

**Инструкция ответственного
за организацию обработки персональных данных
в МАОУ «Белоевская СОШ»**

1. Общие положения

1.1. Инструкция ответственного за организацию обработки персональных данных в МАОУ «Белоевская СОШ» (далее - Инструкция) определяет в обязанности и права сотрудника, назначенного ответственным за организацию обработки персональных данных.

1.2. В настоящей Инструкции используются сокращения, термины и определения, приведенные в таблицах 1 и 2 соответственно.

Таблица 1 – Перечень сокращений

Сокращение	Расшифровка сокращений
ИСПДн	Информационная система персональных данных
ПДн	Персональные данные
Роскомнадзор	Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций - уполномоченный орган по защите прав субъектов персональных данных
ФАПСИ	Федеральное агентство правительственной связи и информации при Президенте Российской Федерации
ФСТЭК России	Федеральная служба по техническому и экспортному контролю

Таблица 2 – Перечень терминов и определений

Термин	Определение	Источник
Автоматизированная обработка персональных данных	Обработка персональных данных с помощью средств вычислительной техники	Федеральный закон Российской Федерации от 27.06.2006 № 152-ФЗ «О персональных данных»
Администратор безопасности	Сотрудник, ответственный за обеспечение безопасности персональных данных в информационной системе	постановление Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»
Безопасность информации	Деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и	ГОСТ Р 50922-2006

	непреднамеренных воздействий на защищаемую информацию	
Доступность информации (ресурсов информационной системы)	Состояние информации (ресурсов автоматизированной информационной системы), при котором субъекты, имеющие право доступа, могут реализовать их беспрепятственно	Р 50.1.056-2005
Защита информации	Состояние защищенности информации (данных), при котором обеспечены ее их (конфиденциальность, доступность и целостность)	ГОСТ Р 50922-2006
Информационная система персональных данных	Совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств	Федеральный закон Российской Федерации от 27.06.2006 № 152-ФЗ «О персональных данных»
Информационные технологии	Процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов	Федеральный закон Российской Федерации от 27.06.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»
Контролируемая зона	Пространство, в пределах которого осуществляется контроль над пребыванием и действиями лиц и/или транспортных средств.	ГОСТ Р 56115-2014
Конфиденциальность информации	Обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя	Федеральный закон Российской Федерации от 27.06.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»
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	Федеральный закон Российской Федерации от 27.06.2006 № 152-ФЗ «О персональных данных»
Персональные данные	Любая информация, относящаяся прямо или косвенно к определенному или определяемому физическому лицу (субъекту персональных данных)	Федеральный закон Российской Федерации от 27.06.2006 № 152-ФЗ

		«О персональных данных»
Система защиты информации	Совокупность органов и (или) исполнителей, используемой ими техники защиты информации, а также объектов защиты информации, организованная и функционирующая по правилам и нормам, установленными соответствующими документами в области защиты информации	ГОСТ Р 50922-2006
Событие информационной безопасности	Выявленное состояние системы, услуги или состояние сети, указывающее на возможное нарушение политики обеспечения информационной безопасности, нарушение или отказ мер и средств контроля и управления или прежде неизвестная ситуация, которая может иметь значение для безопасности	ГОСТ Р ИСО/МЭК 27000-2012
Средства вычислительной техники	Совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем	ГОСТ Р 50739-95
Средства криптографической защиты информации	Шифровальные (криптографические) средства защиты информации конфиденциального характера К СКЗИ относятся: - реализующие криптографические алгоритмы преобразования информации аппаратные, программные и аппаратно-программные средства, системы и комплексы, обеспечивающие безопасность информации при ее обработке, хранении и передаче по каналам связи, включая СКЗИ; - реализующие криптографические алгоритмы преобразования информации аппаратные, программные и аппаратно-программные средства, системы и комплексы защиты от несанкционированного доступа к информации при ее обработке и хранении; - реализующие криптографические алгоритмы преобразования информации аппаратные, программные и аппаратно-программные средства, системы и комплексы защиты от навязывания ложной информации, включая средства имитозащиты и "электронной подписи"; - аппаратные, программные и аппаратно-программные средства, системы и комплексы изготовления и распределения ключевых документов для СКЗИ независимо от вида носителя ключевой информации.	Приказ ФАПСИ от 13.06.2001 № 152

Уязвимость	Недостаток (слабость) программного (программно-технического) средства или информационной системы в целом, который (которая) может быть использована для реализации угроз безопасности информации	ГОСТ Р 56545-2015
Целостность информации	Состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими на него право	Р 50.1.056-2005
Обработка персональных данных без использования средств автоматизации	Действия с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, которые осуществляются при непосредственном участии человека	Постановление Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»

1.3. Настоящая Инструкция разработана на основании следующих нормативных правовых актов:

- Федеральный закон от 27.06.2006 № 152-ФЗ «О персональных данных»;
- постановление Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состав и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;
- приказ ФАПСИ от 13.06.2001 № 152 «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну»;
- приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 27.10.2022 № 178 «Об утверждении Требований к оценке вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона «О персональных данных»;
- приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 28.10.2022 № 179 «Об утверждении Требований к подтверждению удаления персональных данных»;
- приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 28.10.2022 № 180 «Об утверждении форм уведомлений о намерении осуществлять обработку персональных данных, об

изменении сведений, содержащихся в уведомлении о намерении осуществлять обработку персональных данных, о прекращении обработки персональных данных»;

– приказ Федеральной службы безопасности Российской Федерации от 13.02.2023 № 77 «Об утверждении порядка взаимодействия операторов с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, включая информирование ФСБ России о компьютерных инцидентах, повлекших неправомерную передачу (предоставление, распространение, доступ) персональных данных».

1.4. При назначении сотрудника ответственным за организацию обработки ПДн, его должностная инструкция дополняется правами и обязанностями, предусмотренными настоящей Инструкцией, с соблюдением положений действующего законодательства Российской Федерации.

В своей деятельности ответственный за организацию обработки ПДн руководствуется законодательством Российской Федерации, локальными актами МАОУ «Белоевская СОШ» (далее – Учреждение), относящимися к обработке и защите ПДн, а также настоящей Инструкцией.

Ответственный за организацию обработки ПДн включается в состав комиссии по определению уровня защищенности ПДн при их обработке в ИСПДн, утверждаемый приказом руководителя Учреждения.

1.5. Ответственный за организацию обработки ПДн осуществляет методическое руководство деятельностью администратора безопасности.

1.6. С настоящей Инструкцией и дополненной должностной инструкцией ответственный за организацию обработки ПДн знакомится под подпись.

2. Обязанности ответственного за организацию обработки персональных данных

2.1. Ответственный за организацию обработки ПДн:

– обязан знать и выполнять требования законодательства Российской Федерации и локальных актов Учреждения, устанавливающих правила обработки и защиты ПДн;

– знать цели обработки ПДн и перечень, обрабатываемых ПДн в ИСПДн, а также обрабатываемых без использования средств автоматизации;

– обеспечивать взаимодействие с Роскомнадзором в соответствии с «Инструкцией о порядке взаимодействия с уполномоченным органом по защите прав субъектов персональных данных в МАОУ «Белоевская СОШ», в том числе по своевременному направлению в территориальный орган по защите прав субъектов ПДн уведомления об изменении сведений, содержащихся в уведомлении о намерении осуществлять обработку персональных данных, а также в случае установления факта неправомерной или случайной передачи (предоставления, распространения, доступа) ПДн, повлекшей нарушение прав субъектов ПДн;

– организовывать взаимодействие с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, включая информирование федерального органа исполнительной власти, уполномоченного в области обеспечения безопасности, о компьютерных инцидентах, повлекших неправомерную передачу (предоставление, распространение, доступ) персональных данных, в порядке, определенном указанным федеральным органом исполнительной власти;

– осуществлять оценку вреда, который может быть причинен субъектам персональных данных, персональные данные которых обрабатываются в Учреждении

(далее – оценка вреда). По результатам оценки вреда составлять соответствующий акт по форме, утверждаемой приказом руководителя Учреждения;

- организовывать размещение на официальном сайте Учреждения (при его наличии) «Политики в отношении обработки персональных данных в МАОУ «Белоевская СОШ», а также обеспечивать её актуализацию;

- организовывать ведение перечня сотрудников Учреждения, доступ которых к ПДн, обрабатываемым в ИСПДн и без использования средств автоматизации, необходим для выполнения ими трудовых (служебных) обязанностей;

- обеспечивать поддержание в актуальном состоянии перечня ПДн, обрабатываемых в ИСПДн в Учреждении;

- организовывать режим обеспечения безопасности помещений, в которых размещены средства вычислительной техники ИСПДн, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения, а также осуществлять периодическую проверку состояния физической защиты ИСПДн (средства охраны и физического доступа в контролируемых зонах ИСПДн);

- обеспечивать актуальность перечня помещений, в которых осуществляется обработка ПДн и размещены средства вычислительной техники ИСПДн;

- в случае необходимости вносить предложения руководителю по обеспечению антивирусной защиты в ИСПДн;

- контролировать изменения в конфигурации ИСПДн и оценивать возможный вред, который может быть причинен субъектам ПДн в результате указанных изменений, а также организовывать работы по восстановлению конфигурации ИСПДн и системы защиты информации;

- обеспечивать контроль за организацией и проведением мероприятий по выявлению (поиску), анализу и устранению уязвимостей в ИСПДн, а также внеплановых процедур выявления (поиска) анализа и устранения уязвимостей на основе анализа журналов событий информационной безопасности;

- контролировать уровень защищенности ПДн, обрабатываемых в ИСПДн и организовывать мероприятия по доработке системы защиты информации с целью обеспечения установленного для ИСПДн уровня защищенности ПДн;

- организовывать проведение мероприятий по заключению договоров на работы по защите ПДн;

- доводить до сведения сотрудников Учреждения положения законодательства Российской Федерации о персональных данных, локальных актов по вопросам обработки персональных данных, требований к защите персональных данных;

- организовывать обучение и контроль знаний сотрудников, осуществляющих обработку ПДн в ИСПДн, а также без использования средств автоматизации, в области защиты и обработки ПДн с письменным подтверждением проведения указанных мероприятий;

- обеспечивать своевременное выполнение сотрудниками требований действующего законодательства Российской Федерации, а также нормативных актов в сфере обработки и обеспечения безопасности персональных данных;

- организовывать прием и обработку обращений и запросов субъектов персональных данных или их представителей и (или) осуществлять контроль за приемом и обработкой таких обращений и запросов;

- осуществлять внутренний контроль за соблюдением сотрудниками норм действующего законодательства Российской Федерации в сфере обработки и обеспечения безопасности ПДн. Результаты внутреннего контроля докладываются руководителю отчетом либо служебной запиской;

- инициировать не реже 1 раза в 3 года контроль за выполнением требований к защите персональных данных при их обработке в информационных системах персональных данных, утвержденных постановлением Правительства Российской Федерации от 01.11.2012 № 1119;

- инициировать не реже 1 раза в год проведение проверки наличия средств криптографической защиты информации, эксплуатационной и технической документации к ним, соблюдения условий использования средств криптографической защиты информации.

3. Права

3.1. Ответственный имеет право:

- знакомиться в установленном порядке с документами и материалами, необходимыми для выполнения возложенных на него обязанностей;

- подготавливать предложения руководителю Учреждения по защите ПДн, обрабатываемых в ИСПДн, и обеспечения работ по организации обработки ПДн;

- разрабатывать проекты организационно-распорядительных документов (приказы, распоряжения) по защите ПДн, обрабатываемых в ИСПДн, и организации обработки ПДн в целом;

- требовать от сотрудников соблюдения требований действующего законодательства Российской Федерации в сфере обработки и обеспечения безопасности, а также требований, установленных организационно-распорядительной документацией по защите ПДн МАОУ «Белоевская СОШ»;

- вносить предложения руководителю Учреждения о привлечении к дисциплинарной ответственности сотрудников, систематически нарушающих требования по обработке и защите ПДн;

- давать сотрудникам обязательные для выполнения указания по обработке и защите ПДн, определяемые законодательством Российской Федерации и локальными актами Учреждения.