированным программным обеспечением, гарантирующим предотвращение восстановления удаленных данных.

5.1.4 После окончания процедуры удаления персональных данных комиссией по проведению мероприятий по защите персональных данных должен быть составлен акт уничтожения персональных данных.

6 Внутренние проверки состояния защищенности информационной системы персональных данных

6.1 Проверка состояния защищенности ИСПДн осуществляется комиссией по проведению мероприятий по защите персональных данных.

6.2 Проверка состояния защищенности ИСПДн осуществляется с целью определения соответствия нормативных, организационных, практических и технических мероприятий, реализуемых Министерством требованиям законов и иных нормативных правовых актов Российской Федерации в области информационной безопасности и защиты персональных данных.

6.3 Проверка состояния защищенности ИСПДн включает в себя:

6.3.1 Определение характера циркулирующих персональных данных и установленных в ИСПДн режимов их обработки.

6.3.2 Определение актуальности организационно-распорядительной документации, учитывающей конкретные условия функционирования средств вычислительной техники различного уровня и назначения (рабочие станции пользователей, серверное и периферийное оборудование, технические средства защиты информации, в том числе средства криптографической защиты информации), порядок работы сотрудников организации при эксплуатации средств вычислительной техники.

6.3.3 Анализ принятых мер (программных, технических, организационных), обеспечивающих защиту средств вычислительной техники, информационной системы и баз данных от несанкционированного доступа, оценка продуктивности организационного процесса защиты информации. Достаточность технических средств обработки и защиты информации, наличие подтверждений соответствия по требованиям информационной безопасности (сертификатов соответствия).

6.3.4 Проведение анализа конфигураций активного сетевого оборудования, маршрутизаторов, коммутаторов, серверов с целью выявления уязвимых мест в системе защиты информации.

6.3.5 Проведение инструментального анализа сетевого и серверного оборудования локально-вычислительных сетей, информационных систем и баз данных с применением программно-аппаратных средств.

6.3.6 Проверка работоспособности используемых программных и программно-аппаратных средств обнаружения и предотвращения компьютерных атак.

6.3.7 Проверка наличия лицензионных средств защиты от вредоносных программ и вирусов или сертифицированных свободно распространяемых антивирусных средств защиты.

6.3.8 Проверка оснащения серверных и кроссовых помещений средствами контроля доступа и пожаротушения, обеспечения температурного режима, регламент доступа к серверным и кроссовым помещениям.

6.3.9 Проверка состояния защищенности информационных ресурсов от сбоев в системе электропитания (система резервирования и автоматического ввода резерва).

6.3.10 Проверка состояния линейно-кабельного оборудования локально-вычислительных сетей (наличие запирающих и опечатывающих устройств, оборудования распределительных шкафов).

6.4 Внутренняя проверка Комиссии по проведению мероприятий по защите персональных данных завершается подведением итогов (обобщением) результатов проверки и составлением акта о результате проверки состояния защищенности ИСПДн.

6.5 Акт должен содержать:

6.5.1 Дата, время и место составления акта.

6.5.2 Дата и место проведения проверки.

6.5.3 Сведения о результатах проверки, в том числе о выявленных нарушениях и их характере.

6.5.4 Достоверное и обоснованное изложение состояния защищенности информационной системы и ресурсов, выявленных недостатков и нарушений со ссылками на соответствующие документы и факты, выводы и предложения по их устранению с указанием конкретных сроков.

7 Обязанности субъекта персональных данных и Оператора

7.1 В целях обеспечения достоверности персональных данных субъект ПДн обязан:

7.1.1 Предоставлять Министерству полные и достоверные данные о себе.

7.1.2 В случае изменения своих персональных данных сообщать данную информацию Министерству.

7.2 Министерство обязано:

7.2.1 Осуществлять защиту персональных данных субъекта ПДн.

7.2.2 Обеспечивать хранение документации, содержащей персональные данные субъектов ПДн, при этом персональные данные не должны храниться дольше, чем это оправдано выполнением задач, для которых они собирались, или дольше, чем это требуется в интересах лиц, о которых собраны данные.

8 Права субъекта ПДн в целях защиты персональных данных

8.1 Субъект персональных данных вправе требовать от Оператора уточнения его персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

8.2 Субъект персональных данных имеет право на получение информации, касающейся обработки его персональных данных, в том числе содержащей:

- подтверждение факта обработки персональных данных Оператором;
- правовые основания и цели обработки персональных данных;

– цели и применяемые Оператором способы обработки персональных данных;

– сроки обработки персональных данных, в том числе сроки их хранения;

8.3 Субъект персональных данных имеет право на определение представителей для защиты своих персональных данных.

8.4 Субъект персональных данных имеет право требовать исключить или исправить неверные или неполные персональные данные, а также данные, обрабатываемые с нарушением требований Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

8.5 Субъект персональных данных имеет право требовать об извещении Министерством всех лиц, которым ранее были сообщены неверные или неполные персональные данные субъекта ПДн, обо всех произведенных в них исключениях, исправлениях или дополнениях.

8.6 Субъект персональных данных имеет право на обжалование в судебном порядке любых неправомерных действий или бездействии Министерства при обработке и защите его персональных данных.

9 Ответственность за нарушение норм, регулирующих получение, обработку и защиту персональных данных субъекта ПДн

9.1 Лица, виновные в нарушении требований федеральных законов, несут предусмотренную законодательством Российской Федерации ответственность.

9.2 Моральный вред, причиненный субъекту ПДн вследствие нарушения его прав, нарушения правил обработки персональных данных, установленных федеральными законами, а также нарушения требований к защите персональных данных подлежит возмещению в соответствии с законодательством Российской Федерации. Возмещение морального вреда осуществляется независимо от возмещения имущественного вреда и понесенных субъектом персональных данных убытков.

Приложение № 3
к приказу министерства образования
и молодежной политики
Рязанской области
от «16» 02 2018 г. № 1467

ПОЛОЖЕНИЕ
об обработке персональных данных работников министерства образования и молодежной политики Рязанской области

1 Общие положения

1.1 Настоящие Положение об обработке персональных данных работников (далее - Положение) определяет порядок получения, хранения, обработки, комбинирования, передачи и любого другого использования персональных данных государственных гражданских служащих, и иных работников, не являющихся государственными гражданскими служащими (далее – служащие и работники соответственно) министерства образования и молодежной политики Рязанской области (далее – Организация или Работодатель), а также ведения их личных дел в соответствии со статьей 42 Федерального закона от 27 июля 2004 г. № 79-ФЗ «О государственной гражданской службе Российской Федерации», Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных», Трудовым кодексом Российской Федерации и другими нормативными правовыми актами Российской Федерации.

1.2 Настоящее Положение разработано в соответствии с:

- Конституцией Российской Федерации;
- Трудовым кодексом Российской Федерации;
- Федеральным законом от 27 июля 2004 г. № 79-ФЗ «О государственной гражданской службе Российской Федерации»;
- Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных»
- Федеральным законом от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральным законом от 29 июля 2004 г. № 98-ФЗ «О коммерческой тайне»;
- Федеральным законом от 22 октября 2004 г. № 125-ФЗ «Об архивном деле в Российской Федерации»;
- Закон Российской Федерации от 21 июля 1993 г. № 5485-1 «О государственной тайне»;
- Перечнем сведений конфиденциального характера, утвержденным Указом Президента Российской Федерации от 06 марта 1997 г. № 188.

1.3. В настоящем Положении используются следующие основные понятия:

Персональные данные служащего, работника – любая информация, относящаяся к прямо или косвенно определённому физическому лицу (субъекту

персональных данных).

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

Распространение персональных данных служащего, работника - действия, направленные на раскрытие персональных данных неопределённому лицу.

Использование персональных данных служащего, работника - действия с персональными данными, совершаемые служащими, работниками Организации, иными уполномоченными лицами 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.

Защита персональных данных - деятельность уполномоченных лиц по обеспечению с помощью локального регулирования порядка обработки персональных данных и организационно-технических мер конфиденциальности информации о конкретном служащем, работнике, полученной Работодателем в связи с прохождением служащим государственной гражданской службы и в связи с трудовыми отношениями.

2 Получение, обработка и защита персональных данных служащего, работника

2.1 Персональные данные служащего, работника относятся к конфиденциальной информации, то есть порядок работы с ними регламентирован трудовым законодательством Российской Федерации, Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных» и осуществляется с соблюдением строго определенных правил и условий. Данные требования установлены статьей 86 Трудового кодекса Российской Федерации и не подлежат изменению, исключению, так как являются обязательными для сторон трудовых отношений.

2.2 В целях обеспечения прав и свобод человека и гражданина Работодатель и его представители при обработке персональных данных служащего, работника обязаны соблюдать следующие требования:

2.2.1 Обработка персональных данных может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия служащим, работникам в прохождении государственной гражданской службы, в трудоустройстве, обучении и продвижении по службе, обеспечения личной безопасности служащих, работников, контроля количества и качества выполняемой работы и обеспечения сохранности имущества Работодателя, служащих, работников и третьих лиц.

2.2.2 При определении объема и содержания обрабатываемых

персональных данных служащего, работника Работодатель должен руководствоваться Конституцией Российской Федерации, Трудовым кодексом Российской Федерации, Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных», Федеральным законом от 27 июля 2004 г. № 79-ФЗ «О государственной гражданской службе Российской Федерации» и иными федеральными законами.

2.2.3 Все персональные данные служащего, работника следует получать лично у служащего, работника. Если персональные данные служащего, работника возможно получить только у третьей стороны, то служащий, работник должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие. Работодатель должен сообщить служащему, работнику о целях, предполагаемых источниках и способах получения персональных данных, характере подлежащих получению персональных данных (например, оформление запроса на прежнее место работы служащего, работника в целях выяснения его профессиональных качеств, запроса в учебное заведение о подлинности документа об образовании и т.п.) и последствиях отказа служащего, работника дать письменное согласие на их получение.

2.2.4 Работодатель не имеет права получать и обрабатывать персональные данные служащего, работника о его политических, религиозных и иных убеждениях и частной жизни. В случаях, непосредственно связанных с вопросами трудовых отношений, в соответствии со статьей 24 Конституции Российской Федерации Работодатель вправе получать и обрабатывать данные о частной жизни служащего, работника только с его письменного согласия.

2.2.5 Работодатель не имеет права получать и обрабатывать персональные данные служащего, работника о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных федеральными законами.

2.2.6 При принятии решений, затрагивающих интересы служащего, работника, Работодатель не имеет права основываться на персональных данных служащего, работника, полученных исключительно в результате их автоматизированной обработки или электронно.

2.3 При поступлении на государственную гражданскую службу, на работу служащий, работник предоставляет персональные данные о себе в документированной форме, а именно:

- паспорт или иной документ, удостоверяющий личность;
- трудовую книжку, за исключением случаев, когда служебный контракт, трудовой договор заключается впервые;
- страховое свидетельство государственного пенсионного страхования;
- документы воинского учета - для военнообязанных и лиц, подлежащих призыву на военную службу;
- документ об образовании, о присвоении ученой степени, ученого звания, о квалификации или наличии специальных знаний;
- документы, необходимые для оформления допуска к государственной тайне в соответствии с требованиями Закона Российской Федерации от 21 июля 1993 г. № 5485-1 «О государственной тайне»;

- страховой медицинский полис обязательного медицинского страхования;

- служащие также предоставляют:

- сведения о доходах, имуществе и обязательствах имущественного характера служащего;

- медицинское заключение установленной формы об отсутствии у гражданина заболевания, препятствующего поступлению на гражданскую службу или ее прохождению.

2.4 Запрещается требовать от лица, поступающего на работу, документы помимо предусмотренных Трудовым кодексом Российской Федерации, иными федеральными законами, указами Президента Российской Федерации и постановлениями Правительства Российской Федерации.

2.5 При заключении служебного контракта, трудового договора и в ходе прохождения государственной гражданской службы, трудовой деятельности может возникнуть необходимость о предоставлении служащим, работником документов:

- о возрасте детей;
- о беременности женщины;
- об инвалидности;
- о донорстве;
- о составе семьи, изменении семейного положения;
- о доходе с предыдущего места работы;
- о необходимости ухода за больным членом семьи;
- прочие.

2.6 После поступления служащего на государственную гражданскую службу, приема работника на работу, а также впоследствии в процессе прохождения государственной гражданской службы, трудовой деятельности к документам, содержащим персональные данные служащего, работника, также будут относиться:

- копия акта Работодателя о назначении на должность государственной гражданской службы, о приеме на работу;

- экземпляр служебного контракта (трудового договора), а также экземпляры письменных дополнительных соглашений, которыми оформляются изменения и дополнения, внесенные в служебный контракт (трудовой договор);

- для служащих: письменное заявление с просьбой о поступлении на государственную гражданскую службу (далее – гражданская служба) и замещении должности государственной гражданской службы (далее – должность гражданской службы);

- для работников: письменное заявление о приеме на работу;

- для служащих: собственноручно заполненная и подписанная гражданином анкета установленной формы с приложением фотографии;

- для работников: автобиография;

- документы о прохождении конкурса на замещение вакантной должности гражданской службы (если гражданин назначен на должность по результатам конкурса);

- копии решений о награждении государственными наградами, присвоении почетных, воинских и специальных званий, присуждении государственных премий (если таковые имеются);

- копии актов государственного органа о переводе служащего на иную должность гражданской службы, о временном замещении им иной должности гражданской службы;

- копия акта государственного органа об освобождении служащего от замещаемой должности гражданской службы, о прекращении служебного контракта или его приостановлении;

- аттестационный лист служащего, прошедшего аттестацию, и отзыв об исполнении им должностных обязанностей за аттестационный период;

- экзаменационный лист гражданского служащего и отзыв об уровне его знаний, навыков и умений (профессиональном уровне) и о возможности присвоения ему классного чина государственной гражданской службы Рязанской области;

- копии документов о присвоении служащему классного чина государственной гражданской службы Рязанской области (иного классного чина, квалификационного разряда, дипломатического ранга);

- копии документов о включении служащего в кадровый резерв, а также об исключении его из кадрового резерва;

- копии решений о поощрении служащего, а также о наложении на него дисциплинарного взыскания до его снятия или отмены;

- копии документов о начале служебной проверки, ее результатах, об отстранении служащего от замещаемой должности гражданской службы;

- копия свидетельства о постановке на учет в налоговом органе физического лица по месту жительства на территории Российской Федерации;

- справка о результатах проверки достоверности и полноты представленных служащим сведений о доходах, имуществе и обязательствах имущественного характера, а также сведений о соблюдении служащим ограничений, установленных федеральными законами;

- карточка унифицированной формы Т-2, утвержденная постановлением Госкомстата России от 05.01.2004 г. № 1;

- другие документы.

2.7 Лица, получающие персональные данные служащего, работника, обязаны соблюдать режим конфиденциальности. Данное положение не распространяется на обмен персональными данными служащих, работников в порядке, установленном Трудовым кодексом Российской Федерации и иными федеральными законами.

2.8 Защита персональных данных служащего, работника от неправомерного их использования или утраты должна быть обеспечена Работодателем за счет его средств в порядке, установленном Трудовым кодексом Российской Федерации, Федеральным законом от 27 июля 2004 г. № 79-ФЗ «О государственной гражданской службе Российской Федерации», иными федеральными законами.

2.9 Служащие, работники, их представители должны быть ознакомлены

под роспись с документами Организации, устанавливающими порядок обработки персональных данных служащих, работников, а также осведомлены об их правах и обязанностях в этой области.

2.10 Служащие, работники не должны отказываться от прав на сохранение и защиту своих персональных данных. Если в служебном контракте, трудовом договоре будет содержаться норма об отказе служащего, работника от этого права, то в этой части служебный контракт, трудовой договор будет считаться недействительным.

2.11 Работодатель, служащие, работники и их представители должны совместно вырабатывать меры защиты персональных данных служащих, работников.

3 Хранение персональных данных служащего, работника

3.1 Персональные данные служащего, работника содержатся на бумажных носителях, в том числе в основном документе персонального учета служащих, работников - личном деле служащего, работника.

3.2 В личное дело служащего, работника вносятся его персональные данные и иные сведения, связанные с поступлением на гражданскую службу, ее прохождением и увольнением со службы (приемом на работу, работой, увольнением), и необходимые для обеспечения деятельности Работодателя.

Личное дело служащего, работника ведется в отделе правовой, кадровой и мобилизационной работы.

3.3 Персональные данные, внесенные в личные дела служащих, работников, иные сведения, содержащиеся в личных делах служащих, работников, относятся к сведениям конфиденциального характера (за исключением сведений, которые в установленных федеральными законами случаях могут быть опубликованы в средствах массовой информации), а в случаях, установленных федеральными законами и иными нормативными правовыми актами Российской Федерации, - к сведениям, составляющим государственную тайну.

3.4 К личному делу служащего приобщаются:

а) письменное заявление с просьбой о поступлении на гражданскую службу и замещении должности гражданской службы;

б) собственноручно заполненная и подписанная гражданином анкета установленной формы с приложением фотографии;

в) документы о прохождении конкурса на замещение вакантной должности гражданской службы (если гражданин назначен на должность по результатам конкурса);

г) копия паспорта и копии свидетельств о государственной регистрации актов гражданского состояния;

д) копия трудовой книжки или документа, подтверждающего прохождение военной или иной службы;

е) копии документов о профессиональном образовании, профессиональной переподготовке, повышении квалификации, стажировке, присвоении ученой

степени, ученого звания (если таковые имеются);

ж) копии решений о награждении государственными наградами Российской Федерации, Почетной грамотой Президента Российской Федерации, об объявлении благодарности Президента Российской Федерации, присвоении почетных, воинских и специальных званий, присуждении государственных премий (если таковые имеются);

з) копия акта Работодателя о назначении на должность гражданской службы;

и) экземпляр служебного контракта, а также экземпляры письменных дополнительных соглашений, которыми оформляются изменения и дополнения, внесенные в служебный контракт;

к) копии актов государственного органа о переводе служащего на иную должность гражданской службы, о временном замещении им иной должности гражданской службы;

л) копии документов воинского учета (для военнообязанных и лиц, подлежащих призыву на военную службу);

м) копия акта государственного органа об освобождении служащего от замещаемой должности гражданской службы, о прекращении служебного контракта или его приостановлении;

н) аттестационный лист служащего, прошедшего аттестацию, и отзыв об исполнении им должностных обязанностей за аттестационный период;

о) экзаменационный лист служащего и отзыв об уровне его знаний, навыков и умений (профессиональном уровне) и о возможности присвоения ему классного чина государственной гражданской службы Рязанской области;

п) копии документов о присвоении служащему классного чина государственной гражданской службы Рязанской области (иного классного чина, квалификационного разряда, дипломатического ранга);

р) копии документов о включении служащего в кадровый резерв, а также об исключении его из кадрового резерва;

с) копии решений о поощрении служащего, а также о наложении на него дисциплинарного взыскания до его снятия или отмены;

т) копии документов о начале служебной проверки, ее результатах, об отстранении служащего от замещаемой должности гражданской службы;

у) документы, связанные с оформлением допуска к сведениям, составляющим государственную или иную охраняемую законом тайну, если исполнение обязанностей по замещаемой должности гражданской службы связано с использованием таких сведений;

ф) сведения о доходах, имуществе и обязательствах имущественного характера служащего;

х) копия страхового свидетельства обязательного пенсионного страхования;

ц) копия свидетельства о постановке на учет в налоговом органе физического лица по месту жительства на территории Российской Федерации;

ч) копия страхового медицинского полиса обязательного медицинского страхования граждан;

ш) медицинское заключение установленной формы об отсутствии у

гражданина заболевания, препятствующего поступлению на гражданскую службу или ее прохождению;

щ) справка о результатах проверки достоверности и полноты представленных служащим сведений о доходах, имуществе и обязательствах имущественного характера, а также сведений о соблюдении служащим ограничений, установленных федеральными законами.

В личное дело служащего вносятся также письменные объяснения служащего, если такие объяснения даны им после ознакомления с документами своего личного дела.

К личному делу служащего приобщаются иные документы, предусмотренные федеральными законами и иными нормативными правовыми актами Российской Федерации.

Документы, приобщенные к личному делу служащего, брошюруются, страницы нумеруются, к личному делу прилагается опись.

При назначении служащего на государственную должность Российской Федерации или государственную должность субъекта Российской Федерации его личное дело передается в государственный орган по месту замещения государственной должности Российской Федерации или государственной должности субъекта Российской Федерации.

Личные дела служащих, уволенных из министерства образования и молодежной политики Рязанской области, хранятся в архиве министерства образования и молодежной политики Рязанской области в течение 50 лет со дня увольнения из министерства образования и молодежной политики Рязанской области.

Личные дела служащих, содержащие сведения, составляющие государственную тайну, хранятся отделом правовой, кадровой и мобилизационной работы в соответствии с законодательством Российской Федерации о государственной тайне.

Работодатель вправе подвергать обработке (в том числе автоматизированной) персональные данные служащих при формировании кадрового резерва.

В соответствии со статьей 15 Федерального закона от 27 мая 2003 г. № 58-ФЗ «О системе государственной службы Российской Федерации» на основе персональных данных служащих в Организации формируются и ведутся, в том числе и на электронных носителях, реестры служащих.

В обязанности отдела правовой, кадровой и мобилизационной работы Работодателя, осуществляющей ведение личных дел служащих, входит:

а) приобщение документов, указанных в настоящем пункте, к личным делам служащих;

б) обеспечение сохранности личных дел служащих;

в) обеспечение конфиденциальности сведений, содержащихся в личных делах служащих, в соответствии с от 27 июля 2004 г. № 79-ФЗ «О государственной гражданской службе Российской Федерации», другими федеральными законами, иными нормативными правовыми актами Российской Федерации, а также в соответствии с настоящим Положением;

г) ознакомление служащего с документами своего личного дела не реже одного раза в год, а также по просьбе служащего и во всех иных случаях, предусмотренных законодательством Российской Федерации.

3.5 К личному делу работника приобщаются:

а) письменное заявление о приеме на работу;

б) собственноручно заполненная и подписанная гражданином анкета установленной формы с приложением фотографии;

в) копия паспорта и копии свидетельств о государственной регистрации актов гражданского состояния;

г) копия трудовой книжки или документа, подтверждающего прохождение военной или иной службы;

д) копии документов о профессиональном образовании, профессиональной переподготовке, повышении квалификации, стажировке, присвоении ученой степени, ученого звания (если таковые имеются);

е) копии решений о награждении государственными наградами, присвоении почетных, воинских и специальных званий, присуждении государственных премий (если таковые имеются);

ж) экземпляр трудового договора, а также экземпляры письменных дополнительных соглашений, которыми оформляются изменения и дополнения, внесенные в трудовой договор;

з) копии документов воинского учета (для военнообязанных и лиц, подлежащих призыву на военную службу);

и) копия страхового свидетельства обязательного пенсионного страхования;

к) копия страхового медицинского полиса обязательного медицинского страхования граждан;

л) автобиография.

В личное дело работника включается также опись всех документов, находящихся в деле.

3.6 В случае временного изъятия документа из личного дела служащего, работника, вместо него вкладывается лист-заменитель. Изъятие документов из личного дела производится исключительно с разрешения руководителя Организации.

3.7 Сведения о служащих, работниках Организации на бумажных носителях хранятся в специально оборудованных шкафах и сейфах, которые запираются и опечатываются. Ключи от шкафов и сейфов, в которых хранятся сведения о служащих, работниках Организации, находятся у ответственных должностных лиц. Личные дела уволенных служащих, работников хранятся в специально оборудованных шкафах и сейфах.

3.8 Конкретные обязанности по хранению личных дел служащих, работников, заполнению, хранению и выдаче трудовых книжек (дубликатов трудовых книжек), иных документов, отражающих персональные данные служащих, работников, возлагаются на ответственных должностных лиц и закрепляются в должностных инструкциях.

3.9 Информация, содержащая персональные данные служащего, работника, может также обрабатываться с использованием автоматизированных

систем обработки данных. В этом случае должны выполняться требования и рекомендации нормативно-методических документов уполномоченных регулирующих органов Российской Федерации по обеспечению защиты персональных данных в информационных системах персональных данных, обрабатываемых с использованием средств автоматизации. Съемные электронные носители, на которых хранятся персональные данные служащих, работников, должны быть отмаркированы и учтены в соответствующем журнале.

3.10 Работодатель обеспечивает ограничение доступа к персональным данным служащих, работников лицам, не уполномоченным законодательством Российской Федерации либо Работодателем для получения соответствующих сведений.

3.11 Доступ к персональным данным служащих, работников без специального разрешения руководителя Организации имеют служащие, работники, указанные в Приложении № 1 к настоящему Положению.

3.12 При получении сведений, составляющих персональные данные служащего, работника, указанные лица имеют право получать только те персональные данные служащего, работника, которые необходимы для выполнения конкретных функций и заданий.

3.13 В целях информационного обеспечения могут создаваться общедоступные источники персональных данных в виде справочников. В справочники могут включаться на основании настоящего Положения следующие персональные данные: фамилия, имя, отчество, день, месяц и год рождения, номер рабочего телефона (в том числе мобильного), занимаемая должность.

3.14 Сведения о субъекте персональных данных могут быть в любое время исключены из общедоступных источников персональных данных по требованию служащего, работника.

4 Передача персональных данных служащего работника

4.1 При передаче персональных данных служащего, работника Работодатель должен соблюдать следующие требования:

4.1.1 Не сообщать персональные данные служащего, работника третьей стороне без письменного согласия служащего, работника, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровья служащего, работника, а также в случаях, установленных Трудовым кодексом Российской Федерации или другими федеральными законами.

4.1.1.1 Учитывая, что Трудовой кодекс Российской Федерации не определяет критерии ситуаций, представляющих угрозу жизни и здоровью служащего, работника, Работодатель в каждом конкретном случае делает самостоятельную оценку серьезности, неминуемости, степени такой угрозы.

4.1.1.2 Если же лицо, обратившееся с запросом, не уполномочено федеральным законом на получение персональных данных служащего, работника, либо отсутствует письменное согласие служащего, работника на предоставление его персональных данных, либо, по мнению Работодателя, отсутствует угроза жизни и здоровью служащего, работника, Работодатель обязан отказать в

предоставлении персональных данных, лицу, обратившемуся с запросом, выдается письменное уведомление об отказе в предоставлении персональных данных.

4.1.1.3 Письменное согласие служащего, работника на передачу Работодателем своих персональных данных третьей стороне должно включать в себя:

- фамилию, имя, отчество, адрес субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;
- наименование (фамилию, имя, отчество) и адрес оператора, получающего согласие субъекта персональных данных;
- цель обработки персональных данных;
- перечень персональных данных, на обработку которых дается согласие субъекта персональных данных;
- перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых оператором способов обработки персональных данных;
- срок, в течение которого действует согласие, а также порядок его отзыва.

4.1.2 Не сообщать персональные данные служащего, работника в коммерческих целях без его письменного согласия.

4.1.3 Предупреждать лиц, получающих персональные данные служащего, работника, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждения того, что это правило соблюдено.

4.1.4 Осуществлять передачу данных служащего, работника в пределах Организации в соответствии с настоящим Положением.

4.1.5 Разрешать доступ к персональным данным служащего, работника только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те персональные данные служащего, работника, которые необходимы для выполнения конкретных функций.

4.1.6 Не запрашивать информацию о состоянии здоровья служащего, работника, за исключением тех сведений, которые относятся к вопросу о возможности выполнения служащим, работником служебных обязанностей, трудовой функции, (например, допустимо обращение за информацией о состоянии здоровья беременной женщины при решении вопроса ее перевода на другую работу).

4.1.7 Передавать персональные данные служащего, работника представителю служащего, работника в порядке, установленном Трудовым кодексом, иными федеральными законами и настоящим Положением, и ограничивать эту информацию только теми персональными данными, которые необходимы для выполнения указанными представителями их функций.

4.2 Данные требования установлены статьей 88 Трудового кодекса Российской Федерации и не подлежат изменению, исключению, так как являются обязательными для сторон трудовых отношений.

5 Обязанности служащего, работника и работодателя

5.1 В целях обеспечения достоверности персональных данных служащий, работник обязан:

5.1.1 При приеме на работу предоставить Работодателю полные и достоверные данные о себе.

5.1.2 В случае изменения сведений, составляющих персональные данные служащего, работника, незамедлительно предоставить данную информацию Работодателю.

5.2 Работодатель обязан:

5.2.1 Осуществлять защиту персональных данных служащего, работника.

5.2.2 Обеспечивать хранение первичной учетной документации по учету труда и его оплаты, к которой, в частности, относятся документы по учету кадров, документы по учету использования рабочего времени и расчетов со служащими, работниками по оплате труда и др. При этом персональные данные не должны храниться дольше, чем это оправдано выполнением задач, для которых они собирались, или дольше, чем это требуется в интересах лиц, о которых собраны данные.

5.2.3 Осуществлять заполнение документации, содержащей персональные данные служащего, работника, в соответствии с требованиями действующего законодательства Российской Федерации.

5.2.4 Выдавать служащему, работнику по его письменному заявлению, не позднее трех дней со дня подачи этого заявления, копии документов, связанных с работой (копии приказа о приеме на работу, приказов о переводах на другую работу, приказа об увольнении с работы; выписки из трудовой книжки или копии трудовой книжки; справки о заработной плате, периоде работы у данного работодателя и другое). Копии документов, связанных с работой, должны быть заверены надлежащим образом и предоставляться служащему, работнику безвозмездно.

5.2.5 Вести учет передачи персональных данных служащего, работника третьим лицам путем ведения соответствующего журнала, отражающего сведения о поступившем запросе (кто является отправителем запроса, дата поступления запроса), дату ответа на запрос, когда именно информация была передана либо отметку об отказе в ее предоставлении, либо ограничиваться помещением в личное дело служащего, работника выписок, копий документов, отражающих сведения о поступившем запросе и результатах его рассмотрения.

6 Права служащего, работника

6.1 В целях обеспечения защиты персональных данных, хранящихся у Работодателя, служащие, работники имеют право:

6.1.1 На полную информацию о своих персональных данных и методах их обработки, в частности, служащий, работник имеет право знать перечень обрабатываемых персональных данных, кто и в каких целях использует или использовал его персональные данные.

6.1.2 На свободный запрос и бесплатный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей персональные данные служащего, работника, за исключением случаев, предусмотренных Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

6.1.3 На определение представителей для защиты своих персональных данных.

6.1.4 Требовать исключения или исправлении неверных или неполных персональных данных, а также данных, обработанных с нарушением требований Трудового кодекса Российской Федерации, Федеральным законом от 27 июля 2004 г. № 79-ФЗ «О государственной гражданской службе Российской Федерации» и Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных». При отказе Работодателя исключить или исправить персональные данные служащий, работник имеет право заявить в письменной форме Работодателю о своем несогласии с соответствующим обоснованием такого несогласия. Персональные данные оценочного характера служащий, работник имеет право дополнить заявлением выражающим его собственную точку зрения.

6.1.5 Требование об извещении Работодателем всех лиц, которым ранее были сообщены неверные или неполные персональные данные служащего, работника, обо всех произведенных в них исключениях, исправлениях или дополнениях.

6.1.6.Обжалование в судебном порядке любых неправомерных действий или бездействии Работодателя при обработке и защите его персональных данных.

7 Ответственность за нарушение норм, регулирующих получение, обработку и защиту персональных данных служащего, работника

7.1 Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных служащего, работника, несут предусмотренную законодательством Российской Федерации ответственность.

7.2 Неправомерный отказ Работодателя исключить или исправить персональные данные служащего, работника, а также любое иное нарушение прав служащего, работника на защиту персональных данных влечет возникновение у служащего, работника права требовать устранения нарушения его прав и компенсации причиненного таким нарушением морального вреда.

7.3 Моральный вред, причиненный субъекту ПДн вследствие нарушения его прав, нарушения правил обработки персональных данных, установленных федеральными законами, а также нарушения требований к защите персональных данных подлежит возмещению в соответствии с законодательством Российской Федерации. Возмещение морального вреда осуществляется независимо от возмещения имущественного вреда и понесенных субъектом персональных данных убытков.

Приложение № 4
к приказу министерства образования и молодежной политики
Рязанской области
от «16» ноября 2018 г. № 1467

ОБЯЗАТЕЛЬСТВО
о неразглашении персональных данных

Я, _____,
(Фамилия Имя Отчество)

работник министерства образования и молодежной политики Рязанской области предупрежден(а), что на период исполнения должностных обязанностей в соответствии с должностной инструкцией (должностным регламентом) мне будет предоставлен допуск к персональным данным. Настоящим добровольно принимаю на себя обязательства:

1 Не распространять третьим лицам персональные данные, которые мне доверены (будут доверены) или станут известными в связи с выполнением должностных обязанностей.

2 В случае попытки третьих лиц получить от меня персональные данные, сообщать непосредственному руководителю, а также лицу, ответственному за обработку персональных данных в ИСПДн министерства образования и молодежной политики Рязанской области.

3 Выполнять относящиеся ко мне требования приказов, инструкций и положений в области обработки и защиты персональных данных, с которыми я ознакомлен(а).

4 Не использовать персональные данные с целью получения выгоды.

5 Выполнять требования нормативных правовых актов, регламентирующих вопросы защиты персональных данных.

В случае увольнения с работы я обязуюсь неукоснительно соблюдать требования пунктов «1» и «2» настоящего обязательства.

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

«____» _____ 20___г. _____
(Подпись)

Приложение № 5
к приказу министерства образования и молодежной политики
Рязанской области
от «16» ноября 2018 г. № 1467

СОГЛАСИЕ
на обработку персональных данных

Я, _____
(ФИО полностью)
проживающий по адресу (регистрация) _____
_____,
паспорт _____ № _____, выдан _____
_____,
(Дата выдачи, название выдавшего органа)
в соответствии с требованиями статьи 9 Федерального закона от 27.07.2006 г. № 152 - ФЗ «О персональных данных», подтверждаю свое согласие на обработку министерством образования и молодежной политики Рязанской области (далее - Оператор) по адресу: г. Рязань, ул. Каширина, д. 1 моих персональных данных, включающих: фамилию, имя, отчество; место, год и дату рождения; регистрацию по месту жительства; адрес проживания (фактический); телефонный номер (домашний, рабочий, мобильный); паспортные данные (серия, номер паспорта, кем и когда выдан); информацию о трудовом стаже (место работы, должность, период работы, причины увольнения); информацию о заработной плате (№ заработных карт); данные о служебном контракте (трудовом договоре) (дата начала и дата окончания служебного контракта (трудового договора), вид работы, характер работы, форма оплаты, категория персонала, продолжительность рабочей недели, система оплаты); данные о повышении квалификации; данные о наградах, медалях, поощрениях, почетных званиях; информацию о номере, серии и дате выдачи трудовой книжки (вкладыша в неё) и записях в ней; ИНН; номер страхового пенсионного свидетельства; информацию о семейном положении; информацию об имущественном положении; данные о воинском учёте, необходимые сведения в целях исполнения служебного контракта (трудового договора), заключенного мной с Оператором.

Предоставляю Оператору право осуществлять все действия (операции) с моими персональными данными, включая сбор, систематизацию, накопление, хранение, обновление, изменение, использование, обезличивание, блокирование, уничтожение.

Даю согласие на передачу моих персональных данных в целях, связанных со служебной деятельностью, в Правительство Рязанской области.

Настоящее соглашение действует с момента его подписания на срок выполнения трудовых обязательств и в течение 50 (пятидесяти) лет после окончания действия трудовых обязательств согласно положениям Трудового кодекса.

Я оставляю за собой право отозвать свое согласие посредством составления соответствующего письменного документа, который может быть направлен мной в адрес Оператора по почте заказным письмом с уведомлением о вручении либо вручен лично под расписку представителю Оператора.

Я ознакомлен с юридическими последствиями моего отказа о предоставлении Оператору моих персональных данных, необходимых для исполнения служебного контракта (трудового договора).

В случае получения моего письменного заявления об отзыве настоящего согласия на обработку персональных данных, Оператор обязан прекратить обработку персональных данных и уничтожить персональные данные в срок, не превышающий тридцати рабочих дней с даты поступления указанного отзыва.

«___» _____ 20___ г. _____
(Подпись)

Приложение № 6
к приказу министерства образования и
молодежной политики
Рязанской области
от «16» ноября 2018 г. № 1467

Согласие лиц, не являющихся работниками министерства образования и молодежной политики Рязанской области, на обработку персональных данных

Я, _____
(ФИО полностью)
проживающий по адресу (регистрация) _____
_____,
паспорт _____ № _____, выдан _____
_____,
(Дата выдачи, название выдавшего органа)
в соответствии с требованиями статьи 9 Федерального закона от 27.07.2006 г. № 152 - ФЗ «О персональных данных», подтверждаю свое согласие на обработку министерством образования и молодежной политики Рязанской области (далее - Оператор) по адресу: г. Рязань, ул. Каширина, д. 1 моих персональных данных, включающих: _____
_____
_____
_____
_____,
необходимые сведения в целях исполнения _____.

Предоставляю Оператору право осуществлять все действия (операции) с моими персональными данными, включая сбор, систематизацию, накопление, хранение, обновление, изменение, использование, обезличивание, блокирование, уничтожение. Оператор вправе обрабатывать мои персональные данные посредством внесения их в электронную базу данных, передавать в необходимом объеме в:

_____
_____
_____
(Наименование организации и ссылка на законодательство, на основании которого происходит передача персональных данных)

Я оставляю за собой право отозвать свое согласие посредством составления соответствующего письменного документа, который может быть направлен мной в адрес Оператора по почте заказным письмом с уведомлением о вручении либо вручен лично под расписку представителю Оператора.

Я ознакомлен с юридическими последствиями моего отказа о предоставлении Оператору моих персональных данных, необходимых для исполнения _____.

В случае получения моего письменного заявления об отзыве настоящего согласия на обработку персональных данных, Оператор обязан прекратить обработку персональных данных и уничтожить персональные данные в срок, не превышающий тридцати рабочих дней с даты поступления указанного отзыва.

«____» _____ 20___ г. _____
(Подпись)