УТВЕРЖДАЮ
Директор МБУ ИЦСО

_____Клехо М.А.

Приказ № 11 от 01. 02. 2016 г.

ПОЛОЖЕНИЕ

О ПОРЯДКЕ ОРГАНИЗАЦИИ И ПРОВЕДЕНИЯ РАБОТ ПО ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ В МУНИЦИПАЛЬНОМ БЮДЖЕТНОМ УЧРЕЖДЕНИИ «ИТ-ЦЕНТР СОЦИАЛЬНЫХ ОРГАНИЗАЦИЙ»

г. Мытищи
2016 г.

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящее Положение разработано на основании требований:

- Федерального закона Российской Федерации от 27.07.2006 № 152 «О персональных данных»;
- Федерального закона Российской Федерации от 27.07.2006 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- постановления Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

постановления Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении положения об обеспечении безопасности персональных данных, осуществляемой без использования средств автоматизации»

- постановления Правительства Московской области от 27.11.2002 № 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».

1.2. Цель данного Положения – определение порядка организации, и проведения работ в муниципальном бюджетном учреждение «ИТ-центр социальных организаций» (далее – МБУ ИЦСО) для построения эффективной системы защиты информации от несанкционированного доступа, и её последующей эксплуатации. В частности, с целью обеспечение защиты прав и свобод субъектов персональных данных при обработке их персональных данных в информационных системах МБУ ИЦСО, а также установление ответственности должностных лиц, имеющих доступ к персональным данным, за невыполнение требований норм, регулирующих обработку и защиту персональных данных.

1.3. Положение предназначено для практического использования должностным лицам ответственным за защиту персональных данных.

1.4. Требования настоящего Положения являются обязательными для исполнения всеми должностными лицами МБУ ИЦСО.

1.5. За общее состояние защиты персональных данных в МБУ ИЦСО отвечает его руководитель.

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

Проведения работ по защите персональных данных в информационных системах с помощью встроенных средств безопасности сертифицированных лицензионных операционных систем и антивирусного программного обеспечения возлагается на **администратора ИС.**

Контроль выполнения требований настоящего Положения возлагается на **ответственного за защиту персональных данных** в МБУ ИЦСО (далее – ответственный).

1.6. Лица, виновные в нарушение установленного законом порядка сбора, хранения, использования или распространения персональных данных о гражданах

несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с федеральным законодательством.

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

1.8. Положение может уточняться и корректироваться по мере необходимости.

2 ОСНОВНЫЕ ПОНЯТИЯ

2.1. **Персональные данные** (далее - ПДн) - любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация;

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

2.3. **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.

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.;

2.4. **Субъект** - субъект ПДн;

2.5. **Оператор** - государственный орган, муниципальный орган, юридическое или физическое лицо, организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели и содержание обработки персональных данных;

2.6. **Конфиденциальность персональных данных** - обязательное для соблюдения оператором или иным получившим доступ к ПДн лицом требование не допускать их распространения без согласия субъекта ПДн или наличия иного законного основания;

2.7. **Общедоступные персональные данные** - ПДн, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта ПДн или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности;

2.8. **Обработка персональных данных** - действия (операции) с ПДн, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных;

2.9. **Распространение персональных данных** - действия, направленные на передачу ПДн определенному кругу лиц (передача ПДн) или на ознакомление с

ПДн неограниченного круга лиц, в том числе обнародование ПДн в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к ПДн каким-либо иным способом;

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

2.11. **Блокирование персональных данных** - временное прекращение сбора, систематизации, накопления, использования, распространения ПДн, в том числе их передачи;

2.12. **Уничтожение персональных данных** - действия, в результате которых невозможно восстановить содержание ПДн в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных;

2.13. **Обезличивание персональных данных** - действия, в результате которых невозможно определить принадлежность ПДн конкретному субъекту ПДн;

3 ЦЕЛИ И ЗАДАЧИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

3.1. Правовое основание обработки ПДн МБУ ИЦСО:

Федеральные законы Российской Федерации:

- «Об образовании» от 29.12.2012 г. № 273;
- 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 г. № 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.

3.2. Цель обработки ПДн:

- обработка персональных данных сотрудников МБУ ИЦСО и сведений об их профессиональной служебной деятельности для реализации полномочий учреждения;
- обработка персональных данных сотрудников, учащихся и их законных представителей, образовательных учреждений Мытищинского муниципального района, для реализации полномочий учреждения и обеспечения наиболее полного исполнения образовательными учреждениями своих обязанностей, обязательств и компетенций, определённых Федеральным законом «Об образовании»;
- начисление денежного содержания сотрудникам МБУ ИЦСО и выплаты страховых взносов в Пенсионный фонд Российской Федерации, Фонд

социального страхования Российской Федерации, Федеральный фонд обязательного медицинского страхования;

3.3. Категория ПДн:

категория 2 (персональные данные, позволяющие идентифицировать субъекта персональных данных и получить о нем дополнительную информацию, за исключением персональных данных, относящихся к категории 1) - фамилия, имя, отчество, год, месяц, дата, место рождения, адрес, ИНН, телефон, доходы, образование, состав семьи, льготы, сведения о профессиональной служебной деятельности.

3.4. Категории субъектов ПДн, персональные данные которых обрабатываются:

- сотрудники МБУ ИЦСО;
- сотрудники, учащиеся и их законные представители образовательных учреждений Мытищинского муниципального района.

3.5. Все ПДн субъекта 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 МБУ ИЦСО 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.

3.6. МБУ ИЦСО 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.

3.7. 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.

3.8. 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.

3.9. Согласие на обработку ПДн может быть отозвано субъектом ПДн по письменному запросу на имя руководителя МБУ ИЦСО.

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

3.11. 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.

3.12. 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.

3.13. 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.

3.14. 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 МБУ ИЦСО или уполномоченного руководителем лицо.

3.15. 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 Москве и Московской области) или в судебном порядке неправомерные действия или бездействия должностных лиц МБУ ИЦСО при обработке и защите его ПДн.

4 ОХРАНЯЕМЫЕ СВЕДЕНИЯ И АКТУАЛЬНЫЕ УГРОЗЫ

4.1. Охраняемые сведения - ПДН, обрабатываемые в ИС МБУ ИЦСО, а также представленные в виде носителей на бумажной, магнитной и иной материальной основе.

4.2. Объекты защиты:

- ИС различного назначения, участвующие в обработке информации;
- помещения, где установлены ИС или хранится ПДн на материальных носителях.

2.4. Актуальные угрозы безопасности объектов защиты.

В соответствии с моделями угроз безопасности персональных данных в ИСПДн, разработанными и утверждёнными в МБУ ИЦСО, **актуальными являются только угрозы несанкционированного доступа** к информационным ресурсам ИС 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 ИС МБУ ИЦСО **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 ИС от НСД нарушителей и непреднамеренных действий пользователей;
- выводимой на экраны мониторов компьютеров;
- хранящейся на материальных носителях;
- циркулирующей в ЛВС при несанкционированном подключении к данной сети.

5 ОРГАНИЗАЦИОННЫЕ И ТЕХНИЧЕСКИЕ МЕРОПРИЯТИЯ ПО ЗАЩИТЕ ИНФОРМАЦИИ

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

5.2. Целью технической защиты ПДн в МБУ ИЦСО является предотвращение НСД к информации при её обработке в ИС, связанные с действиями нарушителей, включая пользователей ИС, реализующих угрозы непосредственно в ИС, а также нарушителей, не имеющих доступ к ИС, реализующих угрозы из сетей международного информационного обмена с целью её разрушения, искажения, уничтожения, блокировки и несанкционированного копирования.

5.3. Целями организационных мероприятий по защите ПДн в МБУ ИЦСО являются:

- исключение непреднамеренных действий пользователей ИС, приводящих к утечке, искажению, разрушению ПДн, 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 электронном или бумажном носителях);
- исключение ознакомления сотрудников с такими сведениями, если это не предусмотрено их должностными обязанностями.

5.4. Руководитель МБУ ИЦСО 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 ПДн;
- издание комплекта документов, определяющих политику в отношении обработки ПДн в МБУ ИЦСО, 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 XP / 7 Professional» (далее - ОС), обладающих встроенными средствами защиты от НСД;
- настройка ОС на компьютерах ИС в соответствии с «Руководством по безопасной настройке»;
- сертификация вышеуказанных ОС по требованиям безопасности информации;
- выбор дополнительных технических средств, сертифицированных по требованиям безопасности ПДн, для компьютеров, подключенных к сетям связи общего пользования МБУ ИЦСО и Интернет;
- использование средств антивирусной защиты;
- предотвращение организационными мерами НСД к обрабатываемым ПДн;
- организация процесса резервного копирования и архивирования как неотъемлемой части политики защиты ПДн;
- осуществление учета материальных носителей ПДн и их хранение в шкафах надежно запираемых помещений, находящихся под постоянным контролем и доступ в которые ограничен;
- строгое соблюдение сотрудниками МБУ ИЦСО «Инструкции по работе пользователей информационной системы».

5.5. Документальное оформление мероприятий по защите объекта информатизации включает:

- приказ об организации работ по защите ПДн;
- положение о порядке организации и проведения работ по защите ПДн в МБУ ИЦСО;
- список лиц, допущенных в соответствии с их должностными обязанностями к ПДн;
- технические паспорта ИС;
- 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».

6. ВВОД В ЭКСПЛУАТАЦИЮ ИНФОРМАЦИОННЫХ СИСТЕМ

6.1. Необходимым условием для ввода в эксплуатацию информационных систем МБУ ИЦСО 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

нормативно-методической документации ФСТЭК России по безопасности информации.

6.2. Руководитель МБУ ИЦСО самостоятельно принимает решение по организации работ по построению систем защиты ИСПДн или с привлечением сторонней организации, имеющей лицензию ФСТЭК России на проведения таких работ, при условии классификации ИСПДн по 3 классу.

6.3. В случае привлечения сторонней организации она проводит аттестационные испытания ИСПДн в соответствии с программой испытаний, согласованной с МБУ ИЦСО. Испытания завершаются выдачей «Аттестата соответствия ИСПДн требованиям безопасности ПДн».

6.4. В случае проведения работ по построению системы защиты ИСПДн силами самого учреждения оценка полученного результата проводится **в форме декларирования.**

6.5. Для декларирования соответствия ИС требованиям п. 5.1 комиссией, утвержденной приказом руководителя МБУ ИЦСО, подготавливаются и представляются на систему:

- технический паспорт;
- организационно-распорядительная документация разрешительной системы доступа персонала к защищаемым ресурсам;
- модель угроз безопасности персональных данных;
- сертификаты средств защиты ПДн, используемые при построении системы защиты;
- инструкция по работе пользователей;
- инструкция ответственного за защиту информации.

6.6. По результатам декларирования соответствия **ответственным** разрабатываются и доводятся до сотрудников МБУ ИЦСО под роспись «Инструкция по работе пользователей ИСПДн» и рекомендации о порядке выполнения мероприятий по защите информации.

7. ОБЯЗАННОСТИ И ПРАВА ДОЛЖНОСТНЫХ ЛИЦ

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

В частности,

1. Назначает ответственного за организацию защиты ПДн из числа сотрудников МБУ ИЦСО.

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 защиты информации, 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. **Ответственный по организации и проведению работ по защите ПДн в МБУ ИЦСО:**

- составляет Перечень сведений ограниченного доступа в МБУ ИЦСО;
- предотвращает организационными мерами НСД к обрабатываемой в ИСПДн информации;
- контролирует порядок подготовки, учета и хранения документов с ПДн;
- контролирует порядок передачи ПДн другим органам и организациям, а также между сотрудниками своей организации.
- разрабатывает организационно-распорядительные документы по вопросам защиты ПДн при её обработке с помощью ИС;
- контролирует исполнение приказов и распоряжений вышестоящих организаций по вопросам обеспечения безопасности ПДн;
- знакомит работников МБУ ИЦСО, непосредственно осуществляющих обработку ПДн, с положениями законодательства Российской Федерации о ПДн, в том числе требованиями к защите ПДн;
- обеспечивает защиту ПДн, циркулирующей на объектах информатизации, организовывает работы по декларированию (аттестации) ИС на соответствие нормативным требованиям;
- проводит систематический контроль работы средств защиты информации, 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 средств защиты информации (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 ПДн;
- присутствует (участвует) в работах по внесению изменений в аппаратно-программную конфигурацию ИСПДн;
- определяет порядок и осуществляет контроль ремонта средств вычислительной техники, входящих в состав ИСПДн;
- принимает меры по оперативному изменению паролей при увольнении или перемещении сотрудников, имевших допуск к ИСПДн;
- требует от сотрудников устранения выявленных нарушений и недостатков, давать обязательные для исполнения указания по вопросам обеспечения положений инструкций по защите ПДн;
- требует от работников представления письменных объяснений по фактам нарушения режима конфиденциальности;
- об имеющихся недостатках и выявленных нарушениях требований нормативных и руководящих документов по защите ПДн, а также в случае выявления попыток НСД к ПДн или попыток хищения, копирования, изменения незамедлительно принимает меры пресечения и докладывает руководителю МБУ ИЦСО;

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

8. КОНТРОЛЬ СОСТОЯНИЯ ЗАЩИТЫ ИНФОРМАЦИИ

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

8.2. Контроль заключается в проверке по действующим методикам выполнения требований нормативных документов по защите ПДн, а также в оценке обоснованности и эффективности принятых мер.

8.3. Повседневный контроль выполнения организационных мероприятий, направленных на обеспечение защиты информации, проводится ответственным за организацию защиты ПДн МБУ ИЦСО.

8.4. Периодический контроль за эффективностью средств защиты информации 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.

8.5. Плановые и внеплановые проверки за соответствием обработки персональных данных требованиям законодательства могут осуществляться территориальными органами Федеральной службы по надзору в сфере связи и массовых коммуникаций (далее - Роскомнадзор).

8.6. 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.

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

8.8. Результаты проверок отражаются в Актах проверок.

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

8.10. Защита ПДн считается эффективной, если принимаемые меры соответствуют установленным требованиям и нормам.

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

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

Ответственный
за организацию защиты ПДн _____ / А.Ю. Никишин /