СОГЛАСОВАНО
Заместитель руководителя Управления Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций по Центральному федеральному округу

Г. М. Королёва

( )

УТВЕРЖДАЮ
Министр образования Московской области

М. Б. Захарова

«__» _____ 20 г.

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ

ГОСУДАРСТВЕННЫМ ПРОФЕССИОНАЛЬНЫМ ОБРАЗОВАТЕЛЬНЫМ ОРГАНИЗАЦИЯМ МОСКОВСКОЙ ОБЛАСТИ В СФЕРЕ ОРГАНИЗАЦИИ ОБРАБОТКИ И ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ИНФОРМАЦИИ ОГРАНИЧЕННОГО ДОСТУПА

СОГЛАСОВАНО
Заведующий отделом мобилизационной подготовки и защиты информации

И.В. Тимохин

« » _____ 20 г.

РАЗРАБОТАЛ
Консультант отдела мобилизационной подготовки и защиты информации

И.И. Лысенко

« » _____ 20 г.

СОДЕРЖАНИЕ

1. Введение……..…..8
2. Нормативные правовые акты, регламентирующие обработку информации ограниченного доступа……..…….....9
3. Персональные данные……10
4. Согласие субъекта персональных данных ……...……13
5. Оператор персональных данных...……..15
6. Перечень действий по приведению процессов обработки персональных данных в соответствие требованиям федерального законодательства ……17
6.1. Назначение ответственного лица и администратора информационных систем ……...……18
6.2. Описание процессов и сведений ограниченного доступа, обрабатываемых в Организации ……...……19
6.3. Оценка вреда, который может быть причинен субъектам персональных данных ……19
6.4. Определение перечня лиц, допущенных в соответствии с их должностными обязанностями к обработке информации ……..…20
6.5. Издание Политики Организации в отношении обработки персональных данных ……..……....21
6.6. Выделение информационных систем персональных данных ....…..……....21
6.7. Определение актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных…...23
6.8. Определение уровня защищённости персональных данных при их обработке в информационных системах персональных данных ……..…24
6.9. Организация обработки персональных данных, осуществляемой без использования средств автоматизации ...……..25
6.10. Издание Положения о порядке организации и проведения работ по защите информации……...26
6.11. Разработка и внедрение системы защиты информации ограниченного доступа…….……....27
6.12. Оценка эффективности принимаемых мер по обеспечению безопасности информации ограниченного доступа……..29
7. Регуляторы в области персональных данных……...30
7.1. Направление уведомления об обработке персональных данных в Управление Роскомнадзора по Центральному федеральному округу……...32
8. Ответственность за нарушение норм, регулирующих обработку и защиту информации……..……...33

9. Приложения:

Приложение 1. Типовая форма согласия на обработку персональных данных.
Приложение 2. Типовая форма приказа об организации работ по приведению процессов обработки и обеспечения безопасности информации ограниченного доступа в соответствие требованиям законодательства.
Приложение 3. Типовая форма положения о порядке организации и проведения работ по защите информации ограниченного доступа.
Приложение 4. Типовая форма инструкции ответственного по защите информации ограниченного доступа.
Приложение 5. Типовая форма перечня процессов и сведений ограниченного доступа, обрабатываемых в Организации.
Приложение 6. Типовая форма протокола оценки вреда, который может быть причинён субъектам, при обработке их персональных данных.
Приложение 7. Типовая форма списка лиц, допущенных в соответствии с их должностными обязанностями к обработке информации ограниченного доступа.
Приложение 8. Типовая форма политики в отношении обработки персональных данных.
Приложение 9. Типовая форма перечня информационных систем персональных данных.
Приложение 10. Типовая форма технического паспорта на ИСПДн.
Приложение 11. Типовая форма списка пользователей информационных систем персональных данных.
Приложение 12. Типовая форма инструкции по работе пользователей информационной системы персональных данных.
Приложение 13. Типовая форма модели угроз безопасности персональных данных при их обработке в информационной системе персональных данных.
Приложение 14. Типовая форма акта определения уровня защищенности персональных данных при их обработке в ИСПДн.
Приложение 15. Типовая форма перечня мест хранения бумажных носителей персональных данных.
Приложение 16. Типовая форма приказа об утверждении документов по вопросам обработки и обеспечения безопасности информации.
Приложение 17. Типовая форма журнала учёта паролей пользователей ИСПДн.
Приложение 18. Типовая форма журнала учёта МНИ.
Приложение 19. Типовая форма Декларации соответствия требованиям безопасности информационных систем персональных данных.
Приложение 20. Типовая форма уведомления об обработки персональных данных.

Термины и определения

Термин	Определение
Автоматизированная обработка персональных данных	Обработка персональных данных с помощью средств вычислительной техники.
Безопасность персональных данных	Безопасность персональных данных при их обработке в информационных системах обеспечивается с помощью системы защиты персональных данных, нейтрализующей актуальные угрозы, определённые в соответствии с ч. 5 статьи 19 Федерального закона «О персональных данных».
Доступ к персональным данным	Возможность получения персональных данных и их использования.
Доступность информации	Обеспечение доступа к информации и связанным с ней активам авторизованных пользователей по мере необходимости.
Информационная система	Совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.
Информационная система персональных данных	Совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.
Конфиденциальность персональных данных	Операторы и иные лица, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять ПДн без согласия субъекта ПДн, если иное не предусмотрено федеральным законом.
Крипто база данных	Программно-аппаратный комплекс для обеспечения усиления функций безопасности при хранении информации и программ в базах данных, а так же при аудите доступа к чувствительной информации.
Материальный носитель биометрических персональных данных	Машиночитаемый носитель информации (в том числе магнитный и электронный), на котором осуществляется запись и хранение сведений, характеризующих физиологические особенности человека и на основе которого можно установить его личность.

Термин	Определение
Межсетевой экран	Система межсетевой защиты (комплекс аппаратных или программных средств), позволяющая разделить каждую сеть на две и более части с целью реализации набора правил, определяющих условия прохождения сетевых пакетов с данными через границу из одной части общей сети в другую.
Неавтоматизированная обработка персональных данных	Обработка персональных данных без использования средств автоматизации, если такая обработка соответствует характеру действий (операций), совершаемых с персональными данными с использованием средств автоматизации, то есть позволяет осуществлять в соответствии с заданным алгоритмом поиск персональных данных, зафиксированных на материальном носителе и содержащихся в картотеках или иных систематизированных собраниях персональных данных, и (или) доступ к таким персональным данным.
Несанкционированный доступ (несанкционированные действия)	Доступ к информации или действия с информацией, осуществляемые с нарушением установленных прав и (или) правил доступа к информации или действий с ней с применением штатных средств информационной системы или средств, аналогичных им по своим функциональному предназначению и техническим характеристикам.
Недекларированные возможности (НДВ)	Недостаток или слабое место в системмном или прикладном программном обеспечении, которое может быть использовано для реализации угрозы безопасности персональных данных.
Носитель персональных данных	Бумажный или машинный носитель информации, содержащий персональные данные, например: бумажные документы, магнитные диски, CD/DVD, USB-флэш диски и т.п.).
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.

Термин	Определение
Обучающиеся	Физическое лицо, осваивающее образовательную программу.
Общедоступные источники персональных данных	Это персональные данные, доступ неограниченного круга лиц, к которым предоставлен самим субъектом персональных данных либо по его просьбе. В целях информационного обеспечения могут создаваться общедоступные источники персональных данных (адресные книги, справочники), в которые с письменного согласия субъекта персональных данных могут включаться его фамилия, имя, отчество, год и место рождения, адрес, абонентский номер, сведения о профессии и иные персональные данные, сообщаемые субъектом персональных данных. Сведения, включенные в указанные общедоступные источники, должны быть в любое время оттуда исключены по требованию субъекта персональных данных.
Оператор персональных данных	Лицо, которое обрабатывает персональные данные с помощью информационных систем обработки персональных данных и которое привлекается для проведения работ по обеспечению безопасности персональных данных на основании заключённого с этим лицом договора.
Персональные данные	Сведения о личности, которые включаются в информационную систему государственных, общественных и частных, корпоративных организаций по инициативе индивидуума или в силу закона в целях реализации его прав и обязанностей в процессе участия в самых разных социальных процессах и отношениях. Это любая информация, относящаяся к определённому или определяемому на основании такой информации физическому лицу.
Предоставление персональных данных	Действия, направленные на раскрытие персональных данных определённому лицу или определённому кругу лиц.
Распространение персональных данных	Действия, направленные на раскрытие персональных данных неопределенному кругу лиц.
Трансграничная передача персональных данных	Передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

Термин	Определение
Угроза безопасности персональных данных	Совокупность условий и факторов, создающих потенциальную опасность несанкционированных действий, в том числе случайного доступа к персональным данным, результатом которых могут стать уничтожение, изменение, блокирование, копирование, представление, распространение персональных данных, а так же иные неправомерные действия при их обработке в информационных системах.
Уровень защищённости персональных данных	Комплексный показатель, характеризующий требования, исполнение которых обеспечивает нейтрализацию определённых угроз безопасности персональных данных при их обработке в информационных системах.
Целостность информации	Состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими на него право.

Сокращения

АРМ	Автоматизированное рабочее место
ИС	Информационная система
ИСПДн	Информационная система персональных данных
МНИ	Машинные носители информации
НДВ	Недекларированные возможности
НСД	Несанкционированный доступ (несанкционированные действия)
Организация	Государственная бюджетная (автономная) профессиональная образовательная организация Московской области
ОС	Операционная система
ПДн	Персональные данные
ПК	Персональный компьютер
ПО	Программное обеспечение
Роскомнадзор	Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций
СЗИ	Средство защиты информации
СКУД	Система контроля управления доступа
УБПДн	Угрозы безопасности персональных данных
УЗ	Уровень защищенности
ФСБ	Федеральная служба безопасности
ФСТЭК	Федеральная служба по техническому и экспортному контролю

1. Введение

Настоящий документ представляет собой методические рекомендации (далее – Рекомендации), разъясняющие руководителям Организаций последовательность действий силами самого образовательного учреждения по приведению процессов обработки и обеспечения безопасности информации ограниченного доступа (за исключением информации, составляющей государственную тайну) в соответствие требованиям федерального законодательства.

Под информацией ограниченного доступа (далее – информация) понимаются сведения, доступ к которым ограничен нормативно-правовыми актами. Они устанавливают условия отнесения информации к сведениям, составляющим коммерческую тайну, служебную тайну и иную тайну, обязательность соблюдения конфиденциальности такой информации, а также ответственность за ее разглашение[1].

ПДн относятся к информации ограниченного доступа, так как попадают под действие Федерального закона Российской Федерации от 27.07.2006 № 152 «О персональных данных» (далее - Закон), целью которого является «обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну»[2] (реализация статьи 23 п. 1. Конституции Российской Федерации на законодательном уровне).

Именно ПДн сотрудников и обучающихся составляют значительную часть в общем объёме информации, обрабатываемой в Организации. Поэтому Рекомендации в основном посвящены вопросам, связанным с ПДн.

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

Цели Рекомендаций:

- описание единого подхода к обеспечению безопасности информации и приведению ИС Организаций в соответствие с законодательством;
- предоставление Операторам типовых решений и комплекта шаблонов организационно-распорядительных документов по организации системы защиты информации с целью снижения и оптимизации финансовых и трудовых затрат при приведении Организации в соответствие с требованиями законодательства.

[1] Федеральный закон РФ от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

[2] Федеральный закон РФ от 27.07.2006 № 152-ФЗ «О персональных данных», Статья 2.

Представленные образцы типовых документов разработаны с учётом общих требований законодательства Российской Федерации в сфере защиты ПДн.

Организация вправе редактировать структуру представленных типовых документов по согласованию с отделом мобилизационной подготовки и защиты информации Министерства образования Московской области, если существует необходимость таких изменений.

Организация несёт ответственность в соответствии с нормами действующего законодательства Российской Федерации за форму и содержание организационно-распорядительных документов, разработанных ею на основании предоставленных типовых документов и с учётом Рекомендаций.

Кроме организационно-распорядительных документов Рекомендации включают разъяснения по вопросам применения законодательства Российской Федерации о ПДн, которые по своему правовому статусу:

- не являются нормативным правовым актом;
- имеют информационно-разъяснительный характер;
- не препятствуют Организации руководствоваться нормами законодательства Российской Федерации о ПДн в понимании, отличающемся от трактовки, изложенной в Рекомендациях.

В случае, если для реализации требований Рекомендаций привлекается сторонняя организация, такая организация должна иметь лицензию ФСТЭК России на осуществление деятельности по технической защите конфиденциальной информации, а также, в случае поставки, установки или обслуживания шифровальных (криптографических) средств, соответствующую лицензию ФСБ России.

Рекомендации могут уточняться и корректироваться по мере необходимости.

2. Нормативные правовые акты, регламентирующие обработку информации ограниченного доступа

Правовые отношения, связанные с обработкой информации в Организациях, регламентируются следующими нормативными правовыми актами Российской Федерации:

1. Конституцией Российской Федерации.
2. Федеральными законами Российской Федерации:

- от 19.12.2005 г. № 160-ФЗ «О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных»;
- от 27.07.2006 г. №149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- от 27.07.2006 г. № 152-ФЗ «О персональных данных»;
- от 30.12.2001 г. № 197-ФЗ «Трудовой кодекс Российской Федерации»;
- от 27.07. 2004 г. № 79-ФЗ «О государственной гражданской службе РФ»;
- от 26.12.2008 г. № 294-ФЗ «О защите прав юридических лиц и индивидуальных предпринимателей при осуществлении государственного контроля (надзора) и муниципального контроля».

- от 25.07.2011 г. № 261-ФЗ «О внесении изменений в Федеральный закон «О персональных данных»».

3. Указом Президента РФ от 30.05.2005 г. № 609 «Об утверждении Положения о персональных данных государственного гражданского служащего РФ и ведении его личного дела».

4. Постановлений Правительства Российской Федерации:

- от 01.11.2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- от 15.09.2008 г. № 687 «Об утверждении Положения об обеспечении безопасности персональных данных, осуществляемой без использования средств автоматизации»;
- от 06.07.2008 г. № 512 «Об утверждении требований к материальным носителям биометрических персональных данных и технологиях хранения таких данных вне информационных систем персональных данных»;
- от 21.03.2012 г. № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных ФЗ «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами».

5. Постановления Правительства Московской области от 27.11.2002 г. № 573/46 «Об утверждении положения о порядке обращения с информацией ограниченного доступа в исполнительных органах государственной власти Московской области, государственных органах и государственных учреждений Московской области».

6. Приказами ФСТЭК России:

- от 18.02.2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;
- от 15.03.2013 г. № 274 «Об утверждении перечня иностранных государств, не являющихся сторонами Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных и обеспечивающих адекватную защиту прав субъектов персональных данных».

7. Приказом ФСБ России 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».

3. Персональные данные

Закон гласит: Персональные данные (ПДн) - это любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных)[3].

[3] Федеральный закон РФ от 27.07.206 № 152-ФЗ «О персональных данных», статья 3.

Словосочетание «любая информация» ясно указывает на широкое определение этого понятия.

Персональные данные – это так же сведения о личности, которые включаются в информационную систему государственных, общественных и частных, корпоративных организаций по инициативе индивидуума или в силу закона в целях реализации его прав и обязанностей в процессе участия в самых разных социальных процессах и отношениях. Это та часть частной жизни, которая определённым образом представлена и присутствует в публичном и гражданском секторах правовых отношений индивида с другими субъектами права.

ПДн – «содержание и объем обрабатываемых персональных данных должны соответствовать заявленным целям обработки. Обрабатываемые персональные данные не должны быть избыточными по отношению к заявленным целям их обработки»[4]

В Организации обрабатывается информация, необходимая работодателю в связи с трудовыми отношениями и касающаяся конкретного работника, а также об обучающихся и их родителях (законных представителей).

ПДн могут быть в любой форме – текстовой, цифровой, графической и т.д. Сюда входит все: и информация, зафиксированная на бумаге, и информация, хранимая в памяти компьютера и на машинных носителях информации (магнитных, оптических и т.д.).

ПДн – не однородны. Есть несколько категорий таких данных:

- специальные категории, если обрабатываются ПДн, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни субъектов персональных данных;
- биометрические, если обрабатываются сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность, и которые используются оператором для установления личности субъекта персональных данных и не обрабатываются сведения, относящиеся к специальным категориям ПДн;
- общедоступные, если обрабатываются ПДн субъектов персональных данных, полученные только из общедоступных источников ПДн;
- ПДн сотрудников оператора, если обрабатываются ПДн только указанных сотрудников оператора;
- иные категории, если не обрабатываются ранее указанные ПДн.

В связи с многочисленными вопросами, связанными с обработкой биометрических ПДн, Роскомнадзор, уполномоченный федеральный орган по защите прав субъектов ПДн, дал следующие разъяснения, касающиеся фотографических изображений, содержащихся в СКУД и паспортах субъектов персональных данных: «….необходимо принимать во внимание цель, которую преследует оператор при осуществлении действий, связанных с обработкой ПДн. В случае, если они используются оператором для установления личности субъекта персональных данных, то они являются биометрическими ПДн, поскольку, позволяют установить, принадлежит ли данному лицу предъявляемый СКУД пропуск.

[4] Федеральный закон РФ от 27.07.206 № 152-ФЗ «О персональных данных», статья 5, пункт 5

В случаях, когда сканирование паспорта осуществляется оператором для подтверждения осуществления определенных действий конкретным лицом без проведения процедур идентификации (установления личности), данные действия не могут считаться обработкой биометрических ПДн».

Также не являются биометрическими ПДн фотографическое изображение, содержащееся в личном деле работника (обучающегося), поскольку действия с использованием указанных данных направлены на подтверждение их принадлежности конкретному физическому лицу, чья личность уже определена и чьи ПДн уже имеются в распоряжении оператора»[5].

ПДн, набор которых не позволяет идентифицировать субъект, являются обезличенными. К защите обезличенных персональных данных требования законодательства минимальны.

С понятием «персональные данные» связан термин «обработка».

Под обработкой ПДн понимается любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств, включая:

- сбор – взятие у субъектов ПДн их данных;
- систематизацию – произведение действий по сортировке ПДн для выполнения целей обработки;
- накопление – произведение действий по хранению ПДн после их сбора;
- хранение – длительное хранение ПДн в базе данных ИСПДн или на бумажных (машинных) носителях информации для выполнения целей обработки;
- уточнение (обновление, изменение) – внесение изменений о субъекте ПДн в базу данных ИСПДн или на бумажных (машинных) носителях информации;
- использование – осуществление с помощью ПДн основной (производственной) и сопутствующей деятельности;
- распространение – передача ПДн в другие организации и информационные системы;
- обезличивание – процесс деперсонализации ПДн;
- блокирование – действие по приостановке процесса обработки ПДн;
- уничтожение – изъятие ПДн из ИСПДн или бумажных (машинных) носителей информации по достижению поставленной цели обработки, по требованию субъекта ПДн или по истечению сроков хранения, установленных действующим законодательством Российской Федерации.

Обработка ПДн бывает двух видов: автоматизированная и неавтоматизированная.

Автоматизированная обработка (обработка с помощью средств автоматизации - компьютера) осуществляется в ИСПДн и ей посвящена большая часть данных Рекомендаций.

[5] Разъяснения Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 30.08.2013 г.

Данный тип обработки ПДн регулируется постановлением Правительства Российской Федерации от 01.11.2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

Неавтоматизированная обработка (без использования средств автоматизации) – обработка ПДн, производящаяся на неэлектронных носителях (бумаге). Она регулируется постановлением Правительства Российской Федерации от 15.09.2008г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

4. Согласие субъекта ПДн

Одним из важнейших условий обработки ПДн является наличие явного согласия субъекта персональных данных на их обработку. Без такого согласия любые действия с персональными данными – незаконны.

Согласие – это свидетельство того, что субъект принял решение о предоставлении своих ПДн для обработки в соответствии с целями, которые заявляет оператор. Содержание согласия на обработку ПДн должно отвечать требованиям законодательства[6].

Письменное согласие требуется не во всех случаях, а только в строго ограниченных случаях:

· если ПДн для информационного обеспечения будут размещаться в общедоступных источниках (в том числе справочники, адресные книги)[7],

· если будут обрабатываться специальные категории ПДн[8];

· если биометрические ПДн используются для идентификации личности[9];

· если ПДн передаются за границу в страну, где не обеспечивается адекватная защита прав субъектов ПДн[10];

· если будет приниматься решение, порождающее юридические последствия в отношении субъекта персональных данных или иным образом затрагивающее его права и законные интересы, на основе исключительно автоматизированной обработки его ПДн[11];

· в случаях прямо предусмотренных иными федеральными законами (например, ст. 88 Трудового Кодекса РФ, или ст. 53 Закона «О связи»).

[6] Федеральный закон от 27.07.206 № 152-ФЗ «О персональных данных», статья 9, пункт 4.
[7] Федеральный закон РФ от 27.07.2006 г. № 152-ФЗ «О персональных данных», статья 8.1.
[8] Федеральный закон РФ от 27.07.2006 г. № 152-ФЗ «О персональных данных», статья 10.2., пункт 1.
[9] Федеральный закон РФ от 27.07.2006 г. № 152-ФЗ «О персональных данных», статья 11.1.
[10] Федеральный закон РФ от 27.07.2006 г. № 152-ФЗ «О персональных данных», статья 12.4., пункт 1
[11] Федеральный закон РФ от 27.07.2006 г. № 152-ФЗ «О персональных данных», статья 16.2.

Согласия субъекта не требуется, если обработка ПДн необходима для исполнения договора, стороной которого является сам субъект. Это исключение позволяет не требовать согласия при обработке ПДн сотрудников Организации, если эти данные обрабатываются в рамках трудового договора и при этом не распространяются, а также не предоставляются третьим лицам без согласия субъекта персональных данных[12].

Однако если Организация передаёт сведения о работнике, например, в банк для оформления зарплатных банковских карточек, то работодателю необходимо иметь согласие от этого работника, аналогично в случае зачисления стипендии на банковскую карточку.

Кроме того, при привлечении сторонних организаций для ведения кадрового и бухгалтерского учёта работодатель обязан соблюдать требования законодательства[13], в том числе, получить согласие работников на передачу их ПДн.

Поэтому рекомендуется единовременно получить у работников Организации и других субъектов (законных представителей несовершеннолетних учащихся, совершеннолетних обучающихся) согласие на обработку в письменной форме, предусмотрев разнообразные жизненные ситуации.

Типовая форма согласия приведена в Приложении № 1.

Также при передаче ПДн работника третьим лицам работодателю не требуется его согласия в следующих случаях если:

- обработка ПДн близких родственников работника осуществляется в объёме, предусмотренном унифицированной формой № Т-2[14], либо в случаях, установленных законодательством Российской Федерации (получение алиментов, оформление допуска к государственной тайне, оформление социальных выплат). В иных случаях, получение согласия близких родственников работника является обязательным условием обработки их ПДн;
- это необходимо в целях предупреждения угрозы жизни и здоровью работника, а также в других случаях, предусмотренных Трудовым кодексом Российской Федерации или иными федеральными законами;
- производится обработка ПДн работника при осуществлении пропускного режима на территорию служебных зданий и помещений работодателя, при условии, что организация пропускного режима осуществляется работодателем самостоятельно либо если указанная обработка соответствует порядку, предусмотренному коллективным договором, локальными актами работодателя, принятыми в соответствии со ст. 372 Трудового кодекса Российской Федерации.

[12] Федеральный закон РФ от 30.12. 2001 г. № 197-ФЗ Трудовой кодекс, статья 88.

[13] Федеральный закон РФ от 27.07.2006 г. № 152-ФЗ «О персональных данных», статья 6.

[14] Постановление Госкомстата Российской Федерации от 05.01.2004 г. № 1 «Об утверждении унифицированных форм первичной учетной документации по учету труда и его оплаты».

Кроме того, в соответствии с законодательством Российской Федерации[15] Организация обязана формировать открытые и общедоступные информационные ресурсы, содержащие информацию об их деятельности, и обеспечить доступ к этими ресурсам посредством размещения их в информационно-телекоммуникационных сетях, в том числе на официальном сайте образовательной организации в сети "Интернет".

Эта информация, должна содержать следующие ПДн: фамилию, имя, отчество руководителя образовательного учреждения (структурных подразделений, включая филиалы и представительства), его местонахождение, график работы, адрес электронной почты, справочные телефоны, информацию о персональном составе педагогических работников, их фамилии, имена, отчества, занимаемые должности, их уровень образования, квалификация, наличие учёной степени, учёного звания.

5. Оператор персональных данных

Оператор – это государственный орган или юридическое лицо самостоятельно или совместно с другими лицами осуществляющие обработку ПДн, а также определяющие цели обработки ПДн, состав ПДн и действия, совершаемые с ними[16].

То есть, Организация, как юридическое лицо, является оператором, осуществляющим обработку ПДн сотрудников и обучающихся с целью:

- ведения кадрового учёта сотрудников, состоящих в трудовых и служебных отношениях с Организацией;
- организации учебного процесса и контроля качества образования; учёта и анализа успеваемости обучающихся, оказания государственных услуг гражданам;
- начисления денежного содержания сотрудникам Организации и выплаты страховых взносов в Пенсионный фонд Российской Федерации, Фонд социального страхования Российской Федерации, Федеральный фонд обязательного медицинского страхования;
- начисления стипендий обучающимся.

Правовой основой этого процесса являются Федеральные законы Российской Федерации:

- от 29.12.2012 г. № 273-ФЗ «Об образовании в Российской Федерации»;
- от 30.12.2001 г. № 197-ФЗ Трудовой кодекс Российской Федерации;
- от 05.08.2000 г. № 117-ФЗ Налоговый кодекс Российской Федерации,
- от 06.12.2011 г. № 402-ФЗ «О бухгалтерском учёте»;

[15] Федеральный закон РФ от 29.12.2012 г. № 273-ФЗ «Об образовании в Российской Федерации», статья 29.
[16] Федеральный закон РФ от 27.07.2006 г. № 152-ФЗ «О персональных данных», статья 3.

- от 24.07.2009 г. № 212-ФЗ «О страховых взносах в Пенсионный фонд Российской Федерации, Фонд социального страхования Российской Федерации, Федеральный фонд обязательного медицинского страхования и территориальные фонды обязательного медицинского страхования»;
- от 26.02.1997 г. № 31-ФЗ «О мобилизационной подготовке и мобилизации в Российской Федерации».

Организация в качестве оператора вправе поручить обработку ПДн другому лицу на основании заключаемого с этим лицом договора. При этом ответственность перед субъектом ПДн за действия указанного лица несёт оператор. Лицо, осуществляющее обработку ПДн по поручению оператора, несёт в свою очередь ответственность перед оператором.

В ситуации, когда оператор арендует вычислительные мощности и программное обеспечение, в частности «1С: Предприятие - хх», в «облаке», предоставляемом компанией, которая в этом случае не является обработчиком ПДн., но в договоре обязательно должна быть установлена обязанность такого лица соблюдать конфиденциальность ПДн и обеспечивать безопасность при их обработке.

Оператор так же несёт определённую ответственность по выполнению обязательств, накладываемых федеральным законодательством[17], в том числе:

- он обязан до начала обработки ПДн уведомить уполномоченный орган по защите прав субъектов персональных данных о своём намерении осуществлять их;
- он обязан получить согласие субъекта на обработку его ПДн. А каждый субъект вправе требовать от оператора уточнения своих ПДн, их блокирования или уничтожения, если информация является неполной, устаревшей, неточной, незаконно полученной;
- он обязан при обработке ПДн принимать меры, необходимые для их защиты: правовые, организационные и технические.

Организация работ по защите информации возлагается на руководителя оператора, а методическое руководство и контроль за эффективностью предусмотренных мер защиты информации – на ответственного за защиту информации (в том числе за организацию обработки ПДн).

[17] Федеральный закон от 27.07.2006 г. № 152-ФЗ «О персональных данных», статьи 6.(пункт 1.), 18.1. (пункт 1.) и 22.

6. Перечень действий по приведению процессов обработки информации ограниченного доступа в соответствие требованиям федерального законодательства

Мероприятия по приведению процессов обработки ПДн и обеспечению безопасности информации в соответствие с требованиями федерального законодательства в этой области, проводимые Организацией, можно условно разделить на следующие этапы:

- назначение лица ответственного за защиту информации в Организации (далее - ответственный);
- описание процессов и сведений ограниченного доступа, обрабатываемых в Организации;
- оценка вреда, который может быть причинён субъектам ПДн;
- определение перечня лиц, допущенных в соответствии с их должностными обязанностями к обработке конфиденциальной информации;
- издание Политики Организации в отношении обработки ПДн;
- выделение информационных систем персональных данных;
- определение актуальных угроз безопасности ПДн при их обработке в ИСПДн;
- определение исходного уровня защищённости (УЗ) персональных данных при их обработке в ИСПДн;
- организация обработки ПДн, осуществляемой без использования средств автоматизации;
- издание Положения об обработке и обеспечении безопасности информации ограниченного доступа;
- разработка и внедрение системы защиты информации в Организации;
- ознакомление работников Оператора, непосредственно осуществляющих обработку ПДн, с положениями законодательства Российской Федерации о ПДн, в том числе требованиями по защите ПДн, документами, определяющими политику оператора в отношении обработки ПДн, другими локальными актами по вопросам обработки ПДн;
- оценка эффективности принимаемых мер по обеспечению безопасности информации;
- направление уведомления об обработке ПДн в Управление Роскомнадзора по Центральному федеральному округу.

Описание каждого из этапов приводятся в соответствующих разделах Рекомендаций.

6.1. Назначение ответственного лица и администратора ИСПДн

Назначение ответственного – первый шаг на пути оператора по приведению процессов обработки и обеспечению безопасности информации в соответствие требованиями федерального законодательства.

Ответственным может быть, лицо, отвечающее за обеспечение режима безопасности, или любой другой сотрудник Организации, на которого возложены эти обязанности в приказном порядке.

При выборе указанного лица необходимо учитывать, что оно будет обязано:

– осуществлять внутренний контроль за соблюдением Организацией и его работниками законодательства Российской Федерации о защите информации, в том числе требований по защите ПДн;

– доводить до сведения работников Организации положения федерального законодательства о персональных данных, локальных актов по вопросам обработки ПДн и требований по их защите;

– проводить работы по защите информации в ИСПДн.

Подробное описание прав и обязанностей ответственного приведено в «Положении о порядке организации и проведения работ по защите информации ограниченного доступа» (Приложение № 3) и в «Инструкции ответственного по защите информации ограниченного доступа» (Приложения № 4).

В помощь ответственному в техническом вопросе защиты информации может быть по приказу назначен администратор ИС, на которого возлагаются работы по настройке и сопровождению СЗИ, техническому обслуживанию АРМ информационных систем, ведению журнала выдачи паролей и т.д.

Ответственному вначале его деятельности по приведению процессов, в рамках которых происходит обработка информации, в соответствии с требованиями законодательства, необходимо провести предварительный анализ информационных ресурсов Организации:

– изучение содержания входящих и исходящих информационных потоков путём интервьюирования должностных лиц и специалистов Организации;

– изучение внутренней и внешней организационно-распорядительной документации;

– выявление в информационных потоках ПДн;

– анализ оснований установления категорий и степеней конфиденциальности выявленных ПДн;

– уточнение целей, выявление условий начала и прекращения обработки ПДн, определение сроков обработки для каждой установленной категории ПДн;

– определение структурных подразделений и должностных лиц, использующих в своей деятельности ПДн, их правомочности в принятии решений, касающихся определения целей, условий и сроков обработки ПДн;

– выявление реализованных на данный момент мер обеспечения безопасности ПДн.

Типовая форма приказа приведена в Приложении № 2.

6.2. Описание процессов и сведений ограниченного доступа, обрабатываемых в Организации

Ответственному для проведения инвентаризации информационных ресурсов Организации целесообразно в помощь привлечь сотрудников, имеющих представление о процессах и наличии в их составе сведений ограниченного доступа. Особое внимание необходимо обратить на документы, обрабатываемые в таких подразделениях, как:

- кадровое делопроизводство;
- учебная часть;
- бухгалтерия;
- преподавательская;
- медицинский кабинет;
- архивы, в том числе электронные;
- библиотека.

Результатом работы ответственного должен стать «Перечень процессов и сведений ограниченного доступа, обрабатываемых в Организации» (далее – Перечень), содержащий:

– наименования процессов обработки информации;

– цели обработки;

– способ обработки;

– категории субъектов ПДн, чьи данные обрабатываются или тип обрабатываемой информации;

– содержание сведений ограниченного доступа;

– правовые основания обработки;

– наименование подразделений (должностей работников), использующих в работе сведения такого рода.

Типовая форма и пример заполнения Перечня приведена в Приложении № 5.

Данный документ должен содержать сведения, являющиеся исходными данными для оценки вреда субъекту ПДн и планирования дальнейших действий по организации защиты ПДн.

6.3. Оценка вреда, который может быть причинён субъектам персональных данных

Оценка вреда субъекту ПДн проводится относительно каждого информационного ресурса, установленного в ходе инвентаризации. Однако в настоящее время единой методики оценки вреда и определения влияния его размера на состав принимаемых оператором мер защиты ПДн, пока не существует.

Формально размер потенциального вреда должен влиять на требуемый уровень защищённости ПДн и чем выше потенциальный вред, тем более строгие меры защиты обязан принимать оператор.

Поэтому оценку степени возможного вреда, который может быть причинён субъекту ПДн в результате нарушения свойств безопасности ПДн (конфиденциальности, целостности, доступности) целесообразно проводить экспертным методом комиссией, назначаемой приказом по Организации.

В состав комиссии включаются ответственный и руководители (представители) подразделений, осуществляющих обработку ПДн. Комиссия на основании экспертных оценок в зависимости от степени возможных негативных последствий для субъектов ПДн оценивает степень возможного вреда по следующей качественной (вербальной) шкале:

– **низкий уровень вреда** – если нарушение требований законодательства в области ПДн может привести к незначительным негативным последствиям;

– **средний уровень вреда** – если нарушение требований законодательства в области ПДн может привести к определённым негативным последствиям;

– **высокий уровень вреда** – если нарушение требований законодательства в области ПДн может привести к значительным негативным последствиям.

В дальнейшем при разработке мер необходимо соотносить данный указанный вред и принимаемые оператором меры, направленные на обеспечение выполнения обязанностей, предусмотренных законодательством в области ПДн.

Результат оценки вреда, который может быть причинён субъектам ПДн, оформляется документально соответствующим Протоколом (Приложение № 6).

6.4. Определение перечня лиц, допущенных в соответствии с их должностными обязанностями к конфиденциальной информации

Ответственному необходимо определить и утвердить перечень лиц, доступ которых к конфиденциальной информации, необходим для выполнения ими служебных (трудовых) обязанностей.

Типовая форма «Списка лиц, допущенных в соответствии с их должностными обязанностями к информации ограниченного доступа» приведена в Приложении № 7.

Для этих сотрудников необходимо предусмотреть в трудовом договоре соглашение о неразглашении конфиденциальной информации. Также требуется под роспись ознакомить их с положениями законодательства Российской Федерации о ПДн, в том числе требованиями по защите ПДн, другими документами Организации, устанавливающими порядок обработки и обеспечения безопасности Информации[18], а также с «Инструкцией по работе пользователей в информационной системе персональных данных» (Приложение № 12).

[18] Федерального закона «О персональных данных» от 27.07.2006 г., статья 18.1., п. 1. п.п. 6.

6.5. Издание Политики Организация в отношении обработки персональных данных

В соответствии с законодательством РФ[19] Организация обязана «опубликовать или иным образом обеспечить неограниченный доступ к документу, определяющему его политику в отношении обработки персональных данных, а также к сведениям реализуемых требований по защите персональных данных».

Поэтому ответственному необходимо разработать, утвердить и разместить в открытом доступе (например, на сайте или информационном стенде Организации) «Политику в отношении обработки персональных данных Организации». Типовая форма такой политики приведена в Приложении № 8.

6.6. Выделение информационных систем персональных данных

Определение способа обработки ПДн оказывает существенное влияние на состав мер их защиты. Если при автоматизированной обработке информации обязательно применение тех или иных технических мер защиты, то при неавтоматизированной – можно обойтись только некоторыми организационными мерами, что проще и дешевле.

При выделении ИСПДн ответственному необходимо принять во внимание следующее:

1. ИСПДн определяется как совокупность ПДн, содержащихся в базе данных, а также комплекс информационных технологий и технических средств, позволяющих осуществлять обработку таких данных. Эти информационные системы могут объединять несколько средств обработки (компьютеры, серверы, принтеры) или состоять только из одного рабочего места (компьютера).

2. Предназначение системы (цель обработки ПДн в ИСПДн) так, как не допускается объединение баз данных в ИСПДн, обработка которых осуществляется в целях, несовместимых между собой.

3. В какой локальной вычислительной сети Организации ведётся обработка ПДн. Необходимо провести сегментацию сети, используя представление о процессах и схеме самой сети, выделить в её инфраструктуре отдельные совокупности технических средств (сегменты сети), в каждом из которых:

- обрабатываются исключительно свойственные для данной совокупности технических средств категории ПДн;
- ставятся цели обработки ПДн, отличные от целей обработки ПДн в других сегментах сети.

4. Каждый, выделенный таким образом, сегмент сети может представлять собой отдельную ИСПДн.

Полученный перечень и состав ИСПДн и будет содержать объекты защиты информации в Организации, для которых применение организационных мер будет недостаточно.

[19] Федерального закона «О персональных данных» от 27.07.2006 г., статья 18.1.

В частности отделение сегмента от остальной сети должно осуществляться сертифицированным межсетевым экраном соответствующего класса.

Типовая форма такого перечня приведена в Приложении № 9.

На данный момент типовыми ИСПДн для Организации являются:

- ИС бухгалтерского учёта (наряду с ПДн сотрудников присутствуют сведения, относящиеся к бухгалтерской тайне);
- ИСПДн кадрового учёта;
- ИСПДн учебной части;
- ИСПДн дистанционного обучения.

Первые две информационные системы имеются во всех Организациях с целью ведения бухгалтерского и кадрового учёта и отсылки ведомостей в государственные органы. Основными особенностями данных систем, позволяющих определить их и выделить в отдельную категорию, является то, что их наличие обязательно для учреждения с точки зрения законодательства, а при обработке используются стандартные учётные программы или их модификации, обрабатываются только ПДн сотрудников. Чаще всего подобные системы представляют собой:

- автоматизированные рабочие места (ИСПДн кадрового учёта) с (без) наличием (я) постоянного подключения к сетям Интернет. В данном типе ИСПДн данные обрабатываются на одном компьютере;
- локальные вычислительные системы (ИС бухгалтерского учёта). Системы данного типа характеризуются обработкой ПДн на нескольких компьютерах, связанных между собой локальной вычислительной сетью Организации с (без) наличием (я) постоянного подключения к сетям Интернет.

Кроме того информационные системы различаются режимами обработки информации: - многопользовательский и однопользовательский.

Однопользовательский режим, это когда пользователь единолично выполняет все функции по обработке ПДн. Во всех остальных случаях ПДн обрабатываются в многопользовательском режиме с разграничением или без разграничения прав доступа.

ПДн обрабатываются в программах, имеющих подробную документацию и оговоренный функционал, а информация в эти системы поступает из личных дел сотрудников и пересылается через сеть Интернет, посредством машинных носителей информации (МНИ) или в бумажном виде.

Относительно обработки ПДн обучающихся в учебной части ответственному можно рассмотреть два варианта:

- обработка ведётся с помощью ИСПДн;
- ПДн обучающихся обрабатываются на бумажных носителях, а для оформления справок используется компьютер в качестве печатной машинки с последующим удалением из его памяти набранного текста. Если же документы сохранены в виде файла в памяти компьютера, то в этом случае нужно рассматривать такие действия как автоматизированную обработку ПДн.

На каждую ИСПДн ответственному необходимо разработать свой Технический паспорт, в котором требуется отразить назначение, техническую и программную составляющие информационной системы, а также применяемые средства защиты информации.

Типовая форма «Технического паспорта на информационную систему персональных данных» приведена в Приложении № 10.

Кроме вышеуказанных документов ответственный обязан разработать поимённый список сотрудников, участвующих в обработке конфиденциальной информации (Приложение № 11), и инструкцию по работе их в ИСПДн (Приложение № 12).

6.7. Определение актуальных угроз безопасности персональным данным при их обработке в информационных системах персональных данных

Определение типа угроз безопасности ПДн актуальных для каждой ИСПДн Организации, отражённых в соответствующем перечне, является прерогативой оператора[20], который проводит эту работу, руководствуясь следующими методическими документами:

– Методикой определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утверждённой заместителем директора ФСТЭК России 14.02.2008 г.;

– Базовой моделью угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утверждённой заместителем директора ФСТЭК России 15.02.2008 г., и по следующему алгоритму:

– необходимо определить уровень исходной защищённости ИСПДн;

– необходимо выделить основные типы потенциальных нарушителей на основании анализа круга лиц, имеющих возможность доступа к ИСПДн (как санкционированного, так и несанкционированного), определить перечень доверенных лиц, актуальных нарушителей; проанализировать возможности актуальных нарушителей;

– необходимо провести классификацию угроз безопасности ПДн и определить их перечень;

– необходимо экспертным методом оценить опасность угрозы и возможность её реализации;

– необходимо определить актуальность каждой из угроз и составить перечень актуальных угроз.

При этом под актуальной угрозой понимается совокупность условий и факторов, создающих актуальную опасность несанкционированного доступа в том числе случайного доступа к ПДн при их обработке в ИСПДн, результатом которого может стать: уничтожение, изменение, блокирование, копирование, представление, распространение ПДн, а так же иные неправомерные действия.

Выделяют следующие типы актуальных угроз безопасности ПДн для ИСПДн:

- 1-й тип – если для ИСПДн имеются угрозы, связанные с наличием недекларированных возможностей (НДВ) в системном программном обеспечении ИСПДн;

[20] Федерального закона РФ «О персональных данных» от 27.07.2006 г , статья 19., пункт 2.

- 2-й тип – если для ИСПДн имеются угрозы, связанные с наличием НДВ в прикладном программном обеспечении ИСПДн;

- 3-й тип – если имеются угрозы, не связанные с НДВ в системном и прикладном программном обеспечении ИСПДн;

Результатом этой деятельности является следующий документ - «Модель угроз безопасности персональных данных при их обработке в информационной системе персональных данных» (Приложение № 13).

6.8. Определение уровня защищённости персональных данных при их обработке в ИСПДн

Определение необходимого УЗ персональных данных при их обработке в ИСПДн предусматривает проведение следующих мероприятий:

- назначение комиссии. (Для определения УЗ персональных данных при их обработке в ИСПДн приказом по Организации назначается комиссия и её председатель. В состав комиссии включаются ответственный, руководители (представители) подразделений, осуществляющих обработку ПДн, преподаватели ИТ);
- изучение таких характеристик ИСПДн, как количество и категории субъектов ПДн, обрабатываемых в системе;
- рассмотрение перечня актуальных угроз безопасности ПДн.

Основные требования к защите ИСПДн по уровням защищённости представлены в таблице 1.

Таблица 1

Требования к защите ПДн при их обработке в ИСПДн

№ п\п	Т Р Е Б О В А Н И Я	Уровни защищённости			
		1	2	3	4
1	Режим обеспечения безопасности помещений, где обрабатываются ПДн.	+	+	+	+
2	Обеспечение сохранности носителей ПДн.	+	+	+	+
3	Утверждение переченя лиц, допущенных к обработке ПДн.	+	+	+	+
4	Использование систем защиты информации, прошедших процедуру оценки соответствия требованиям законодательства РФ.	+	+	+	+
5	Назначение должностного лица (работника), ответственного за обеспечение безопасности ПДн в ИСПДн.	+	+	+	–
6	Ограничение доступа лиц к содержанию электронного журнала сообщений.	+	+	–	–
7	Обязательная автоматическая регистрация в электронном журнале безопасности изменений полномочий сотрудников (операторов) по доступу к ПДн.	+	–	–	–
8	Наличие структурного подразделения, ответственного за обеспечение безопасности ПДн.	+	–	–	–

Зависимость уровней защищённости (УЗ) от характеристик ИСПДн и актуальных угроз безопасности различного типа представлена в таблице 2.

Таблица 2

Количество субъектов	Категория персональных данных	Категория субъектов	Актуальные угрозы	УЗ
Более 100 000	Специальные категории	Сотрудников	Угрозы 1-го типа	1
			Угрозы 2-го типа	2
			Угрозы 3-го типа	3
		Не сотрудников	Угрозы 1-го типа	1
			Угрозы 2-го типа	1
			Угрозы 3-го типа	2
	Биометрические данные	Сотрудников и не сотрудников	Угрозы 1-го типа	1
			Угрозы 2-го типа	2
			Угрозы 3-го типа	3
	Иные категории	Сотрудников	Угрозы 1-го типа	1
			Угрозы 2-го типа	3
			Угрозы 3-го типа	4
		Не сотрудников	Угрозы 1-го типа	1
			Угрозы 2-го типа	2
			Угрозы 3-го типа	3
	Общедоступные данные	Сотрудников	Угрозы 1-го типа	2
			Угрозы 2-го типа	3
			Угрозы 3-го типа	4
		Не сотрудников	Угрозы 1-го типа	2
			Угрозы 2-го типа	2
			Угрозы 3-го типа	4
Менее 100 000	Специальные категории	Сотрудников и не сотрудников	Угрозы 1-го типа	1
			Угрозы 2-го типа	2
			Угрозы 3-го типа	3
	Биометрические данные	Сотрудников и не сотрудников	Угрозы 1-го типа	1
			Угрозы 2-го типа	2
			Угрозы 3-го типа	3
	Иные категории	Сотрудников и не сотрудников	Угрозы 1-го типа	1
			Угрозы 2-го типа	3
			Угрозы 3-го типа	4
	Общедоступные данные	Сотрудников и не сотрудников	Угрозы 1-го типа	2
			Угрозы 2-го типа	3
			Угрозы 3-го типа	4

Результат определения требуемого УЗ персональных данных оформляется документально соответствующим Актом (Приложение № 14).

Важно: На каждую ИСПДн оформляется отдельный акт.

6.9. Организация обработки персональных данных, осуществляемой без использования средств автоматизации

Под неавтоматизированной обработкой ПДн понимается обработка ПДн, производящаяся на неэлектронных носителях (бумаге).

К неавтоматизированной обработке относятся:

- личные дела сотрудников;
- личные дела обучающихся;
- сведения о здоровье субъектов ПДн;
- различные виды бумажных журналов;
- другие виды обработки ПДн, производящиеся исключительно на бумаге.

Обработка ПДн, осуществляемая без использования средств автоматизации, должна осуществляться таким образом, чтобы в отношении каждой категории ПДн можно было определить места хранения их материальных носителей. При этом необходимо обеспечивать раздельное хранение материальных носителей ПДн, обработка которых осуществляется в различных целях.

Особое внимание ответственному необходимо уделить обработке сведений о здоровье субъектов ПДн, относящихся к специальной категории ПДн. Эти сведения следует обрабатывать на бумажных носителях (медицинская карта, листок здоровья и т.д.) и хранить в специально отведенном месте (медицинском кабинете). Обрабатывать эти персональные данные на компьютере не рекомендуется.

Типовая форма «Перечня мест хранения бумажных носителей персональных данных в Организации» приведена в Приложении № 15.

При хранении материальных носителей должны соблюдаться условия, обеспечивающие сохранность ПДн и исключающие несанкционированный доступ к ним. Перечень мер, необходимых для обеспечения таких условий, порядок их принятия, а также обязанности ответственного в «Положении о порядке организации и проведения работ по защите информации ограниченного доступа» указаны в Приложении № 3.

Смежными действиями, в плане обеспечения безопасности при неавтоматизированной обработке, так же являются требования положений законодательства об архивном делопроизводстве[21].

6.10. Издание Положения о порядке организации и проведения работ по защите информации ограниченного доступа

Необходимо разработать и утвердить «Положение о порядке организации и проведения работ по защите информации ограниченного доступа» (далее – Положение), устанавливающее в том числе:

– порядок организации и проведения работ в Организации для построения эффективной системы защиты информации от НСД, и её последующей эксплуатации;

[21] Федеральный закон РФ от 22.10.2004 г. № 125-ФЗ «Об архивном деле в Российской Федерации»

– права и обязанности должностных лиц Организации, ответственного и администратора ИСПДн за организацию и обеспечение безопасности информации;

– организационные и технические мероприятия по защите информации;

– условия ввода в эксплуатацию ИСПДн;

– порядок обработки информации, содержащей ПДн;

– особенности и правила обработки ПДн, осуществляемой без использования средств автоматизации;

– порядок обращения с ПДн и обеспечения сохранности носителей информации.

Типовая форма Положения приведена в Приложении № 3.

6.11. Разработка и внедрение системы защиты информации ограниченного доступа

Разработка и внедрение системы защиты информации предполагает реализацию в Организации совокупности организационно-технических мер.

В частности:

- утверждение разработанного ответственным пакета документации по защите информации (Приложении № 16) и его последующую реализацию в Организации;
- организацию режима обеспечения безопасности помещений, в которых размещены информационные системы, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения (установка замков, систем сигнализации и видеонаблюдения и т.п.);
- сведение к минимуму возможности нарушения политики безопасности с помощью любых средств, не связанных непосредственно с использованием ИС (физический вынос конфиденциальной информации на электронных или бумажных носителях);
- исключение ознакомления сотрудников с такими сведениями, если это не предусмотрено их должностными обязанностями;
- определение базового набора мер защиты информации для установленного УЗ ПДн в соответствии с Приказом ФСТЭК № 21[22];
- адаптацию выбранного базового набора мер с учётом структурно-функциональных характеристик и особенностей функционирования ИСПДн, информационных технологий, (в том числе исключение мер, непосредственно связанных с информационными технологиями, не используемыми в ИСПДн, или структурно-функциональных характеристик, не свойственных ей).

Например, перечень исключённых мер, типовых для информационных систем Организации, приведён в табл. 3.

[22] Приказ ФСТЭК России от 18.02.2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»

Таблица 3.

Индекс меры	Наименование меры	Обоснование
ИАФ.6	Идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей)	В ИС отсутствуют внешние пользователи
УПД.13	Реализация защищённого удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети	В ИС не предусмотрен удалённый доступ через сети Интернет
УПД.14	Регламентация и контроль использования в ИС технологий беспроводного доступа	В ИС не предусмотрено использование технологий беспроводного доступа
УПД.15	Регламентация и контроль использования в ИС мобильных технических средств	В ИС не предусмотрено использование мобильных технических средств
УПД.16	Управление взаимодействием с ИС сторонних организаций (внешние ИС)	Взаимодействие с внешними ИС не осуществляется
ЗСВ.1	Идентификация и аутентификация субъектов доступа и объектов доступа в виртуальной инфраструктуре, в том числе администраторов управления средствами виртуализации	В ИС не применяется виртуальная инфраструктура
ЗСВ.2	Управление доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре, в том числе внутри виртуальных машин	В ИС не применяется виртуальная инфраструктура
ЗИС.3	Обеспечение защиты информации от раскрытия, модификации и навязывания (ввода ложной информации) при её передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны, в том числе беспроводным каналам связи	Передача информации по каналам связи, имеющим выход за пределы контролируемой зоны, в том числе беспроводным каналам связи не осуществляется

- уточнение адаптированного базового набора мер с учётом не выбранных ранее мер, приведенных в Приказе ФСТЭК № 21, в результате чего определяются меры по обеспечению безопасности ПДн, направленные на нейтрализацию всех актуальных угроз безопасности персональных данных;
- дополнение уточнённого адаптированного базового набора мер мерами, обеспечивающими выполнение требований к защите ПДн, установленными иными нормативными правовыми актами в области обеспечения защиты информации;
- использование при построении систем защиты информации технических средств, прошедших в установленном порядке процедуру оценки соответствия требованиям безопасности. **Важно:** При покупке этих СЗИ требуйте от поставщика копии сертификатов ФСТЭК России об их применимости, заверенные их печатью;
- определение режима разграничения прав доступа пользователей информационной системы. Разграничение доступа - это когда вход в систему осуществляется по индивидуальному паролю пользователя (будь то пароль ОС или специального ПО). **Важно:** в Организации должны существовать процедуры предоставления и прекращения доступа. Предоставление доступа должен осуществлять ответственный (администратор ИСПДн) путём выдачи пароля пользователю с подписью в журнале учёта паролей (Приложении № 17). Прекращение доступа должно осуществляться после завершения производственной необходимости в доступе к ИС с последующей фиксацией в вышеуказанном журнале. Журнал хранится у администратора ИСПДн (ответственного);
- резервирование информации на МНИ, учтённых в соответствующем журнале (Приложении № 18), с последующим восстановлением работоспособности ИСПДн в случаях нарушения целостности и доступности информации. Журнал учёта хранится у ответственного, который в конце каждого года проверяет наличие МНИ у пользователей;
- обеспечение безопасного хранения материальных носителей ПДн (закупка и установка сейфов, металлических шкафов, создание специально оборудованных помещений и т.п.);
- использование средств гарантированного уничтожения материальных носителей ПДн (средства измельчения, сжигания, размагничивания и т.п.).

6.12. Оценка эффективности принимаемых мер по обеспечению безопасности информации

После реализации организационно-технических мероприятий по приведению информационных систем Организации в соответствие с требованиями федерального законодательства в области защиты информации силами самого образовательного учреждения оператор проводит оценку полученного результата в форме декларирования.

Декларирование соответствия – это подтверждение соответствия характеристик ИСПДн предъявляемым к ней требованиям, установленным законодательством Российской Федерации, руководящими и нормативно-методическими документами ФСТЭК России и ФСБ России. Декларирование соответствия может осуществляться на основе собственных доказательств оператора или на основании доказательств, полученных с участием привлечённых на договорной основе организаций, имеющих необходимые лицензии на осуществление деятельности по технической защите конфиденциальной информации.

Типовая форма Декларация приведена в Приложении № 19.

7. Регуляторы в области персональных данных

Государство осуществляет контроль за обработкой ПДн и защитой интересов субъектов ПДн.

Регулирование в этой обрасти осуществляют:

- Правительство Российской Федерации;
- Роскомнадзор России;
- ФСТЭК России;
- ФСБ России;
- Роструд РФ (Федеральная служба по труду и занятости РФ).

Правительство Российской Федерации осуществляет меры по обеспечению законности прав и свобод граждан. В сфере защиты ПДн Правительство Российской Федерации уполномочено[23]:

- устанавливать перечень мер, направленных на выполнение требований по обеспечению безопасности ПДн при их обработке;
- устанавливать УЗ определённых информационных систем;
- устанавливать требования к материальным носителям биометрических ПДн и технологиям хранения таких данных вне ИСПДн;
- определять государственные органы, осуществляющие лицензирование деятельности в этой области и утверждать положения о лицензировании.

Роскомнадзор определён уполномоченным органом по защите прав субъектов ПДн[24]. На Роскомнадзор возлагаются организационно-распорядительные функции обеспечения контроля, надзора и координации действий за соответствием обработки персональных данных требованиям закона[25]. Полномочия в этой области предусматривают проведение проверок, как в плановом режиме, так и по заявлениям субъектов. В рамках исполнения своих функций, должностные лица Роскомнадзора имеют право:

- выдавать обязательные для выполнения предписания по устранению выявленных нарушений в области обработки ПДн;

[23]Федеральный закон РФ от 27.07.2006 г. №152-ФЗ «О персональных данных»
[24]Постановление Правительства РФ от 15.12.2007 г. № 878.
[25]Постановление Правительства РФ от 16.03.2009 года № 228, «Об утверждении Положения о Федеральной службе по надзору в сфере связи и массовых коммуникаций».

- составлять протоколы об административном правонарушении или направлять в органы прокуратуры материалы для решения вопроса о возбуждении дел об административных правонарушениях, а также о возбуждении уголовных дел по признакам преступлений, связанных с нарушением прав субъектов ПДн;
- направлять заявления в орган, осуществляющий лицензирование деятельности оператора, для рассмотрения вопроса о принятии мер по приостановлению действия или аннулированию соответствующей лицензии;
- принимать меры по приостановлению или прекращению обработки ПДн, осуществляемой с нарушениями требований законодательства;
- рассматривать жалобы и обращения субъектов ПДн.

В структуре Роскомнадзора созданы соответствующие Управления в частности по Центральному федеральному округу. Именно в этот орган в соответствии с законодательством[26] могут обратиться субъекты ПДн, права и законные интересы которых были нарушены в связи с разглашением информации или иным неправомерным использованием такой информации, за судебной защитой своих прав, в том числе с исками о возмещении убытков, компенсации морального вреда, защите чести, достоинства и деловой репутации.

ФСТЭК Росси является регулятором в области обеспечения безопасности информации не криптографическими методами, а её нормативные акты, касающиеся защиты информации, являются обязательными для всех организаций, которые находятся под юрисдикцией России[27]. Она имеет свою систему сертификации СЗИ[28]. В рамках этой системы проводится обязательная сертификация средств, предназначенных для защиты ПДн. ФСТЭК России наделена следующими полномочиями:

- устанавливать требования по защите информации не криптографическими методами;
- определять состав и содержание организационных и технических мер по обеспечению безопасности информации ограниченного доступа;
- проводить лицензирование видов деятельности, связанных с защитой информации (в том числе ПДн);
- организовывать и проводить сертификацию СЗИ, использующих не криптографические методы защиты,
- осуществлять контроль и надзор за выполнением требований по обеспечению безопасности информации.

ФСБ России является регулятором в области использования криптографических СЗИ. ФСБ России отвечает за все вопросы применения криптографических методов защиты информации.

[26] Федеральный закон РФ от 27.07.2006 г. №149-ФЗ «Об информации, информационных технологиях и о защите информации», статья 17.

[27] Указ Президента РФ от 16.08.2004 г. № 1085 «Вопросы федеральной службы по техническому и экспортному контролю», п. 5 Положения о Федеральной службе по техническому и экспортному контролю.

[28] Регистрационный номер Госстандарта России РОСС RU.0001.01БИ00. «Положение о сертификации средств защиты информации по требованиям безопасности информации» Утв. Приказом Гостехкомиссии при Президенте РФ от 27.10.1995 г. № 199

ФСБ России имеет систему сертификации средств криптографической защиты информации[29]. В рамках этой системы проводится сертификация шифровальных средств.

Все органы действуют строго в рамках своей компетенции.

Таким образом:

- Роскомнадзор отвечает за общий контроль и надзор, представление интересов субъектов при обработке и защите их ПДн;
- ФСТЭК России регламентирует вопросы технической защиты ПДн не криптографическим методами;
- ФСБ регламентирует вопросы защиты ПДн криптографическими методами.

Причём при осуществлении своих функций знакомиться с ПДн, обрабатываемыми в Организации, имеют право только сотрудники Роскомнадзора.

7.1. Направление уведомления об обработке персональных данных в Управление Роскомнадзора по Центральному федеральному округу

Целью данного мероприятия является включение Организации в Реестр операторов, осуществляющих обработку ПДн, который ведёт Роскомнадзор.

Необходимо подчеркнуть, что отсутствие оператора в вышеуказанном реестре не помешает представителям Роскомнадзора посетить любую Организацию с плановой или внеплановой проверкой.

Ответственному необходимо разработать, утвердить и направить заказным письмом в Управление Роскомнадзора по Центральному федеральному округу уведомление об обработке ПДн по адресу: 117997, г. Москва, ГСП-7, Старокаширское шоссе, д. 2, корп. 10.

Для подготовки уведомления об обработке ПДн рекомендуется использовать электронную форму (http://pd.rkn.gov.ru/operators-registry/notification/) или воспользоваться Приложением № 20.

Организация вправе в установленных случаях не направлять уведомление об обработке персональных данных в Роскомнадзор[30].

Роскомнадзор вносит сведения из уведомления в реестр операторов в течение 30 дней с даты поступления документа. О свершившемся факте оператор может узнать самостоятельно на сайте Роскомнадзора по ИНН учреждения. В случае изменения сведений, оператор обязан уведомить о них сотрудников Роскомнадзора в течение 10 рабочих дней с момента возникновения таких изменений.

[29] Регистрационный номер Госстандарта России РОСС RU.0001.030001, Положение утв. Генеральным директором ФАПСИ 28.10.93 г.

[30] Федеральный закон РФ от 27.07.2006 г. №152-ФЗ «О персональных данных», статья 22.

8. Ответственность за нарушение норм, регулирующих обработку и защиту ПДн и информации ограниченного доступа

К нормативно-правовым актам, определяющим ответственность за нарушение в сфере защиты информации, относятся Федеральные законы Российской Федерации:

- от 30.12. 2001 г. № 197-ФЗ «Трудовой кодекс Российской Федерации» (ТК РФ);
- от 30.12.2001г. № 195-ФЗ «Кодекс Российской Федерации об административных правонарушениях» (КоАП РФ);
- от 13.06.1996 г. № 63-ФЗ «Уголовный кодекс Российской Федерации» (УК РФ).

Следовательно, лица, виновные в нарушении норм, регулирующих получение, обработку и защиту информации и ПДн, могут привлекаться к дисциплинарной и материальной ответственности в порядке, установленном ТК РФ, а также могут привлекаться к **гражданско-правовой, административной и уголовной ответственности** в порядке, установленном КоАП РФ и УК РФ.

Ниже в табл. 4 приведены, какие виды ответственности и меры наказания виновных предусмотрены вышеуказанными законами.

Таблица 4.

Статья	Нарушение	Мера наказания
УК РФ		
137. Нарушение неприкосновенности частной жизни	Незаконное собирание или распространение сведений о частной жизни лица, составляющих его личную или семейную тайну, без его согласия либо распространение этих сведений в публичном выступлении, публично демонстрирующемся произведении или средствах массовой информации	- Штраф до 200 000 рублей или в размере заработной платы или иного дохода осужденного за период до 18 месяцев. - Обязательные работы на срок до 360 часов. - Исправительные работы на срок до одного года. - Принудительные работы на срок до двух лет. - Лишение права занимать определённые должности или заниматься определённой деятельностью на срок до трёх лет или без такового. - Арест на срок до 4 месяцев. - Лишение свободы на срок до двух лет с лишением права занимать определённые должности или заниматься определённой деятельностью на срок до трёх лет.

Статья	Нарушение	Мера наказания
140. Отказ в предоставлении гражданину информации	Неправомерный отказ должностного лица в предоставлении собранных в установленном порядке документов и материалов, непосредственно затрагивающих права и свободы гражданина, либо предоставление гражданину неполной или заведомо ложной информации, если эти деяния причинили вред правам и законным интересам граждан.	- Штраф до 200 000 рублей или в размере заработной платы или иного дохода осужденного за период до 18 месяцев. - Лишение права занимать определённые должности или заниматься определённой деятельностью на срок от двух до пяти лет.
272. Неправомерный доступ к компьютерной информации	272.1. Неправомерный доступ к охраняемой законом компьютерной информации, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование компьютерной информации	- Штраф до 200 000 рублей или в размере заработной платы или иного дохода осужденного за период до 18 месяцев. - Исправительные работы на срок до одного года. - Ограничение свободы на срок до 2-х лет. - Принудительные работы на срок до 2-х лет, либо лишением свободы на тот же срок.
	272.2. То же деяние, причинившее крупный ущерб или совершённое из корыстной заинтересованности	- Штраф от 100 000 до 300 000 рублей или в размере заработной платы или иного дохода осужденного за период от одного года до двух лет. - Исправительные работы на срок от одного года до 2-х лет. - Ограничение свободы на срок до 4-х лет. - - Принудительные работы на срок до 4-х лет, либо лишением свободы на тот же срок.
	272.3. Деяния, предусмотренные 272.1 и 272.2, совершенные группой лиц по предварительному сговору или организованной группой либо лицом с использованием своего служебного положения	- Штраф до 500 000 рублей или в размере заработной платы или иного дохода осужденного за период до трёх лет с лишением права занимать определённые должности или заниматься определённой деятельностью на срок до 3 лет. - Ограничение свободы на срок до 4-х лет. - Принудительные работы на срок до 5 лет, либо лишением свободы на тот же срок.

Статья	Нарушение	Мера наказания
	Деяния, предусмотренные частями первой, второй или третьей настоящей статьи, если они повлекли тяжкие последствия или создали угрозу их наступления	- Лишение свободы на срок до семи лет.
273. Создание, использование и распространение вредоносных программ для ПК и сетей	273.1. Создание программ для ПК или внесение изменений в существующие программы заведомо приводящих к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушение работы ПК, системы ПК или их сети, а равно использование, либо распространение таких программ, либо машинных носителей с такими программами	- Лишение свободы на срок до 3-х лет со штрафом до 200 000 рублей.
	273.2. Те же деяния, совершённое по неосторожности и повлекшие тяжкие последствия	- Лишение свободы на срок до семи лет.
274. Нарушение правил эксплуатации ПК, системы ПК или их сети	274.1. Нарушение правил эксплуатации ПК, системы ПК или их сети лицом, имеющим доступ к ним, повлекшее уничтожение, блокирование или модификацию охраняемой законом информации, если эти деяния причинило существенный вред.	- Лишение права занимать определённые должности или заниматься определённой деятельностью на срок до 5 лет; - Либо обязательными работами от 180 до 240 часов; - Ограничением свободы на срок до двух лет.
	274.2. Те же деяния, совершённое по неосторожности и повлекшие тяжкие последствия.	- Лишение свободы на срок до 4-х лет.

Статья	Нарушение	Мера наказания
КоАП РФ		
13.11. Нарушение порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных)	Нарушение порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных)	- штраф: - на граждан в размере от 300 до 500 рублей; - на должностных лиц – от 500 до 1 000 рублей; - на юридических лиц – от 5 000 до 10 000 рублей.
13.12 Нарушение правил защиты информации	1. Нарушение условий, предусмотренных лицензией на осуществление деятельности в области защиты информации (за исключением информации, составляющей государственную тайну)	- штраф: - на граждан в размере от 300 до 500 рублей; - на должностных лиц – от 500 до 1 000 рублей; - на юридических лиц – от 5 000 до 10 000 рублей.
	2. Использование несертифицированных информационных систем, баз и банков данных, а также несертифицированных средств защиты информации, если они подлежат обязательной сертификации (за исключением СЗИ, составляющих государственную тайну)	- штраф: - на граждан в размере от 1 500 до 2 500 рублей с конфискацией несертифицированных СЗИ или без таковой; - на должностных лиц – от 2 500 до 3 000 рублей; - на юридических лиц – от 20 000 до 25 000 рублей с конфискацией несертифицированных СЗИ или без таковой.
	3. Грубое нарушение условий, предусмотренных лицензией на осуществление деятельности в области защиты информации (за исключением информации, составляющей государственную тайну)	- штраф: - на лиц, осуществляющих предпринимательскую деятельность без образования юридического лица в размере от 2 000 до 3 000 рублей или административное приостановление деятельности на срок до девяносто суток; - на должностных лиц – от 2 000 до 3 000 рублей; - на юридических лиц – от 20 000 до 25 000 рублей или административное приостановление деятельности на срок до девяносто суток.

Статья	Нарушение	Мера наказания
	4. Нарушение требований о защите информации (за исключением информации, составляющей государственную тайну), установленных федеральными законами и принятыми в соответствии с ними иными нормативными правовыми актами РФ, за исключением случаев, предусмотренных частями 1, 2, и 3 настоящей статьи	- штраф: - на граждан в размере от 500 до 1000 рублей; - на должностных лиц – от 1 000 до 2 000 рублей; - на юридических лиц – от 10 000 до 15 000 рублей.
13.14. Разглашение информации с ограниченным доступом	Разглашение информации, доступ к которой ограничен федеральным законом (за исключением случаев, если разглашение такой информации влечёт уголовную ответственность), лицом, получившим доступ к такой информации в связи с исполнением служебных или профессиональных обязанностей	- штраф: - на граждан в размере от 500 до 1000 рублей; - на должностных лиц – от 4 000 до 5 000 рублей.
19.4. Неповиновение законному распоряжению должностного лица органа, осуществляющего государственный надзор (контроль), муниципальный контроль.	1. Неповиновение законному распоряжению или требованию должностного лица органа, осуществляющего государственный надзор (контроль), муниципальный контроль.	-штраф: - на граждан в размере от 500 до 1000 рублей - на должностных лиц – от 2 000 до 4 000 рублей.
19.5. Невыполнение в срок законного предписания органа (должностного лица), осуществляющего государственный надзор (контроль), муниципальный контроль.	1. Невыполнение в установленный срок законного предписания (постановления, представления, решения) органа (должностного лица), осуществляющего государственный надзор (контроль), муниципальный контроль, об устранении нарушений законодательства.	- штраф: - на граждан в размере от 300 до 500 рублей; - на должностных лиц – от 1 000 до 2 000 рублей или дисквалификацию на срок до трёх лет; - на юридических лиц – от 10 000 до 20 000 рублей.

Статья	Нарушение	Мера наказания
19.6. Непринятие мер по устранению причин и условий, способствовавших совершению административного правонарушения.	Непринятие по постановлению (представлению) органа (должностного лица), рассмотревшего дело об административном правонарушении, мер по устранению причин и условий, способствовавших совершению административного правонарушения.	- штраф на должностных лиц в размере от 4 000 до 5 000 рублей.
19.7. Непредставление сведений (информации)	Оператор не представил уведомления об обработке ПДн или представили его в неполном объёме или в искажённом виде.	- штраф: - на должностных лиц – от 300 до 500 рублей или дисквалификацию на срок до трёх лет; - на юридических лиц – от 3 000 до 5 000 рублей.
ТК РФ		
90. Ответственность за нарушение норм, регулирующих обработку и защиту персональных данных работника.	Нарушение норм, регулирующих получение, обработку и защиту персональных данных работника	- Привлечение к дисциплинарной и материальной ответственности в порядке, установленном настоящим Кодексом и иными федеральными законами. - Привлечение к гражданско-правовой, административной и уголовной ответственности в порядке, установленном федеральными законами.

Приложение № 1

ЗАЯВЛЕНИЕ
о согласии на обработку персональных данных обучающегося (сотрудника) ГБПОУ МО _____

Я, _____
(фамилия, имя, отчество)
именуемый в дальнейшем «Субъект персональных данных» даю согласие образовательному учреждению ГБПОУ МО _____ на обработку персональных данных в соответствии со статьей 6, пункт 1 Федерального закона от 25.07.2006 № 152-ФЗ «О персональных данных».

Данные обучающегося / сотрудника (субъекта персональных данных):
Основной документ, удостоверяющий личность: __ _____
Серия:_____ Номер: ___ _____
Дата выдачи: _____ Кем выдан:
_____
Адрес по регистрации:_____ _____
Фактический адрес проживания: _____ __ .

Данные об операторе персональных данных:

Наименование: Государственное бюджетное профессиональное образовательное учреждение Московской области
«_____».
Адрес: Московская область, г.
_____

Цель обработки персональных данных *(выбрать)*:

– ***ведение кадрового учета сотрудников, состоящих в трудовых и служебных отношениях с Организацией;***
– организация учебного процесса и контроля качества образования; учет и анализ успеваемости обучающихся, оказание государственных услуг гражданам;
– ***начисление денежного содержания сотрудникам Организации и выплаты страховых взносов в Пенсионный фонд Российской Федерации, Фонд социального страхования Российской Федерации, Федеральный фонд обязательного медицинского страхования;***
– ***начисление стипендий обучающимся;***
– ***организация выездных экскурсий для обучающихся.***

Перечень действий с персональными данными:

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.

Перечень персональных данных, на обработку которых дается согласие субъекта персональных данных:

(Содержание и объем обрабатываемых персональных данных должны соответствовать заявленным целям обработки. Обрабатываемые персональные данные не должны быть избыточными по отношению к заявленным целям их обработки. Ст. 5, п.5. 152-ФЗ)

Срок действия данного согласия устанавливается на период:

Данное согласие действует с момента заключения мною _____ с оператором персональных данных и до истечения сроков, установленных действующим законодательством Российской Федерации.

Дата _____ . Подпись _____

(субъекта персональных данных)

Приложение № 2

Форма

ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ПРОФЕССИОНАЛЬНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ МОСКОВСКОЙ ОБЛАСТИ
«……»

П Р И К А З

_____ *№* _____

г. Энск

Об организации работ по выполнению требований Федерального закона от 27.07. 2006 № 152-ФЗ «О персональных данных» и принятых в соответствии с ним нормативных правовых актов в Государственном бюджетном профессиональном образовательном учреждении Московской области «……»

В соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» (далее - Федеральный закон) и постановлениями Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» (далее - постановление Правительства РФ) и от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», П Р И К А З Ы В А Ю:

1. Назначить ответственным за организацию обработки персональных данных, в Государственном бюджетном профессиональном образовательном учреждении Московской области «……» (далее – ГБПОУ МО «……») заместителя директора ГБПОУ МО «……» по безопасности А,В, Тарабаричева.

2. Назначить администратором безопасности информационных систем персональных данных (далее - ИСПДн) в ГБПОУ МО «……» лаборанта А,К, Маричева.

3. Ответственному за организацию обработки персональных данных:

3.1. Разработать и представить на утверждение проекты следующих организационно-распорядительных документов:

форма заявления о согласии на обработку персональных данных обучающегося (сотрудника) ГБПОУ МО «……»;
политика ГБПОУ МО «……» в отношении обработки персональных данных;
перечень и состав информационных систем персональных данных в ГБПОУ МО «……»;
технические паспорта на информационные системы персональных данных ГБПОУ МО «……»;
список пользователей информационных систем персональных данных
в ГБПОУ МО «……»;
инструкция по работе пользователей в информационной системе персональных данных ГБПОУ МО «……»;
модели угроз безопасности персональных данных при их обработке в информационных системах персональных данных в ГБПОУ МО «……»;
акты определения уровня защищенности персональных данных при их обработке в информационных системах персональных данных в ГБПОУ МО «……»;
перечень мест хранения бумажных носителей персональных данных в ГБПОУ МО «……»;
журнал учета выдачи паролей пользователям информационных систем персональных данных в ГБПОУ МО «……»;
уведомление в адрес уполномоченного органа по защите прав субъектов персональных данных о намерении ГБПОУ МО «……» осуществлять обработку персональных данных;
положение о порядке организации и проведения работ по защите информации ограниченного доступа в ГБПОУ МО «……»;
инструкцию ответственному за организацию обработки персональных данных в ГБПОУ МО «……»;
перечень процессов и сведений ограниченного доступа, обрабатываемых в ГБПОУ МО «……»;
протокол оценки вреда, который может быть причинен субъектам, при обработке их персональных данных в ГБПОУ МО «……»;
список сотрудников ГБПОУ МО «……», допущенных в соответствии с их должностными обязанностями к обработке информации ограниченного доступа;
журнал учета машинных носителей информации в ГБПОУ МО «……»;
программа и методики оценки эффективности реализованных в рамках системы защиты персональных данных мер по обеспечению безопасности персональных данных информационной системы персональных данных ГБПОУ МО «……..»;
форму листа ознакомления работников ГБПОУ МО «……» с положениями законодательства Российской Федерации о персональных данных, локальных актов по вопросам обработки персональных данных, требований к защите персональных данных;

перечень мер, необходимых для обеспечения условий, обеспечивающих сохранность персональных данных и исключающий несанкционированный к ним доступ;
перечень лиц, ответственных за реализацию мер, необходимых для обеспечения условий, обеспечивающих сохранность персональных данных и исключающий несанкционированный к ним доступ.

3.2. Опубликовать на официальном сайте ГБПОУ МО «……»:
документы, определяющие политику ГБПОУ МО «……» в отношении обработки персональных данных;
сведения о реализуемых требованиях в ГБПОУ МО «……» к защите персональных данных.

4. Контроль за исполнением приказа оставляю за собой.

Директор ГБПОУ МО «……»

Приложение № 3

Приложение № 6
к приказу от _____ 2015 г. № ___

ПОЛОЖЕНИЕ

О ПОРЯДКЕ ОРГАНИЗАЦИИ И ПРОВЕДЕНИЯ РАБОТ ПО ЗАЩИТЕ ИНФОРМАЦИИ ОГРАНИЧЕННОГО ДОСТУПА

В ГБПОУ МО ……..

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящее Положение разработано на основании требований:

- Федеральных законов Российской Федерации:
  - от 27.07.2006 г. № 152 «О персональных данных»,
  - от 27.07.2006 г. 149-ФЗ «Об информации, информационных технологиях и о защите информации»,
  - **от 29.07.2004 г. № 98-ФЗ «О коммерческой тайне»,**
  - от 30.12. 2001 г. № 197-ФЗ Трудовой кодекс Российской Федерации;
- постановлений Правительства Российской Федерации:
  - ***от 01.11.2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»,***
  - ***от 15.09.2008 № 687 «Об утверждении Положения об обеспечении безопасности персональных данных, осуществляемой без использования средств автоматизации»;***
- ***постановления Правительства Московской области от 27.11.2002 г. № 573/46 «Об утверждении положения о порядке обращения с информацией ограниченного доступа в исполнительных органах государственной власти Московской области, государственных органах и государственных учреждений Московской области».***

Под информацией ограниченного доступа (далее – информации) понимаются

сведения, доступ к которым ограничен нормативно-правовыми актами, в частности Указом Президента Российской Федерации от 6.03.1997 № 188 «Об утверждении перечня сведений конфиденциального характера», и отраженные в «Сводном перечне сведений конфиденциального характера», утвержденном постановлением Правительства Московской области от 27.11. 2002 № 573/46. Они устанавливают условия отнесения информации к сведениям, составляющим коммерческую тайну, служебную тайну и иную тайну, обязательность соблюдения конфиденциальности такой информации, а также ответственность за ее разглашение.

1.2. Персональные данные **(далее - ПДн) относятся к информации ограниченного доступа, так как попадают под действие Федерального закона Российской Федерации от 27.07.2006 № 152 "О персональных данных". Именно ПДн сотрудников и обучающихся составляют значительную часть в общем объёме информации, обрабатываемой в образовательных организациях.**

1.3. **Цель данного Положения – определение порядка организации и проведения работ в ГБПОУ для построения эффективной системы защиты информации (далее - СЗИ) от несанкционированного доступа, и её последующей эксплуатации. В частности, с целью обеспечение защиты прав и свобод субъектов персональных данных при обработке их ПДн в информационных системах ГБПОУ.**

1.4. **Под обработкой информации понимается любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств.**

1.5. **Информационная система (далее - ИС) – совокупность содержащихся в базах данных информации и обеспечивающих её обработку информационных технологий и технических средств.**

1.6. **Информационная система персональных данных (далее - ИСПДн) - информационная система, представляющая собой совокупность содержащихся в базе данных ПДн, и обеспечивающих их обработку информационных технологий и технических средств.**

1.7. **ИСПДн является информационной системой, обрабатывающей** иные категории персональных данных**, если в ней не обрабатываются персональные данные, относящиеся к специальным категориям ПДн, биометрические и общедоступные ПДн.**

1.8. **Положение предназначено для практического использования должностным лицам ответственным за защиту информации.**

1.9. **Требования настоящего Положения распространяется на все процессы обработки информации в ГБПОУ, как с использованием средств автоматизации, так и без использования таких средств, и являются обязательными для исполнения во всех структурных подразделениях, всеми должностными лицами ГБПОУ.**

1.10. **Настоящее Положение вступает в силу с момента его утверждения директором ГБПОУ и действует бессрочно, до замены его новым Положением.**

1.11. **За общее состояние защиты информации в ГБПОУ отвечает его руководитель.**

Персональная ответственность за организацию и выполнение мероприятий по защите информации в структурных подразделениях ГБПОУ возлагается на руководителей этих подразделений.

Ответственность за обеспечение защиты информации возлагается непосредственно **на пользователя информации** в соответствии с инструкцией «По работе пользователей информационной системы», утвержденной руководителем ГБПОУ.

Вариант № 1:

Проведения работ по защите информации в ИС с помощью встроенных средств безопасности сертифицированных лицензионных операционных систем и антивирусного программного обеспечения возлагается на администратора ИСПДн.

Контроль выполнения требований настоящего Положения возлагается на ответственного за защиту информации **в ГБПОУ (далее –** ответственный**).**

или вариант № 2: в случае, когда администратор ИСПДн и ответственный - одно физическое лицо:

На** ответственного за защиту информации **в ГБПОУ (далее – ответственный) возлагается:

- ***проведения работ по защите информации в ИСПДн с помощью встроенных средств безопасности сертифицированных лицензионных операционных систем и антивирусного программного обеспечения;***
- ***контроль выполнения требований настоящего Положения.***

1.12. Все работники, допущенные к обработке информации, обязаны соблюдать конфиденциальность информации в течение срока действия трудового договора. Для этих сотрудников необходимо предусмотреть в трудовом договоре соглашение о неразглашении информации.

1.13. Лица, виновные в нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных) несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с федеральным законодательством.

1.14. При необходимости для оказания услуг в области аттестации ИС можно привлекать специализированные организации, имеющие лицензию на этот вид деятельности.

1.15. Положение может уточняться и корректироваться по мере необходимости. Все изменения в Положение вносятся приказом.

2. ОХРАНЯЕМЫЕ СВЕДЕНИЯ И АКТУАЛЬНЫЕ УГРОЗЫ

2.1. Охраняемые сведения - информация, обрабатываемая в информационных системах структурных подразделениях ГБПОУ в соответствии с «Перечнем процессов и сведений ограниченного доступа, обрабатываемых в ГБПОУ МО «_____», а также представленная в виде носителей на бумажной, магнитной и иной основе.

2.2. Объекты защиты:

- ИСПДн различного назначения, участвующие в обработке информации, в соответствии с «Перечнем информационных систем ……»;
- помещения, где установлены ИСПДн или хранится информация на бумажных носителях в соответствии с «Перечнем мест хранения бумажных носителей персональных данных в ……..».

2.3. Актуальные угрозы безопасности объектов защиты.

В соответствии с моделями угроз безопасности персональных данных в ИСПДн, разработанными и утверждёнными в ГБПОУ, **актуальными являются только угрозы несанкционированного доступа** к информационным ресурсам ИСПДн с целью получения, разрушения, искажения и блокирования информации. Данный вид угроз в соответствии с постановлением Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении Требований к защите персональных данных при их обработке в информационных системах персональных данных» относится к **угрозам 3-го типа**

Применение средств технической разведки для перехвата информации, циркулирующей в ИСПДн ГБПОУ **маловероятно** с учётом её характера.

Основное внимание должно быть уделено защите информации, в отношении которой угрозы безопасности реализуются **без применения сложных технических средств**:

- обрабатываемой в ИСПДн от НСД нарушителей и непреднамеренных действий сотрудников ГБПОУ;
- выводимой на экраны мониторов компьютеров;
- хранящейся на физических носителях;
- циркулирующей в локальных вычислительных сетях ГБПОУ при несанкционированном подключении к данной сети;
- при подключении ИСПДн к сетям Интернет.

3. ОРГАНИЗАЦИОННЫЕ И ТЕХНИЧЕСКИЕ МЕРОПРИЯТИЯ ПО ЗАЩИТЕ ИНФОРМАЦИИ

3.1. Замыслом достижения целей защиты ИСПДн от НСД является обеспечение защиты информации путем выполнения требований нормативных правовых актов, принятыми ФСТЭК России в исполнении части 4 статьи 19 Федерального закона Российской Федерации «О персональных данных» для **четвёртого уровня**

защищённости ПДн.

3.2. Целью технической защиты информации в ГБПОУ является предотвращение НСД к информации при её обработке в ИСПДн, связанные с действиями нарушителей, включая пользователей информационных систем,

реализующих угрозы непосредственно в ИСПДн, а также нарушителей, не имеющих доступ к ИСПДн, реализующих угрозы из сетей Интернет с целью её разрушения, искажения, уничтожения, блокировки и несанкционированного копирования.

3.3. Целями организационных мероприятий по защите информации в ГБПОУ являются:

- организация режима обеспечения безопасности помещений, в которых размещены информационные системы, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения (установка замков, систем сигнализации и видеонаблюдения и т.п.);
- исключение непреднамеренных действий сотрудников ГБПОУ, приводящих к утечке, искажению, разрушению информации, в том числе ошибки эксплуатации ИС;
- сведение к минимуму возможности нарушения политик безопасности с помощью любых средств, не связанных непосредственно с использованием ИС (физический вынос информации на электронных или бумажных носителях);
- исключение ознакомления сотрудников с такими сведениями, если это не предусмотрено их должностными обязанностями;
- обеспечение безопасного хранения материальных носителей ПДн (закупка и установка сейфов, металлических шкафов, создание специально оборудованных помещений и т.п.);
- использование средств гарантированного уничтожения материальных носителей ПДн (средства измельчения, сжигания, размагничивания и т.п.);
- использование систем пожарной сигнализации и пожаротушения.

3.4. Руководитель ГБПОУ самостоятельно определяет состав и перечень мер, необходимых и достаточных для обеспечения выполнения обязанностей, предусмотренных п.1.1. настоящего Положения.

К таким мерам могут, в частности, относиться:

- назначение ответственного за организацию защиты информации;
- **издание комплекта документов, определяющих политику в отношении обработки ПДн в ГБПОУ, а также локальные акты, устанавливающих процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации**
- выбор в качестве основного средства защиты ИСПДн, не подключённых к сети Интернет, операционных систем «Windows 7 / 8 Professional» (далее - ОС), обладающих встроенными средствами защиты от НСД или других технических

средств защиты от НСД (Страж NT, Secret Net и др.);

- **настройка ОС на компьютерах ИС в соответствии с «Руководством по безопасной настройке» (настройка других технических средств защиты от НСД);**
- **сертификация вышеуказанных ОС (технических средств) по требованиям безопасности информации;**
- **определение режима разграничения прав доступа пользователей информационной системы. Разграничение доступа – это когда вход в систему осуществляется по индивидуальному паролю пользователя (будь то пароль ОС или специального программного обеспечения).**
- **выбор дополнительных технических средств, сертифицированных по требованиям безопасности информации, в случае когда применение таких средств необходимо для нейтрализации актуальных угроз. В частности, для ИСПДн, подключенных к сетям связи общего пользования ГБПОУ и (или) Интернет;**
- **использование средств антивирусной защиты;**
- **предотвращение организационными мерами НСД к обрабатываемой информации;**
- **организация процесса резервного копирования и архивирования как неотъемлемой части политики защиты информации;**
- **осуществление учета машинных носителей информации и их хранение в надежно запираемых и опечатываемых шкафах;**
- строгое соблюдение сотрудниками ГБПОУ «Инструкции по работе пользователей информационной системы».

3.5. Документальное оформление мероприятий по защите объекта информатизации включает:

- приказ об организации работ по приведению процессов обработки и обеспечения безопасности информации ограниченного доступа в соответствие требованиям законодательства;

- **положение о порядке организации и проведения работ по защите информации ограниченного доступа в ГБПОУ;**
- **перечень процессов и сведений ограниченного доступа, обрабатываемых в ГБПОУ;**
- **список лиц, допущенных в соответствии с их должностными обязанностями к обработке информации;**
- **перечень ИСПДн;**
- **акты определения уровня защищенности ИСПДн;**
- **технические паспорта ИС;**
- **список пользователей ИСПДн;**
- **перечень мест хранения бумажных носителей ПДн;**
- **инструкции ответственного и по работе пользователей ИС;**
- **журнал учёта паролей пользователей для работы в ИС;**
- **журнал учёта машинных носителей информации;**

- **декларацию о соответствии требованиям безопасности или «Аттестат соответствия требованиям безопасности».**

4. ВВОД В ЭКСПЛУАТАЦИЮ ИНФОРМАЦИОННЫХ СИСТЕМ

4.1. Необходимым условием для ввода в эксплуатацию информационных систем ГБПОУ является их соответствие требованиям Федерального закона «О персональных данных», постановления Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» и Приказа ФСТЭК России от 18.02.2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

4.2. Руководитель ГБПОУ самостоятельно принимает решение по организации работ по построению систем защиты ИСПДн или с привлечением сторонней организации, имеющей лицензию ФСТЭК России на осуществление деятельности по технической защите конфиденциальной информации, или силами самой образовательной организации.

4.3. В случае привлечения сторонней организации она проводит аттестационные испытания ИСПДн в соответствии с техническим заданием ГБПОУ (ГОСТ 34.602-89) и программой и методикой испытаний (ГОСТ 19.301-79), согласованной с ГБПОУ. В соответствии с национальным стандартом ГОСТ РО 0043-003-2012 «Защита информации. Аттестация объектов информатизации. Общие положения».

Испытания завершаются выдачей «Аттестата соответствия информационной системы требованиям безопасности информации».

4.4. В случае проведения работ по построению системы защиты ИС силами самого образовательной организации оценка полученного результата проводится в форме декларирования.

4.5. Для декларирования соответствия ИСПДн требованиям п. 3.1 комиссией, утвержденной приказом руководителя ГБПОУ, подготавливаются и представляются на систему:

- **акт определения уровня защищенности ИСПДн**
- **технический паспорт;**
- **организационно-распорядительная документация разрешительной системы доступа персонала к защищаемым ресурсам;**
- модель угроз безопасности персональных данных;
- сертификаты средств защиты информации, используемые при построении системы защиты;
- **инструкция по работе пользователей;**

- **инструкция ответственного за защиту информации.**

4.6. При использовании для защиты ИСПДн от НСД технических средств защиты информации их настройка проводится силами самой образовательной организации.

4.7. Контроль эффективности СЗИ осуществляется представителями отдела мобилизационной подготовки и защиты информации Министерства образования Московской области с оформлением акта на выполнение требований федерального законодательства по защите информации по обеспечению безопасности ПДн субъектов ПДн при их обработке с использованием средств автоматизации.

4.8. В случае положительных результатов испытаний СЗИ руководитель ГБПОУ декларирует соответствие ИС требованиям безопасности информации.

4.9. По результатам декларирования соответствия ответственным **разрабатываются и доводятся до сотрудников ГБПОУ под роспись**

«Инструкция по работе пользователей ИСПДн» и рекомендации о порядке выполнения мероприятий по защите информации.

5. ОСОБЕННОСТИ ОБРАБОТКИ ИНФОРМАЦИИ, СОДЕРЖАЩЕЙ ПЕРСОНАЛЬНЫЕ ДАННЫЕ

5.1. Правовое основание обработки ПДн ГБПОУ:

Федеральные законы Российской Федерации:

- «Об образовании в Российской Федерации» от 29.12.2012 № 273-ФЗ;
- Трудовой кодекс Российской Федерации (Федеральный закон от 30.12.2001 № 197-ФЗ);
- Налоговый кодекс Российской Федерации (Федеральный закон от 05.08.2000 № 117-ФЗ),
- «О бухгалтерском учёте» от 06.12.2011 № 402-ФЗ;
- «О страховых взносах в Пенсионный фонд Российской Федерации, Фонд социального страхования Российской Федерации, Федеральный фонд обязательного медицинского страхования и территориальные фонды обязательного медицинского страхования» от 24.07.2009 N 212-ФЗ.

5.2. Цель обработки ПДн:

- обработка персональных данных сотрудников ГБПОУ и сведений об их профессиональной служебной деятельности в целях ведения кадрового учёта;
- обработка персональных данных обучающихся, необходимых для оказания им услуг в области образования;
- начисление денежного содержания сотрудникам ГБПОУ и выплаты страховых взносов в Пенсионный фонд Российской Федерации, Фонд социального страхования Российской Федерации, Федеральный фонд обязательного медицинского страхования;
- начисление стипендий обучающимся.

–

–

– 5.3. Обработке подлежат только ПДн, которые отвечают целям их обработки. Содержание и объем обрабатываемых ГБПОУ ПДн соответствуют заявленным целям обработки, избыточность обрабатываемых данных не допускается.

– 5.4. При обработке ПДн ГБПОУ обеспечивается их точность, достаточность и в необходимых случаях актуальность по отношению к целям обработки персональных данных. ГБПОУ принимаются необходимые меры (обеспечивается их принятие) по удалению или уточнению неполных или неточных ПДн.

– 5.5. Хранение ПДн ГБПОУ осуществляется в форме, позволяющей определить субъекта ПДн, не дольше, чем этого требуют цели обработки ПДн, если срок их хранения не установлен федеральным законом, договором,

стороной которого, выгодоприобретателем или поручителем по которому является субъект ПДн. Обрабатываемые ПДн подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом. Конкретные обязанности по хранению документов возлагаются на лиц, осуществляющих обработку ПДн, в соответствии с их трудовыми функциями и закрепляются в трудовых договорах, должностных инструкциях и иных регламентирующих документах ГБПОУ.

5.6. Перечень ПДн:

- паспортные данные;
- дата и место рождения;
- биографические сведения;
- сведения об образовании;
- сведения о семейном положении;
- сведения о месте регистрации, проживании;
- сведения о состоянии здоровья сведения о наличии/отсутствии судимости;
- иное (указать).

5.7. Категории субъектов ПДн, персональные данные которых обрабатываются:

- сотрудники ГБПОУ;
- обучающиеся.

5.8. Все ПДн субъекта ГБПОУ следует получать у него самого. Если ПДн возможно получить только у третьей стороны, то субъект ПДн должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие. Должностное лицо ГБПОУ должно сообщить субъекту ПДн о целях, предполагаемых источниках и способах получения ПДн, а также о характере подлежащих получению ПДн и последствиях отказа дать письменное согласие на их получение.

5.9. ГБПОУ не имеет права получать и обрабатывать данные субъекта ПДн о его расовой, национальной принадлежности, политических взглядах, религиозных или философских убеждениях, состоянии здоровья, частной жизни. В случаях, непосредственно связанных с вопросами трудовых отношений, в соответствии со ст. 24 Конституции Российской Федерации работодатель вправе получать и обрабатывать данные о частной жизни работника только с его письменного согласия.

5.10. Субъект ПДн самостоятельно принимает решение о предоставлении своих ПДн и дает согласие на их обработку.

Обработка указанных данных возможна без его согласия в соответствии со ст. 6 Федеральным законом от 27.07.2006 № 152 «О персональных данных.

5.11. Согласие на обработку ПДн оформляется в письменном виде.

Письменное согласие на обработку своих персональных данных должно включать в себя:

- фамилию, имя, отчество, адрес субъекта ПДн, 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 ПДн;
- цель обработки ПДн;
- перечень ПДн, на обработку которых дается согласие субъекта персональных данных;
- перечень действий с ПДн, на совершение которых дается согласие, общее описание используемых оператором способов обработки ПДн;
- срок, в течение которого действует согласие, а также порядок его отзыва.

5.12. Согласие на обработку ПДн может быть отозвано субъектом ПДн по письменному запросу на имя руководителя ГБПОУ (*Может быть указано иное лицо, имеющее соответствующие полномочия от руководителя организации*).

5.13. Субъекты ПДн не должны отказываться от своих прав на сохранение и защиту тайны

5.14. Субъект ПДн имеет право на получение следующей информации:

- сведения о лицах, которые имеют доступ к ПДн или которым может быть предоставлен такой доступ;
- перечень обрабатываемых ПДн и источник их получения;
- сроки обработки ПДн, в том числе сроки их хранения;
- сведения о том, какие юридические последствия для субъекта ПДн может повлечь за собой обработка его ПДн.

5.15. Субъект ПДн вправе требовать от оператора уточнения своих ПДн, их блокирования или уничтожения в случае, если ПДн являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки.

5.16. Сведения о ПДн должны быть предоставлены субъекту ПДн оператором в доступной форме, и в них не должны содержаться персональные данные, относящиеся к другим субъектам ПДн.

–
–
–
–
–

–

– 5.17. Доступ к своим ПДн предоставляется субъекту ПДн или его законному представителю оператором при получении письменного запроса субъекта ПДн или его законного представителя. Письменный запрос должен быть адресован на имя руководителя ГБПОУ или уполномоченного руководителем лицо. Копии документов, содержащих ПДн, выдаются ГБПОУ в срок не позднее тридцати дней со дня подачи письменного заявления об их выдаче.При выдаче документов для ознакомления, а также запрашиваемых копий и справок, работник, занимающийся обработкой ПДн, обязан удостовериться в личности запрашивающего (или его представителя) и потребовать предоставление документа, подтверждающего соответствующие полномочия.

5.18. Субъект в праве обжаловать в уполномоченный орган по защите прав субъектов персональных данных (Управление Федеральной службы по надзору в сфере связи и массовых коммуникаций по Центральному федеральному округу) или в судебном порядке неправомерные действия или бездействия должностных лиц ГБПОУ при обработке и защите его ПДн.

– 5.19. Доступ к ПДн должен быть ограничен, в том числе путем определения перечня лиц, доступ которых к персональным данным, необходим для выполнения ими служебных (трудовых) обязанностей. Доступ работников ГБПОУ к ИСПДн ограничен системой разграничения прав доступа, реализуемой в рамках системы защиты ПДн с использованием технических и организационных мероприятий.

– 5.20. Предоставление ПДн третьим сторонам осуществляется только с предварительного письменного согласия субъекта, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью субъекта, а также в случаях, установленных законодательством Российской Федерации, в частности Федеральными законами «Об обязательном пенсионном страховании в Российской Федерации, «Об основах обязательного социального страхования, «Об обязательном медицинском страховании в Российской Федерации».

– Существенным условием договоров с третьими сторонами, в рамках, исполнения которых передаются ПДн, является обязанность соблюдения сторонами мер обеспечения безопасности ПДн при их обработке. Кроме того, в договорах в обязательном порядке определяется порядок передачи ПДн.

– ГБПОУ с согласия субъекта может поручать обработку ПДн третьим сторонам, а также выступать в роли лица, осуществляющего обработку ПДн по поручению других операторов ПДн.

– В случае если ГБПОУ поручает обработку третьей стороне, в поручении на обработку ПДн должны быть в обязательном порядке определены:

1. **перечень действий (операций) с ПДн, которые будут совершаться третьей стороной;**
2. **цели обработки (цели не должны противоречить целям, заявленным перед субъектом – в договоре с оператором, в согласии и т. д.);**

3. **обязанность третьей стороны соблюдать конфиденциальность ПДн и обеспечивать безопасность при их обработке;**
4. **требования к защите ПДн.**

– Федеральным законодательством может устанавливаться обязанность ГБПОУ непосредственно направлять информацию, содержащую ПДн, третьим лицам (отчетность, налоговые декларации и т.д.) либо право третьих лиц запрашивать указанную информацию в пределах их полномочий.

– В последнем случае передача информации осуществляется на основании письменных мотивированных запросов, оформленных на официальных бланках за подписью уполномоченного должностного лица. Запрос должен содержать цели и правовые основания затребования информации, срок предоставления такой информации, если иное не установлено законом.

– Ответы на запросы направляются законным получателям ПДн только в письменном виде и только в затребованном объеме.

– Получателями ПДн на законном основании, в том числе являются:

5. **Фонд социального страхования РФ;**
6. **Пенсионный фонд РФ;**
7. **Федеральная налоговая служба;**
8. **Федеральная инспекция труда;**
9. **иные органы надзора и контроля за соблюдением законодательства о труде;**
10. **правоохранительные и судебные органы.**

6.1.ОБРАЩЕНИЕ С МАТЕРИАЛЬНЫМИ НОСИТЕЛЯМИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Виды носителей

– Персональные данные в ГБПОУ хранятся на материальных носителях двух видов:

11. **машинные магнитные носители (далее – МНИ);**
12. **бумажные носители.**

– Организация обработки поступивших и создаваемых документов, содержащих ПДн, осуществляется в соответствии с принятыми в ГБПОУ нормами документооборота.

Хранение бумажных носителей

Бумажные (документальные) носители ПДн должны храниться в услови-

ях, исключающих несанкционированный доступ к ним посторонних лиц - в служебных помещениях в надежно запираемых шкафах (сейфах). При этом должны быть созданы надлежащие условия, обеспечивающие их сохранность.

–

–

– Хранение бумажных (документальных) носителей ПДн вместе с документами общего доступа запрещается, за исключением случаев, когда документы общего доступа являются приложениями к бумажным (документальным) носителям ПДн.

– Запрещается совместное хранение бумажных (документальных) носителей ПДн, обработка которых осуществляется в различных целях.

– Для каждой категории персональных данных должны быть определены и занесены в Перечень мест хранения бумажных носителей этой категории. В этом перечне указывают:

13. категории субъектов ПДн;
14. категории ПДн;
15. место хранения (номер или наименование помещения, в котором хранятся бумажные носители, номер шкафа (сейфа) в котором хранятся бумажные носители).

ПДн субъектов хранятся не дольше, чем этого требуют цели их обработки, и они подлежат уничтожению по истечению установленных сроков хранения информации, по достижении целей обработки или в случае утраты необходимости в их достижении.

Документы, содержащие ПДн, подлежат хранению и уничтожению в порядке, предусмотренном архивным законодательством Российской Федерации.

Использование и обеспечение сохранности машинных носителей информации

В целях предотвращения разрушения и утери обрабатываемой на компьютере информации пользователь ИСПДн должен осуществлять копирование необходимой информации по мере ее обновления на учтенные в установленном порядке МНИ (такие как: внешние жесткие диски, гибкие магнитные диски, USB флэш-накопители, карты флэш-памяти, оптические носители и др.). Эти носители должны быть учтены в Журнале учёта машинных носителей информации (далее – Журнал).

– В Журнале указывают:

16. **номер машинного носителя;**
17. **тип носителя;**
18. **Ф.И.О. работника;**
19. **дата получения и подпись работника;**
20. **Ф.И.О. Администратора ИСПДн;**
21. **дата возврата и подпись Администратора ИСПДн;**
22. **отметка об уничтожении;**

Кроме того, в этом Журнале необходимо учесть машинные носители информации с ЭЦП, а также те, которые используются для передачи ПДн третьей стороне.

Ответственность за ведение и хранение Журнала несёт ответственный, который в конце каждого года проверяет наличие МНИ у пользователей.

–

– В случае выхода из строя или принятия решения о прекращении использования машинного носителя в процессах обработки МНИ такой носитель уничтожается или с него стираются ПДн (способом исключающим возможность восстановление данных).

Вынос резервных копий баз данных ИСПДн, содержащих информацию персонального характера, из ГБПОУ запрещен. Передача и копирование их допустима только для прямого использования с целью технологической поддержки ИСПДн.

7. ОБЯЗАННОСТИ И ПРАВА ДОЛЖНОСТНЫХ ЛИЦ

7.1. Директор **организует работу по построению системы защиты ИС.**

В частности,

1. Назначает ответственного за организацию защиты информации из числа сотрудников ГБПОУ.
2. Утверждает комплект документов, определяющих политику в отношении обработки ПДн в учреждении, а также локальные акты, устанавливающих процедуры, направленные на предотвращение и выявление нарушений законодательства

Российской Федерации.

3. Утверждает меры и состав средств СЗИ, предложенных для обеспечения безопасности ПДн при их обработке в ИСПДн. При этом оценивает соотношение вреда, который может быть причинен субъектам ПДн и принимаемых мер по защите ИСПДн.

7.2. Заместитель директора по безопасности:

- **составляет Перечень процессов и сведений ограниченного доступа, обрабатываемых в ГБПОУ;**
- **контролирует наличие в трудовых договорах с сотрудниками из «Списка лиц, допущенных в соответствии с их должностными обязанностями к информации ограниченного доступа» соглашения о неразглашении информации;**
- **контролирует работу ответственного по организации и проведению работ по защите информации в ГБПОУ;**
- **предотвращает организационными мерами НСД к обрабатываемой в ИС информации;**
- **контролирует порядок подготовки, учета и хранения документов конфиденциального характера;**
- контролирует порядок передачи информации другим органам и организациям, а также между структурными подразделениями своей организации.

7.3. **Ответственный:**

- **разрабатывает и своевременно обновляет организационно-распорядительные документы по вопросам защиты информации;**

- **своевременно направляет в Управление Роскомнадзора по ЦФО уведомление о намерении Оператора осуществлять обработку персональных данных и сообщает о происшедших изменениях в процессе обработки персональных данных;**
- **организовывает работу по получению согласия субъектов персональных данных на обработку персональных данных в случаях, предусмотренных законодательством в данной сфере;**
- **знакомит работников ГБПОУ, непосредственно осуществляющих обработку ПДн, с положениями законодательства Российской Федерации о ПДн, в том числе требованиями к защите ПДн;**
- **контролирует исполнение приказов и распоряжений вышестоящих организаций по вопросам обеспечения безопасности информации;**
- **обеспечивает защиту информации, циркулирующей на объектах информатизации, организовывает работы по декларированию (аттестации) ИС на соответствие нормативным требованиям;**
- **проводит систематический контроль работы СЗИ, применяемых в ИС, а также за выполнением комплекса организационных мероприятий по обеспечению безопасности информации;**
- проводит инструктаж пользователей ИС;
- **контролирует выполнение администратором ИС обязанностей по обеспечению функционирования СЗИ (настройка и сопровождение подсистемы управления доступом пользователя к защищаемым информационным ресурсам ИС, антивирусная защита, резервное копирование данных и т.д.)**
- контролирует порядок учёта и хранения машинных носителей информации;
- присутствует (участвует) в работах по внесению изменений в аппаратно-программную конфигурацию ИС;
- **определяет порядок и осуществляет контроль ремонта средств вычислительной техники, входящих в состав ИС;**
- **принимает меры по оперативному изменению паролей при увольнении или перемещении сотрудников, имевших допуск к ИС;**
- требует от руководителей проверяемых подразделений устранения выявленных нарушений и недостатков, давать обязательные для исполнения указания по вопросам обеспечения положений инструкций по защите информации;
- требует от работников представления письменных объяснений по фактам нарушения режима конфиденциальности;
- **об имеющихся недостатках и выявленных нарушениях требований нормативных и руководящих документов по защите информации, а также в случае выявления попыток НСД к информации или попыток хищения,**

копирования, изменения незамедлительно принимает меры пресечения и докладывает руководителю ГБПОУ;

- ***вносит предложения руководителю ГБПОУ о внесении изменений в процессы обработки информации, а также в ИСПДн, если это обусловлено необходимостью обеспечения соответствия законодательству в сфере персональных данных;***
- ***вносит предложения руководителю ГБПОУ о поощрении или наложении взысканий на работников в связи с исполнением ими обязанностей, связанных с обработкой информации;***

- **в установленные сроки подготавливает необходимую отчетную документацию о состоянии работ по защите информации.**

7.4. Администратор ИСПДн:

- **обеспечивает настройку и бесперебойную эксплуатацию программных и технических средств обработки ПДн, входящих в состав ИС;**
- **обеспечивает настройку, бесперебойную эксплуатацию и мониторинг средств защиты информации;**
- **настраивает права доступа работников к ПДн и средствам их обработки в соответствии с ролевой моделью доступа;**
- **проводит инструктаж пользователей ИС по правилам эксплуатации программных и технических средств обработки ПДн, а также СЗИ, входящих в состав ИСПДн;**
- **меняет паролей у пользователей ИС не реже одного раза в три месяца либо при компрометации паролей;**
- **хранит дистрибутивы программного обеспечения средств обработки информации ИС;**
- **обеспечивает контроль действий представителей сторонних организаций (подрядчиков), при привлечении последних для обслуживания, настройки и ремонта средств обработки и защиты информации ИС;**
- **предоставляет необходимую информацию при проведении проверок регулирующими органами;**
- **оказывает содействие работникам, участвующим в процессах обработки и обеспечения безопасности ПДн, по вопросам использования средств обработки информации ИС, в рамках своей компетенции;**
- **незамедлительно уведомляет в случае обнаружения попыток или фактов несанкционированного доступа к ПДн о выявленных фактах ответственного.**

7.5. Руководители структурных подразделений**:**

- **лично отвечают за защиту информации в структурных подразделениях, сохранность машинных и иных носителей информации;**

- **организуют выполнение мероприятий по защите информации при использовании технических средств;**
- **участвуют в определении мест установки и количества АРМ, необходимых для обработки информации, а также пользователей этих ИС;**

- **участвуют в определении правил разграничения доступа к информации в ИС, используемых в ГБПОУ.**

8. ПЛАНИРОВАНИЕ РАБОТ ПО ЗАЩИТЕ ИНФОРМАЦИИ

8.1.Планирование работ по защите информации проводится на основании:

- **рекомендаций актов проверок контрольными органами;**
- **результатов анализа деятельности в области защиты информации;**
- **рекомендаций и указаний Роскомнадзора и ФСТЭК России;**
- **решений Московской областной комиссии по информационной безопасности.**

8.2. Для подготовки и реализации организационных и технических мероприятий по защите информации ответственный **составляется годовой план работ по защите информации.**

8.3. Контроль выполнения годового плана возлагается на руководителя ГБПОУ.

9. КОНТРОЛЬ СОСТОЯНИЯ ЗАЩИТЫ ИНФОРМАЦИИ

9.1. С целью своевременного выявления и предотвращения НСД к информации, хищения технических средств и носителей информации, предотвращения специальных программно-технических воздействий, вызывающих нарушение целостности информации или работоспособность систем информатизации, осуществляется контроль состояния и эффективности СЗИ.

– 9.2. Контролю подлежат как принятые меры организации обработки информации, так и меры по обеспечению её безопасности.

– 9.3. Рекомендуется в рамках проведения контроля проверить:

- **актуальность описания процессов обработки информации;**
- **актуальность перечня ИСПДн;**
- **актуальность перечня лиц, доступ которых к информации, обрабатываемой в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей;**
- **актуальность сведений, указанных в Политике в отношении обработки персональных данных организацией, проверка соблюдения ее положений и общедоступности;**

- **наличие письменных согласий субъектов ПДн и соответствия форм согласий требованиям законодательства;**
- **проверка соответствия оценки вреда, который может быть причинен субъектам ПДн текущей ситуации;**
- **наличие договоров с организациями, которым поручается обработка ПДн, на предмет наличия предусмотренных законодательством положений (*для случаев, когда Организация осуществляет поручение обработки персональных данных*);**
- **соответствие организации в ГБПОУ обработки информации, осуществляемой без использования средств автоматизации требованиям законодательства;**
- **проверка осведомленности работников ГБПОУ о положениях законодательства Российской Федерации о персональных данных, документов Организации, устанавливающих порядок обработки и обеспечения безопасности персональных данных, а также об их правах и обязанностях в этой области;**
- **актуальность сведений, указанных в Уведомлении об обработке персональных данных ГБПОУ (при необходимости - отправка нового Уведомления в Роскомнадзор).**

9.4. Повседневный контроль выполнения организационных мероприятий, направленных на обеспечение защиты информации, проводится руководителями структурных подразделений ГБПОУ.

9.5. Периодический контроль за эффективностью СЗИ осуществляет ответственный и представители отдела мобилизационной подготовки и защиты информации Министерства образования Московской области на основании приказа Министерства образования Московской области от 14.04.2009 № 857.

9.6. Плановые (п. 21 Административного регламента проведения проверок Роскомнадзором при осуществлении контроля (надзора) за соответствием обработки персональных данных требованиям законодательства в области персональных данных) и внеплановые (п. 27 Административного регламента) проверки за соответствием обработки персональных данных требованиям законодательства могут осуществляться

Управлением Роскомнадзора по Центральному федеральному округу (территориальный орган Федеральной службы по надзору в сфере связи и массовых коммуникаций).

9.7. ФСТЭК России проводит проверки технической стороны построения системы защиты информации (актуальность угроз, наличие сертификата соответствия на средства защиты, достаточность применяемых мер).

9.8. Допуск представителей этих органов для проведения контроля осуществляется в установленном порядке по предъявлению служебных удостоверений и предписаний на право проверки, подписанных руководителем (заместителем) соответствующего органа.

9.9. Ответственный **обязан присутствовать при всех проверках по вопросам защиты информации.**

9.10. Результаты проверок отражаются в Актах проверок.

9.11. По результатам проверок контролирующими органами ответственный **с привлечением заинтересованных должностных лиц в десятидневный срок разрабатывает план устранения выявленных недостатков.**

9.12. Защита информации считается эффективной, если принимаемые меры соответствуют установленным требованиям и нормам.

Несоответствие мер установленным требованиям или нормам по защите информации является нарушением.

9.13. При обнаружении нарушений руководитель ГБПОУ принимает необходимые меры по их устранению в сроки, согласованные с органом или должностным лицом, проводившим проверку.

10. ОТВЕТСТВЕННОСТЬ

Ответственность за нарушение норм, регулирующих обработку и защиту персональных данных

– Лица, виновные в нарушении норм, регулирующих обработку информации, несут дисциплинарную, административную, гражданскую, уголовную и иную предусмотренную законодательством Российской Федерации ответственность.

– Прекращение доступа к персональным данным и/или увольнение не освобождает работника ГБПОУ от принятых обязательств по неразглашению ПДн, ставших доступными при выполнении должностных обязанностей.

– К административной ответственности за нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах и за нарушение правил защиты информации могут привлекаться как ГБПОУ и его должностные лица, так и конкретные работники, исполняющие соответствующие трудовые функции.

Описание видов ответственности

– Виды дисциплинарных взысканий, порядок их применения и снятия установлены главой 30 Федерального закона Российской Федерации от 30.12. 2001 г. № 197-ФЗ «Трудовой кодекс Российской Федерации» и Правилами внутреннего трудового распорядка ГБПОУ.

– Лица, виновные в нарушении правил работы с информацией, могут привлекаться к административной ответственности по следующим основаниям:

- **нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных) (ст. 13.11 КоАП);**

- **нарушение правил защиты информации (ст. 13.12 КоАП);**

- **разглашение информации, доступ к которой ограничен федеральным законом (за исключением случаев, когда ее разглашение влечет уголовную ответственность), лицом, получившим к ней доступ в связи с исполнением служебных или профессиональных обязанностей (ст. 13.14 КоАП РФ).**

– Уголовная ответственность за нарушение правил работы с ПДн может наступить в следующих случаях:

- **незаконное собирание или распространение сведений о частной жизни лица, составляющих его личную или семейную тайну, без его согласия либо распространение этих сведений в публичном выступлении, публично демонстрируемом произведении или средствах массовой информации, если эти деяния совершены из корыстной или иной личной заинтересованности и причинили вред правам и законным интересам граждан (ст. 137 УК РФ);**

- **неправомерный отказ должностного лица в предоставлении собранных в установленном порядке документов и материалов, непосредственно затрагивающих права и свободы гражданина, либо предоставление гражданину неполной или заведомо ложной информации, если эти деяния причинили вред правам и законным интересам граждан (ст. 140 УК РФ);**

- **неправомерный доступ к охраняемой законом компьютерной информации, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование компьютерной информации (ст. 272 УК РФ);**

- **создание, распространение или использование компьютерных программ либо иной компьютерной информации, заведомо предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации (ст. 273 УК РФ);**

- **нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации либо информационно-телекоммуникационных сетей и оконечного оборудования, а также правил доступа к информационно-телекоммуникационным сетям, повлекшее уничтожение, блокирование, модификацию либо копирование компьютерной информации, причинившее крупный ущерб или повлекшее тяжкие последствия (ст. 274 УК РФ).**

Заместитель директора по безопасности _____

Приложение № 4

Приложение № 8

к приказу от _____ 201 г. № ___

ИНСТРУКЦИЯ
ответственного по защите информации ограниченного доступа

1. Общие положения.

1.1. Настоящая Инструкция определяет основные функции, права и обязанности ответственного по защите информации ограниченного доступа (далее – ответственный) при её обработке в информационных системах персональных данных (далее - ИСПДн) в *наименование ГОУ* (далее - ГБПОУ).

1.2. Ответственный по защите назначается из числа сотрудников ГБПОУ и обеспечивает правильность использования и нормальное функционирование установленной системы защиты информации (далее - СЗИ) в ИСПДн.

1.3. Настоящая Инструкция является дополнением к действующим нормативным документам по вопросам обеспечения защиты сведений ограниченного доступа и не исключает обязательного выполнения их требований.

1.4. В соответствии с моделями угроз безопасности, разработанными для ИСПДн ГОУ, актуальными являются только угрозы несанкционированного доступа (далее – НСД).

1.5. СЗИ ИСПДн построена на базе:

- встроенных в лицензионную операционную систему «Windows XP / 7 Pro» (далее - ОС) механизмов защиты от НСД;
- межсетевого экрана …..
- средств антивирусной защиты;
- организационных мер.

2. Основные функции ответственного

2.1. Контроль за выполнением требований действующих нормативных документов по вопросам обеспечения защиты сведений конфиденциального характера при проведении работ на автоматизированных рабочих местах (далее - АРМ), входящих в состав ИСПДн.

2.2. Проведение инструктажа пользователей АРМ (доведение под роспись требований инструкции «По работе пользователей информационной системы».

2.3. Контроль за соответствием состава ИС техническому паспорту (в т.ч. реальной конфигурации информационных связей).

2.4. Контроль работы СЗИ и за выполнением комплекса организационных мероприятий по обеспечению безопасности информации.

2.5. Контроль над действиями администратора ИСПДн по обеспечению функционирования СЗИ (настройка и сопровождение подсистемы управления доступом пользователя к защищаемым информационным ресурсам ИСПДн, антивирусная защита, резервное копирование данных и т.д.)

2.6. Контроль порядка учета, хранения и обращения с машинными носителями информации.

2.7. Определение порядка и осуществление контроля ремонта АРМ. При проведении технического обслуживания и ремонта средств вычислительной техники запрещается передавать ремонтным организациям узлы и блоки с элементами накопления и хранения конфиденциальной информации.

2.8. Присутствовать (участвовать) в работах по внесению изменений в аппаратно-программную конфигурацию ИСПДн.

2.9. Принятие мер по оперативному изменению паролей при увольнении или перемещении сотрудников, имевших допуск к АРМ ИСПДн.

2.10. Незамедлительное информирование руководителя учреждения об имеющихся недостатках и выявленных нарушениях СЗИ, а также в случае выявления попыток НСД к охраняемым сведениям или попыток их хищения, копирования или изменения.

3. Контролируемые параметры при проверке СЗИ ИСПДн

3.1. Наличие лицензионного программного обеспечения (операционная система, антивирусная программа и офисный пакет) на АРМ ИСПДн.

3.2. Соблюдение следующих требований к личным паролям доступа пользователей к АРМ (выбираются администратором ИСПДн):

- длина пароля должна быть не менее 8-ми буквенно-цифровых символов;
- пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, дни рождения и другие памятные даты, номера телефонов, автомобилей, адреса места жительства, наименования АС, общепринятые сокращения (ЭВМ, ЛВС, USER, SYSOP, GUEST, злоумышленником путем анализа информации о пользователе АРМ;
- не использовать в качестве пароля один и тот же повторяющийся символ либо повторяющуюся комбинацию из нескольких символов;
- не использовать в качестве пароля комбинацию символов, набираемых в закономерном порядке на клавиатуре (например, 1234567 и т.п.);
- при смене пароля новое значение должно отличаться от предыдущего не менее чем в 4 позициях;

- в числе символов пароля, обязательно должны присутствовать буквы в верхнем и нижнем регистрах, а также цифры;

- не использовать ранее использованные пароли.

3.3. Наличие на компьютере у пользователя прав не выше «пользователь» во избежание несанкционированной установки программного обеспечения (далее - ПО).

3.4. Отсутствие на компьютере лишних учетных записей пользователей компьютера, кроме записей «Администратор», «Пользователь» (встроенная учетная запись «Гость» должна быть отключена).

3.5. Наличие пароля на вход в BIOS материнской платы компьютера с целью невозможности изменения настроек.

3.6. Наличие периодического обновления вирусной базы антивирусного ПО.

3.7. Наличие бесперебойного источника питания для штатного завершения процесса обработки информации на компьютере в случае отключения электропитания.

3.8. Отсутствие со стороны пользователя АРМ следующих нарушений:

- записи паролей в очевидных местах, внутренности ящика стола, на мониторе компьютера, на обратной стороне клавиатуры и т.д.;
- хранения паролей в записанном виде на отдельных листах бумаги;
- сообщения посторонним лицам своих паролей, а также сведений о применяемой системе защиты ИСПДн от НСД.

С инструкцией ознакомлен:

Приложение № 5

Приложение № 1

к приказу от _____ 201 № ____

ПЕРЕЧЕНЬ

процессов и сведений ограниченного доступа, обрабатываемых в ГБПОУ МО _____ (далее – Организация)

№ п/п	Категория субъектов персональных данных (Тип информации)	Содержание сведений	Правовое основание для обработки	Подразделения (должность работника), использующие в работе сведения ограниченного доступа
1	**Наименование процесса:** кадровый учет **Цели обработки персональных данных:** выполнение требований Трудового кодекса РФ и других нормативных актов РФ **Способ обработки:** смешанный, часть сведений обрабатываются в ИСПДн *«Канцелярия»*			
1.1.	Работники Организации	Информация, необходимая работодателю в связи с трудовыми отношениями и касающаяся конкретного работника (*Конкретный перечень берётся из согласия работника на обработку ПДн)*	Трудовой кодекс РФ от 30.12.2001 № 197-ФЗ	*Канцелярия / отдел кадров / Администрация / Медпункт*
1.2.	Родственники работников Организации			
1.3.	Уволенные работники Организации			
2.	**Наименование процесса:** образовательная деятельность **Цели обработки персональных данных:** организация учебного процесса и контроль качества образования; учет и анализ успеваемости учащихся, оказание государственных услуг гражданам **Способ обработки:** смешанный, часть сведений обрабатываются в *ИСПДн «Учебная часть»*			
2.1.	Обучающиеся	Персональные данные об учащихся, в том числе сведения о состоянии здоровья (*Конкретный перечень берётся из согласия обучающегося на обработку ПДн)*	Федеральный закон РФ от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации»	*Учебная часть / Администрация / Медпункт /мастера / преподаватели / Библиотека*
2.2.	Поступающие (на которых подано заявление о приеме на обучение	Фамилия, имя, отчество Год рождения Адрес Медицинская справка Реквизиты документа, удостоверяющие его личность Аттестат о неполном среднем образовании	Приказ Министерства образования и науки РФ от 23.01.2014г. № 36 «Об утверждении порядка приёма на обучение по образовательным программам среднего профессионального образования»	*Приёмная комиссия*
2.3.	Родители (законные	Сведения из личной карты обучающегося:	*заполнить!*	

№ п/п	Категория субъектов персональных данных (Тип информации)	Содержание сведений	Правовое основание для обработки	Подразделения (должность работника), использующие в работе сведения ограниченного доступа
	представители) обучающихся	Степень родства Фамилия, имя, отчество Год рождения Адрес Должность и место работы Сведения об образовании Сведения о наличии льгот Сведения о количестве членов семьи Контактные данные <u>Сведения из сводных ведомостей успеваемости:</u> Степень родства Фамилия, имя, отчество Должность и место работы Контактные данные		
2.4.	Ранее обучавшиеся	Персональные данные об учащихся, в том числе сведения о состоянии здоровья.	Перечень типовых управленческих документов, образующихся в деятельности организаций, с указанием сроком хранения, утверждённый Росархивом от 06.10.2000.	
3.	**Наименование процесса:** бухгалтерский учет, начисление зарплат и стипендий **Цели обработки персональных данных:** выполнение обязательств, предусмотренных Трудовым договором **Способ обработки:** смешанный, часть сведений обрабатывается в ИСПДн «Бухгалтерия»			
3.1.	Работники Организации	Фамилия, имя, отчество Должность ИНН СНИЛС Сведения об отпусках Сведения о социальных льготах работника Сведения о доходах Лицевой счёт *(при условии перечисления на банковскую карточку)*	• Федеральный закон РФ от 06.12.2011 № 402-ФЗ «О бухгалтерском учете»; • Налоговый кодекс РФ от 31.07.1998 № 146-ФЗ; • Федеральный закон РФ от 15.12.2001 № 167-ФЗ «Об обязательном пенсионном страховании в РФ»; • Федеральный закон РФ от 24.07.2009 № 212-ФЗ «О страховых взносах в Пенсионный фонд РФ, Фонд социального страхования РФ, Федеральный фонд обязательного медицинского страхования и территориальные фонды обязательного медицинского страхования»; • Постановление Правительства Московской области от 27.12.2013 № 1186/58 «Об оплате труда работников государственных образовательных организаций Московской области»	*Отдел бухгалтерии*
3.2.	Обучающиеся	Фамилия, имя, отчество Лицевой счёт *(при условии перечисления на банковскую карточку)*	Постановление Правительства Московской области от 01.09.2014 № 693/34 «Об установлении нормативов для формирования стипендиального фонда за счёт бюджетных ассигнований бюджета Московской области и о стипендиальном обеспечении в государственных образовательных организациях Московской области и государственных научных организациях Московской области»	
3.3.	Коммерческая тайна	Сведения, содержащиеся в регистрах бухгалтерского учета, внутренней бух-	• Федеральный закон РФ от 06.12.2011 № 402-ФЗ «О бухгалтерском учете»;	

№ п/п	Категория субъектов персональных данных (Тип информации)	Содержание сведений	Правовое основание для обработки	Подразделения (должность работника), использующие в работе сведения ограниченного доступа
		галтерской отчетности организаций	• Федеральный закон РФ от 29.07.2004 № 98-ФЗ «О коммерческой тайне»	
4	**Наименование процесса:** воинский учет и бронирование **Цели обработки персональных данных:** выполнение требований нормативных актов РФ **Способ обработки:** смешанный, часть сведений обрабатываются в *ИСПДн или на компьютере с использованием машинного носителя информации, учтенного надлежащим образом.*			
4.1.	Работники Организации пребывающие в запасе	Фамилия, имя, отчество Категория запаса Воинское звание Категория годности к военной службе	• Федеральный закон РФ от 26.02.1997 № 31-ФЗ «О мобилизационной подготовки и мобилизации в Российской Федерации»; • Постановление Правительства РФ от 27.11.2006 № 719 «Об утверждении Положения о воинском учете»; • Распоряжение Межведомственной комиссии по вопросам бронирования граждан, пребывающих в запасе, от 03.12.2003 «О Выписке из Инструкции по бронированию на период мобилизации и на военное время граждан Российской Федерации, пребывающих в запасе Вооруженных Сил Российской Федерации, федеральных органов исполнительной власти, имеющих запас, и работающих в органах государственной власти, органах местного самоуправления и организациях» (п. 103)	*Канцелярия / отдел кадров*
4.2.	Обучающиеся (призывники)	Фамилия, имя, отчество Категория годности к военной службе		
5.	**Наименование процесса:** Контроль управления доступом и пребывания в Организации. **Способ обработки:** *автоматизированный.*			
5.1.	Работники Организации и обучающиеся	Фотографические изображения Фамилия, имя, отчество Должность / группа	*заполнить!*	*Охрана, Администрация Организации*
6.	**Наименование процесса:** обеспечение антитеррористической защищённости, организация и ведение гражданской обороны **Способ обработки:** смешанный, часть сведений обрабатываются с использованием машинных носителей информации, учтённых определённым образом			
6.1.	Для служебного пользования	Паспорт антитеррористической защищённости учреждения	Федеральный закон РФ от 06.03.06 г. «О противодействии терроризму»	Администрация Организации
6.2.		План гражданской обороны	Федеральный закон РФ от 12.02.1998 № 28-ФЗ «О гражданской обороне»	
7.	**Наименование процесса:** обеспечение информационной безопасности организации **Способ обработки:** неавтоматизированный			
7.1.	Для служебного пользования	Журнал учёта машинных носителей информации	Статья 19. п. 2. п.п. 5 Федерального закона РФ от 27.07.2006 № 152-ФЗ «О персональных данных»	*Ответственный за защиту информации*
7.2.		Журнал учёта паролей пользователей ИСПДн	Статья 19. п. 2. п.п. 8 Федерального закона РФ от 27.07.2006 № 152-ФЗ «О персональных данных»	*Администратор ИСПДн*

Заместитель директора по безопасности ГБПОУ МО

Способы обработки *бывают неавтоматизированный / автоматизированный/ смешанный/ пору-*

чение на обработку

Приложение № 6

Приложение № 5

к приказу от _____ 201 № _____

–

–

– Протокол

– оценки вреда, который может быть причинен субъектам, при обработке их персональных данных в ГБПОУ МО _____

–

– Настоящий Протокол составлен комиссией, назначенной приказом от «___» _____ 2015 г. № _____, с целью оценки вреда, который может быть причинен субъектам, при обработке их персональных данных в случае нарушения требований законодательства в области персональных данных в ГБПОУ МО __.

При проведении оценки вреда комиссия оперировала следующими вербальными градациями этого показателя:

23. Вред отсутствует **– если нарушение требований законодательства в области персональных данных не повлечет негативных последствий для субъекта персональных данных;**

24. Низкий уровень вреда **– если нарушение требований законодательства в области персональных данных может привести к незначительным негативным последствиям для субъекта персональных данных;**

25. Средний уровень вреда **– если нарушение требований законодательства в области персональных данных может привести к негативным последствиям для субъекта персональных данных;**

26. Высокий уровень вреда **– если нарушение требований законодательства в области персональных данных может привести к значительным негативным последствиям для субъекта персональных данных.**

–

– Результаты оценки вреда представлены в табл. 1:

– Таблица 1.

п/п	**Категория субъектов персональных данных**	**Нарушаемое свойство безопасности**	**Уровень возможного вреда для субъекта персональных данных**
1.	**Наименование процесса:** кадровый и бухгалтерский учет		
1.1.	Работники Организации	Конфиденциальность Целостность Доступность	Низкий уровень вреда
1.2.	Родственники работников Организации		
1.3.	Уволенные работники Организации		

п/п	Категория субъектов персональных данных	Нарушаемое свойство безопасности	Уровень возможного вреда для субъекта персональных данных
2.	**Наименование процесса:** образовательная деятельность		
2.1.	Поступающие (на которых подано заявление о приеме на обучение)	Конфиденциальность Целостность Доступность	Низкий уровень вреда
2.2.	Обучающиеся		
2.3	Родители (законные представители) обучающихся		
2.4	Ранее обучавшиеся	Конфиденциальность	Низкий уровень вреда
		Целостность	Низкий уровень вреда
		Доступность	Вред отсутствует
3	**Наименование процесса:** бухгалтерский учет, начисление зарплат и стипендий		
3.1.	Работники Организации	Конфиденциальность Целостность Доступность	Низкий уровень вреда
3.2.	Обучающиеся		

– Председатель комиссии: – _____ / /

–

– Члены комиссии: – _____ / /

– –

Приложение № 7

Приложение № 2
к приказу от _____ 201 г.
№ ____

СПИСОК

сотрудников ГБПОУ МО _____, допущенных в соответствии с их должностными обязанностями к обработке информации ограниченного доступа

п/п	Наименование процесса обработки информации ограниченного доступа	Должность	ФИО
1.	Кадровый учет	Директор	
		Секретарь	
		Инспектор отдела кадров	
		Библиотекарь	
2.	Образовательная деятельность	Директор	
		Секретарь	
		Заместитель директора по УВР	
		Заместители директора по …	
		Медицинский работник	
		Библиотекарь	
		Педагогические работники:	
		Мастера:	
3.	Бухгалтерский учет, начисление зарплат и стипендий	Директор	
		Главный бухгалтер	
4.	Воинский учет и бронирование		
5.	Обеспечение антитеррористической защищённости, организация и ведение гражданской обороны	Директор	
		Заместитель директора по безопасности	
		Начальник штаба ГО	
6.	Обеспечение информационной безопасности организации	Ответственный за защиту информации	
		Администратор ИСПДн	

Заместитель директора по безопасности ГБПОУ МО

Приложение № 8

Приложение № 7
к приказу от _____201 г. № ___

ПОЛИТИКА

ГОСУДАРСТВЕНОЙ БЮДЖЕТНОЙ (АВТОНОМНОЙ) ПРОФЕССИОНАЛЬНОЙ

ОБРАЗОВАТЕЛЬНОГО УЧРЕЖДЕНИЯ

МОСКОВСКОЙ ОБЛАСТИ

В ОТНОШЕНИИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

1. Термины и определения

Термин/Сокращение	Определение
Автоматизированная обработка персональных данных	Обработка персональных данных с помощью средств вычислительной техники
Блокирование персональных данных	Временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных)
ГБПОУ МО	Государственное бюджетное профессиональное образовательное учреждение Московской области
Доступ к персональным данным	Возможность получения персональных данных и их использования
Информационная система персональных данных	Совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств
Закон	Федеральный закон Российской Федерации от 27.07.2006 г. № 152-ФЗ «О персональных данных»
Конфиденциальность персональных данных	Обязательное для выполнения Операторам и иными лицами, получившим доступ к персональным данным, требование не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом
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	Государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки пер-

Термин/Сокращение	Определение
	сональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными
Персональные данные	Любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных)
Предоставление персональных данных	действия, направленные на получение персональных данных определенным кругом лиц или передачу персональных данных определенному кругу лиц
Распространение персональных данных	действия, направленные на раскрытие персональных данных неопределенному кругу лиц
Уничтожение персональных данных	Действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных
Трансграничная передача персональных данных	Передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу
Целостность информации	Состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими на него право

2. Назначение и область применения

– Настоящая Политика в отношении обработки персональных данных (далее – Политика) разработана в соответствии с требованиями Закона и определяет принципы обработки и обеспечения безопасности персональных данных в ГБПОУ МО ___ (далее – Оператор).

– Действие настоящей Политики распространяется на все процессы обработки персональных данных Оператора, как с использованием средств автоматизации, так и без использования таких средств, на всех работников и обучающихся Оператора, участвующих в таких процессах, а также на информационные системы Оператора, используемые в процессах обработки персональных данных.

Является общедоступным документом, декларирующим концептуальные основы деятельности Оператора при обработке и защите персональных данных.

– Оператор до начала обработки персональных осуществил уведомление Управления Роскомнадзора по ЦФО о своем намерении осуществлять обработку персональных данных. Оператор добросовестно и в соответ-

ствующий срок осуществляет актуализацию сведений, указанных в уведомлении.

–

3. Принципы обработки персональных данных

– Обработка персональных данных осуществляется Оператором на законной и справедливой основе и ограничивается достижением конкретных, заранее определенных и законных целей. Оператором не допускается обработка персональных данных, несовместимая с целями сбора персональных данных и объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой.

– Обработке подлежат только персональные данные, которые отвечают целям их обработки. Содержание и объем обрабатываемых Оператором персональных данных соответствуют заявленным целям обработки, избыточность обрабатываемых данных не допускается.

– При обработке персональных данных Оператором обеспечивается точность персональных данных, их достаточность и в необходимых случаях актуальность по отношению к целям обработки персональных данных. Оператором принимаются необходимые меры (обеспечивается их принятие) по удалению или уточнению неполных или неточных персональных данных.

– Хранение персональных данных Оператором осуществляется в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных. Об

–

– рабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

–

4. Условия обработки персональных данных

– Обработка персональных данных осуществляется в соответствии с целями, заранее определенными и заявленными при сборе персональных данных, а также полномочиями Оператора, определенными действующим законодательством Российской Федерации и договорными отношениями с Оператором.

– Получение и обработка персональных данных в случаях, предусмотренных Законом, осуществляется Оператором с письменного согласия субъекта персональных данных. Равнозначным содержащему собственноручную подпись субъекта персональных данных согласию в письменной

форме на бумажном носителе признается согласие в форме электронного документа, подписанного электронной подписью.

– Согласие на обработку персональных данных может быть дано субъектом персональных данных или его представителем в любой позволяющей подтвердить факт его получения форме, если иное не установлено Законом. В случае получения согласия на обработку персональных данных от представителя субъекта персональных данных полномочия данного представителя проверяются Оператором.

– Оператор вправе обрабатывать персональные данные без согласия субъекта персональных данных (или при отзыве субъектом персональных данных согласия на обработку персональных данных) при наличии оснований, указанных в Законе.

– Обработка специальных категорий персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, интимной жизни, Оператором не осуществляется.

– Сведения, которые характеризуют физиологические особенности человека и на основе которых можно установить его личность (биометрические персональные данные) и сведения о состоянии здоровья, могут обрабатываться только при наличии согласия в письменной форме субъекта персональных данных или иных оснований, предусмотренных федеральным законодательством.

– Персональные данные субъекта могут быть получены Оператором от лица, не являющегося субъектом персональных данных, при условии предоставления Оператору подтверждения наличия оснований, указанных в Законе или иных оснований, предусмотренных федеральным законодательством.

–

–

– Право доступа к персональным данным субъектов персональных данных на бумажных и электронных носителях имеют работники Оператора в соответствии с их должностными обязанностями.

– Оператором не осуществляется трансграничная передача персональных данных и не принимаются решения, основанные исключительно на автоматизированной обработке персональных данных субъекта.

5. Цели обработки персональных данных

– В соответствии с принципами и условиями обработки персональных данных, Оператором определены цели обработки персональных данных:

27. обработка персональных данных сотрудников и сведений об их профессиональной служебной деятельности в целях ведения кадрового учёта;

28. обработка персональных данных обучающихся, необходимых для оказания им услуг в области образования;

29. начисление денежного содержания сотрудникам и стипендий обучающимся, выплаты страховых взносов в Пенсионный фонд и Фонд социального страхования Российской Федерации, Федеральный фонд обязательного медицинского страхования.

30. организация выездных экскурсий для обучающихся.

6. Особенности обработки персональных данных и их передачи третьим лицам

– Обработка персональных данных Оператором осуществляется как с использованием средств автоматизации, так и без использования таких средств.

Обработка персональных данных Оператором включает в себя: сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (предоставление, доступ), обезличивание, блокирование, уничтожение.

– Передача персональных данных субъектов персональных данных третьим лицам осуществляется Оператором в соответствии с требованиями действующего законодательства.

– Оператор вправе поручить обработку персональных данных третьей стороне с согласия субъекта персональных данных и в иных случаях, предусмотренных действующим законодательством Российской Федерации, на основании заключаемого с этой стороной договора, (далее – поручение). Третья сторона, осуществляющая обработку персональных данных по поручению Оператора, обязана соблюдать принципы и правила обработки персональных данных, предусмотренные Законом, обеспечивая конфиденциальность и безопасность персональных данных при их обработке.

7. Права субъектов персональных данных

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

31. подтверждение факта обработки персональных данных Оператором;

32. правовые основания и цели обработки персональных данных;

33. цели и применяемые Оператором способы обработки персональных данных;

34. наименование и место нахождения Оператора, сведения о лицах (за исключением работников Оператора), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с Оператором или на основании федерального закона;

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

36. сроки обработки персональных данных, в том числе сроки их хранения;

37. порядок осуществления субъектом персональных данных прав, предусмотренных Законом;

38. информацию об осуществленной или о предполагаемой трансграничной передаче данных;

39. наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению Оператора, если обработка поручена или будет поручена такому лицу;

40. иные сведения, предусмотренные Законом или другими федеральными законами.

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.

Право субъекта персональных данных на доступ к его персональным данным может быть ограничено в соответствии с федеральными законами, в том числе, если доступ субъекта персональных данных к его персональным данным нарушает права и законные интересы третьих лиц.

Для реализации и защиты своих прав и законных интересов субъект персональных данных имеет право обратиться к Оператору. Оператор рассматривает любые обращения и жалобы со стороны субъектов персональных данных, тщательно расследует факты нарушений и принимает все необходимые меры для их немедленного устранения, наказания виновных лиц и урегулирования спорных и конфликтных ситуаций в досудебном порядке.

Субъект персональных данных вправе обжаловать действия или бездействие

Оператора путем обращения в уполномоченный орган по защите прав субъектов персональных данных.

Субъект персональных данных имеет право на защиту своих прав и законных интересов, в том числе на возмещение убытков и/или компенсацию морального вреда в судебном порядке.

8. Реализованные меры обеспечения безопасности персональных данных

– Оператор при обработке персональных данных принимает необходимые правовые, организационные и технические меры или обеспечивает их принятие для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

– К таким мерам, в частности, относятся:

41. назначение лица, ответственного за организацию обработки персональных данных;

42. осуществление внутреннего контроля за соблюдением законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных;

43. ознакомление работников Оператора с положениями законодательства Российской Федерации о персональных данных, локальными актами по вопросам обработки персональных данных, требованиями к защите персональных данных;

44. издание локальных актов по вопросам обработки персональных данных и локальных актов, устанавливающих процедуры, направленные на предотвращение и выявления нарушений законодательства Российской Федерации;

45. определение угроз безопасности персональных данных и необходимого уровня защищённости персональных данных, при их обработке в информационных системах персональных данных;

46. применение организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных;

47. использование средств защиты информации, прошедших в установленном порядке процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации;

48. осуществление оценки эффективности применяемых мер по обеспечению безопасности персональных данных.

9. Доступ к Политике

Действующая редакция Политики на бумажном носителе хранится в месте

нахождения исполнительного органа Оператора по адресу: [*адрес Оператора*].

Электронная версия действующей редакции Политики общедоступна на сайте Оператора в сети «Интернет»: [*адрес веб-сайта Оператора*].

10. Актуализация и утверждение Политики

Политика утверждается и вводится в действие распорядительным документом, подписываемым руководителем Оператора.

Оператор имеет право вносить изменения в настоящую Политику. При внесении изменений в заголовке Политики указывается дата утверждения действующей редакции Политики.

11. Ответственность

Лица, виновные в нарушении норм, регулирующих обработку и защиту персональных данных, несут ответственность, предусмотренную законодательством Российской Федерации, локальными актами Оператора и договорами, регламентирующими правоотношения Оператора с третьими лицами.

Ответственный за организацию обработки персональных данных _____ /

Приложение № 9

Приложение № 3
к приказу от _____ 201 г.
№ ____

Перечень и состав информационных систем персональных данных

в ГБПОУ МО _____

№	Наименование	Помещение	Инвентарный номер компью-тера
Наименование процесса: *бухгалтерский учет, начисление зарплат и стипендий*			
1	**ИСПДн № 1** («Бухгалтерия») в составе:		
	АРМ № 1	13А	004551100
	АРМ № 2	13	……
	АРМ № 3	12	……
	……..		
Наименование процесса: *кадровый учет*			
2	**ИСПДн № 2** («Кадры») в составе:		
	АРМ № 1	24	…….
Наименование процесса: *образовательная деятельность*			
3	**ИСПДн № 3** («Учебная часть) в составе:		
	АРМ № 1	4	……
4	**ИСПДн № 4** («Социальный педагог») в составе:		
	АРМ № 1	32	

Ответственный за защиту
информации ограниченного доступа

Приложение № 10

Приложение № 11

к приказу от _____ 201 г. № _____

На каждую ИСПДн свой паспорт !!!!

ТЕХНИЧЕСКИЙ ПАСПОРТ

на информационную систему персональных данных «Бухгалтерия» («Кадровый учёт» / «Учебная часть»)

РАЗРАБОТАЛ

Ответственный за защиту информации

_____ М. В. Смтттттт

«___» _____201 г.

201 г.

1. Общие сведения об информационной системе персональных данных

1.1. Наименование:

Информационная система персональных данных …… (далее – ИСПДн)

1.2. Расположение ИСПДн:

Административное здание по адресу: ……., ул. , дом, помещения №№ ……

1.3. Назначение:

ИСПДн создана с целью автоматизации системы *(выбрать !!!!)*:

- *обработки персональных данных сотрудников и сведений об их профессиональной служебной деятельности в целях ведения кадрового учёта;*
- *обработки персональных данных обучающихся, необходимых для оказания им услуг в области образования;*
- *начисления денежного содержания сотрудникам и стипендий обучающимся, выплаты страховых взносов в Пенсионный фонд и Фонд социального страхования Российской Федерации, Федеральный фонд обязательного медицинского страхования.*

1.4. Структура: ИСПДн представляет собой *(выбрать !!!!) одноранговую локальную вычислительную сеть / локальную вычислительную сеть с выделенным сервером / автоматизированное рабочее место.*

1.5. Тип ИСПДн: обрабатываются иные категории персональных данных.

2. Состав оборудования ИСПДн

2.1. Перечень основных технических средств, входящих в состав ИСПДн

Таблица 1

№ п/п	Тип ОТСС	Наименование	Заводской (инв.) номер
АРМ № 1			
1	Системный блок	б/н	0045472
2	Монитор	Belinea 1730S1	AA1117590734AC18401685
3	Клавиатура	KraftWay KB-9801	ZCE739702242
4	Манипулятор «мышь»	KraftWay MSO 0502	0709001274

5	ИБП	IPPON	0045466
6	Принтер	HP LJ 3050	CNCKN95454
АРМ № 2			
1	Системный блок	б/н	004541111
2	Монитор	Belinea 1730S1	AA1117590734AC18401685

и так далее !!!!

2.2. Перечень средств защиты информации, установленных в ИСПДн (*пример !!1*)

Таблица 2

№ п/п	Наименование и тип технического средства	Сведения о сертификате
1	Операционная система «Windows 7 Pro»	сертификат ФСТЭК России № 1883 от 11.08.2009
2	Межсетевой экран «Программный комплекс UserGate Proxy & Firewall 5.2.F»	сертификат ФСТЭК России № 2076/1 от 16.05.2011
3	Средство антивирусной защиты Антивирус Каспер-ского 6.0 для Windows Woorkstations	сертификат ФСТЭК России № 1384 от 11.05.2007

2.3. Перечень используемых в ИСПДн программных средств

Таблица 3

№ п/п	Наименование и тип программного средства	Серийный номер (номер лицензии)
АРМ № 1		
1	Операционная система:	
	Windows XP Pro SP2	73211-OEM-0012524-19893
2	Прикладное ПО:	
	Microsoft Office 2003	72217-643-9329615-57075
	Клиентская часть программы 1С:Бухгалтерия 8.0	*Вводится регистрационный номер из лицензионного со-глашения на программный продукт.*
	Abode Reader 9.2	б/н
	Архиватор WinRAR (WinZip)	

3	Антивирус AVP Kaspersky	019E-000451-0358A73C

АРМ № 2		
1	Операционная система:	
	Windows XP Pro SP2	73211-OEM-0012524-19899
2	Прикладное ПО:	
	Microsoft Office 2003	72217-643-9329615-57011
	Серверная часть программы 1С:Бухгалтерия 8.0	*Вводится регистрационный номер из лицензионного соглашения на программный продукт.*
	Abode Reader 9.2	б/н
	Архиватор WinRAR (WinZip)	
3	Антивирус AVP Kaspersky	019E-000451-0358A73C

и так далее !!!!

Приложение № 4
к приказу от _____ 201 г.
№ ____

СПИСОК

пользователей информационных систем персональных данных
в ГБПОУ МО **_____**

№	ФИО	Должность	Объект вычислительной техники
ИСПДн № 1 («**Бухгалтерия**»)			
1			АРМ № 1
2			АРМ № 2
3			АРМ № 3
ИСПДн № 2 («**Канцелярия» / «Кадры**»)			
4	*В случае если за одним ПК работают два человека*		АРМ № 1
5			
ИСПДн № 3 («**Учебная часть**)			
6			АРМ № 1

Ответственный за защиту
информации ограниченного доступа _____

Приложение № 12

Приложение № 9
к приказу от _____ 201 г. № ___

ИНСТРУКЦИЯ

по работе пользователей в информационной системе персональных данных

1. Общие положения

Настоящая инструкция определяет общие положения работы пользователей информационной системы персональных данных (далее - ИСПДн) при обработке (наборе, редактировании и печати) информации ограниченного доступа (далее - информация) и является обязательным для выполнения всеми пользователями.

1.1. Учет работы пользователей в ИСПДн производится ответственным за защиту информации ограниченного доступа (далее - ответственным).

1.2. Допуск пользователей для работы в ИСПДн осуществляется в соответствии со «Списком пользователей информационных систем персональных данных в ГБПОУ МО _____».

1.3. К самостоятельной работе на АРМ, входящих в состав ИСПДн, допускаются лица, изучившие требования настоящей Инструкции и освоившие правила эксплуатации АРМ и технических средств защиты. Допуск производится после проверки администратором ИСПДн *(ответственным)* знания пользователем настоящей Инструкции и практических навыков в работе.

1.4. 1.4. Пользователи имеют право отрабатывать информацию в соответствии с полномочиями доступа «Пользователь» к ресурсам компьютера, присвоенными администратором ИСПДн (*ответственным*) каждому пользователю.

1.5. Работа в ИСПДн должна осуществляться на базе общесистемного лицензионного программного обеспечения.

1.6. Технические средства ИСПДн в помещении размещаются таким образом, чтобы исключить визуальный просмотр экрана видеомонитора лицами, не имеющими отношения к обрабатываемой информации.

1.7. Уборка помещения, где расположены АРМ, входящие в состав ИСПДн, проводятся только под контролем пользователя ИСПДн. При проведении этих работ обработка защищаемой информации запрещается.

1.8. Настоящая Инструкция доводится до пользователей под роспись.

2. Порядок работы пользователей на АРМ ИСПДн

2.1. Пароль на вход в АРМ пользователь получает от администратора ИСПДн *(ответственного)* с фиксацией в журнале паролей.

2.2. После включения компьютера пользователь должен ввести свои учётные данные для идентификации (логин) и аутентификации (пароль) в системе защиты ИСПДн.

2.3. Для сохранности информации пользователь обязан корректно выключать (перезагружать) свой компьютер. **Обязательно** дождаться пока компьютер не выключиться самостоятельно!

2.4. В папке «Мои документы» и на «Рабочем столе» может находиться только информация, связанная с текущей работой.

2.5. При временном отсутствии пользователя на рабочем месте компьютер должен быть выключен или заблокирован.

2.6. В целях предотвращения разрушения и утери обрабатываемой на компьютере информации пользователем должен осуществлять:

- копирование необходимой информации по мере ее обновления на учтенные в соответствующем журнале машинные носители информации (далее - МНИ);
- проверку программой «антивирусом» МНИ, поступивших из других подразделений и сторонних организаций.

2.7. Пользователь должен хранить МНИ в местах, исключающих несанкционированный доступ к ним. В конце года он должен предъявить их ответственному в ходе проводимой им ежегодной проверки.

2.8. При любом сбое АРМ, нестабильности в работе компьютера, сети и т. д. пользователь должен сообщать администратору ИСПДн *(ответственному)*.

2.9. При обнаружении компьютерного вируса пользователь обязан немедленно прекратить какие-либо действия на компьютере и поставить в известность администратора ИСПДн *(ответственного)*.

2.10.Пользователь обязан ставить в известность ответственного в случае появления сведений или подозрений о фактах несанкционированного доступа к информации.

3. Ограничения

Пользователю запрещается:

3.1. Передавать кому-либо пароль, используемый на компьютере.

3.2. Осуществлять ввод пароля в присутствии посторонних лиц

3.3. Оставлять записанные пароли в доступных для других сотрудников местах.

3.4. Оставлять без личного присмотра на рабочем месте или где бы то ни было МНИ и распечатки, содержащие защищаемую информацию.

3.5. Изменять самостоятельно конфигурацию аппаратно-программных средств компьютера, не предусмотренных техническим паспортом ИСПДн или проводить обновление установленного программного обеспечения.

3.6. Осуществлять обработку персональных данных в присутствии посторонних (не допущенных к данной информации) лиц.

3.7. Знакомить других сотрудников с такими сведениями, если это не предусмотрено их должностными обязанностями.

3.8. Оставлять бесконтрольно включенный компьютер, на столе - магнитные носители и распечатанные листы с информацией.

3.9. Записывать и хранить персональные данные на неучтенных МНИ.

3.10. Выключать (приостанавливать защиту) антивирусный сканер на компьютере.

3.11. Отключать (блокировать) программные компоненты системы защиты информации.

3.12. Использовать для обработки информации компьютер, не предназначенный для этих целей.

3.13. Использовать компоненты программного обеспечения компьютера в неслужебных целях.

4. Ответственность

Пользователь несет ответственность за ненадлежащее исполнение своих должностных обязанностей, предусмотренных настоящей инструкцией, а также организационно-распорядительными документами в области защиты информации, в пределах, определенных действующим трудовым, гражданским, административным и уголовным законодательством Российской Федерации.

Ознакомлен:

_____ / _____/
_____ / _____/
_____ / _____/

Приложение 13.

УТВЕРЖДАЮ
Директор ГБПОУ МО
…….
_____
«____» _____ 201__ г.

МОДЕЛЬ
УГРОЗ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ
ПРИ ИХ ОБРАБОТКЕ В ИНФОРМАЦИОННОЙ СИСТЕМЕ
ПЕРСОНАЛЬНЫХ ДАННЫХ
«_____»
В ГБПОУ МО ……

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Информационная система персональных данных	Совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств
Контролируемая зона	Пространство, в котором исключено неконтролируемое пребывание сотрудников и посетителей оператора и посторонних транспортных, технических и иных материальных средств
Нарушитель безопасности персональных 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
Недекларированные возможности	Функциональные возможности средств вычислительной техники, не описанные или не соответствующие описанным в документации, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации
Несанкционированный доступ (несанкционированные действия)	Доступ к информации или действия с информацией, осуществляемые с нарушением установленных прав и (или) правил доступа к информации или действий с ней с применением штатных средств информационной системы или средств, аналогичных им по своим функциональному предназначению и техническим характеристикам
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
Персональные данные	Любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных)
Побочные электромагнитные излучения и наводки	Электромагнитные излучения технических средств обработки защищаемой информации, возникающие как побочное явление и вызванные электрическими сигналами, действующими в их электрических и магнитных цепях, а также электромагнитные наводки этих сигналов на токопроводящие линии, конструкции и цепи питания

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
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
Целостность информации	Состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими на него право

СОКРАЩЕНИЯ

АРМ	Автоматизированное рабочее место
ИСПДн	Информационная система персональных данных
КЗ	Контролируемая зона
НСД	Несанкционированный доступ (несанкционированные действия)
ПДн	Персональные данные
ПО	Программное обеспечение
ПЭМИН	Побочные электромагнитные излучения и наводки
СЗИ	Средство защиты информации
УБПДн	Угрозы безопасности персональных данных
Учреждение	Государственная профессиональная образовательная организация Московской области

1. ОБЩИЕ СВЕДЕНИЯ

Современная система обеспечения безопасности при их обработке в информационных системах персональных данных государственных профессиональных образовательных организаций Московской области должна строиться на основе комплексирования разнообразных мер защиты и опираться на современные методы прогнозирования, анализа и моделирования возможных угроз безопасности информации и последствий их реализации. При этом необходимо придерживаться следующего правила: стоимость реализуемой системы защиты информации не должна превышать величину ущерба, который может быть нанесён собственнику ИСПДн.

Настоящая Модель угроз безопасности персональных данных при их обработке в информационной системе персональных данных *«Канцелярия» / «Бухгалтерия»/ «Учебная часть»* (далее – Модель угроз) определяет подход Учреждения к определению актуальных угроз и категорий нарушителей безопасности персональных данных при их обработке с использованием средств автоматизации.

Модель угроз предназначена для определения требований к системе защиты персональных данных ИСПДн.

Модель угроз разработана на основании следующих нормативно-методических документов:

– Федерального закона от 27.07.2006 года № 152-ФЗ «О персональных данных»;

– постановления Правительства Российской Федерации от 01.11.2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

– Методики определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных утвержденной заместителем директора ФСТЭК России 14.02.2008г.;

– Базовой модели угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденной заместителем директора ФСТЭК России 15.02. 2008г.

УБПДн, обрабатываемых в ИСПДн, и категории нарушителей, содержащиеся в настоящей Модели угроз, могут уточняться и дополняться по мере выявления новых источников угроз, развития способов и средств реализации угроз безопасности персональных данных в ИСПДн, изменения законодательства в области обработки и защиты персональных данных.

Внесение изменений в Модель угроз осуществляется также в случае изменения основных характеристик ИСПДн, указанных в разделе 2.

2. ОПИСАНИЕ ИСПДн

2.1. Общие сведения

ИСПДн по структуре является *(выбрать !!!!)*

Варианты !!!!

- *автономным автоматизированным рабочим местом, не подключенным к сети «Интернет» и иным информационным система;*
- *автономным автоматизированным рабочим местом, подключенным к сети «Интернет»;*
- *комплексом автоматизированных рабочих мест, объединенных в единую информационную систему средствами связи без подключения к сети «Интернет» и иным информационным системам (локальная вычислительная сеть);*
- *комплексом автоматизированных рабочих мест, объединенных в единую информационную систему средствами связи, подключенную к сети «Интернет» и иным информационным системам (локальная вычислительная сеть).*

ИСПДн по режиму обработки ПДн относятся к однопользовательским *(многопользовательским)* системам без разграничения прав доступа *(с равными правами доступа / разграничением прав доступа*) пользователей.

ИСПДн являются информационными системами, обрабатывающей не только персональные данные сотрудников образовательного учреждения, но и персональные данные учащихся.

Объем обрабатываемых персональных данных ИСПДн имеет значение менее чем 100 000 записей.

Все технические средства ИСПДн находятся в пределах Российской Федерации.

2.2. Определение степени исходной защищенности

Под уровнем исходной защищенности ИСПДн понимается обобщенный показатель, зависящий от технических и эксплуатационных характеристик ИСПДн. Технические и эксплуатационные характеристики ИСПДн, определяющие степень исходной защищённости, приведены в табл. 1.

Таблица 1.

Технические и эксплуатационные характеристики ИСПДн	**Уровень защищенности**		
	высокий	**средний**	**низкий**
1. По территориальному размещению *(выбрать!)*:			
локальная (кампусная) ИСПДн, развернутая в пределах нескольких близко расположенных зданий		+	
локальная ИСПДн, развернутая в пределах одного здания	+		

2. По наличию соединения с сетями общего пользования: *(выбрать!)*			
ИСПДн, физически отделённая от сети общего пользования	+		
ИСПДн, имеющая одноточечный выход в сеть общего пользования		+	
3. По встроенным (легальным) операциям с записями баз персональных данных:			
модификация, передача			+
4. По разграничению доступа к персональным данным:			
ИСПДн, к которой имеют доступ определенные перечнем сотрудники организации, являющейся владельцем ИСПДн, либо субъект ПДн;		+	
5. По наличию соединений с другими базами ПДн иных ИСПДн:			
ИСПДн, в которой используется одна база ПДн, принадлежащая организации – владельцу данной ИСПДн	+		
6. По уровню обобщения (обезличивания) ПДн:			
ИСПДн, в которой предоставляемые пользователю данные не являются обезличенными (т.е. присутствует информация, позволяющая идентифицировать субъекта ПДн)			+
7. По объему ПДн, которые предоставляются сторонним пользователям ИСПДн без предварительной обработки: *(выбрать!)*			
ИСПДн, предоставляющая часть ПДн		+	
ИСПДн, не предоставляющая никакой информации	+		

Для ИСПДн не менее 70% характеристик соответствуют среднему и высокому уровню защищенности, а остальные — низкому уровню защищённости. Таким образом, информационные системы имеют среднюю степень исходной защищенности (числовой показатель - $Y_1 = 5$).