УТВЕРЖДАЮ

Директор
ГОУ ЯО ЦДЮТурЭк

_____ А.Н. Логинова

« *21* » *января* 20 *14* г.

ПОЛОЖЕНИЕ

о порядке организации и проведения работ
по обеспечению безопасности персональных данных
при их обработке в информационных системах персональных данных
государственного образовательного учреждения Ярославской области
«Центр детского и юношеского туризма и экскурсий»

1 Основные положения

1.1 Настоящее Положение определяет последовательность действий при организации работ по созданию и эксплуатации информационных систем персональных данных (далее по тексту – ИСПДн) и системы защиты персональных данных (далее по тексту – СЗПДн) в государственном образовательном учреждении Ярославской области «Центр детского и юношеского туризма и экскурсий» (далее по тексту – ГОУ ЯО ЦДЮТурЭк), порядок взаимодействия сотрудников и подразделений ГОУ ЯО ЦДЮТурЭк, а также сторонних организаций при проведении указанных работ, их основные функции на каждом этапе работ, а также закрепляет ответственность всех участников работ по обеспечению безопасности персональных данных (далее по тексту – ПДн), обрабатываемых в ГОУ ЯО ЦДЮТурЭк.

1.2 Настоящее Положение разработано в соответствии с требованиями законодательства Российской Федерации по обеспечению безопасности персональных данных.

1.3 Действие настоящего Положения распространяется на все процессы по сбору, записи, систематизации, накоплению, хранению, уточнению (обновлению, изменению), извлечению, использованию, передаче (распространению, предоставлению, доступу), блокированию, удалению, уничтожению ПДн, осуществляемые в ИСПДн ГОУ ЯО ЦДЮТурЭк.

1.4 Настоящее Положение вступает в силу с даты его утверждения и действует до его отмены либо замены новым Положением.

2 Определения

2.1 Ниже приведён перечень определений, используемых при подготовке настоящего Положения.

Безопасность информации (данных) – состояние защищенности информации (данных), при котором обеспечиваются её (их) конфиденциальность, доступность и целостность.

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

Доступ к информации – возможность получения информации и ее использования.

Доступность информации (ресурсов автоматизированной информационной системы) – состояние информации (ресурсов автоматизированной информационной системы), при котором субъекты, имеющие право доступа, могут реализовывать его беспрепятственно.

Защита информации от несанкционированного доступа – защита информации, направленная на предотвращение получения защищаемой информации заинтересованными субъектами с нарушением установленных нормативными и правовыми документами (актами) или обладателями информации прав или правил разграничения доступа к защищаемой информации.

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

Информация – сведения (сообщения, данные) независимо от их формы представления.

Конфиденциальность информации – обязательное для выполнения лицом, получившим доступ к такой информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя.

Мониторинг безопасности информации (при применении информационных технологий) – процедуры регулярного наблюдения за процессом обеспечения безопасности информации при применении информационных технологий.

Несанкционированный доступ (к информации / ресурсам автоматизированной информационной системы) – доступ к информации (ресурсам автоматизированной информационной системы), осуществляемый с нарушением установленных прав и (или) правил доступа к информации (ресурсам автоматизированной информационной системы).

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 персональных 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).

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

Технические средства информационной системы персональных данных – средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки персональных данных.

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

Угроза (безопасности информации) – совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения конфиденциальности, доступности и (или) целостности информации.

Целостность информации — состояние защищённости информации, характеризуемое способностью автоматизированной системы обеспечивать сохранность и неизменность информации при попытках несанкционированных или случайных воздействий на нее в процессе обработки и хранения.

3 Организационная структура ГОУ ЯО ЦДЮТурЭк в области обеспечения безопасности персональных данных

3.1 Директор ГОУ ЯО ЦДЮТурЭк в рамках обеспечения безопасности ПДн выполняет следующие функции:

- осуществляет общую координацию действий в области защиты ПДн;
- утверждает планы работ в области защиты ПДн;
- обеспечивает реализацию планов в области защиты ПДн;
- организует обучение сотрудников по вопросам обеспечения безопасности ПДн;
- принимает решения о необходимости привлечения сторонних организаций на этапах инвентаризации информационных ресурсов, предпроектного обследования, проектирования ИСПДн и СЗПДн, внедрения ИСПДн и СЗПДн в эксплуатацию и поддержания работоспособности ИСПДн и СЗПДн при их эксплуатации.

3.2 Лицо, ответственное за организацию обработки ПДн, в рамках обеспечения безопасности ПДн выполняет следующие функции:

- обеспечивает контроль соблюдения в ГОУ ЯО ЦДЮТурЭк требований законодательства РФ о ПДн;
- организует (в том числе, осуществляет) разработку и представление на утверждение проектов организационно-распорядительных документов по вопросам обработки и защиты ПДн, поддерживает в актуальном состоянии политику ГОУ ЯО ЦДЮТурЭк в отношении обработки ПДн, обеспечивает ее опубликование;
- доводит до сведения работников ГОУ ЯО ЦДЮТурЭк положения законодательства РФ о ПДн и внутренних документов ГОУ ЯО ЦДЮТурЭк по вопросам защиты информации;

– организует прием и обработку обращений и запросов субъектов ПДн или их представителей;

– осуществляет выбор методов и способов защиты ПДн, участвует в формировании требований по обеспечению безопасности ПДн;

– обеспечивает физическую защиту помещений с установленными техническими средствами, участвующими в обработке ПДн, а также помещений, где хранятся материальные носители ПДн, дистрибутивы и документация к средствам защиты информации;

– разрабатывает планы работ в области защиты ПДн.

3.3 Лицо, ответственное за обеспечение безопасности ПДн в ИСПДн, в рамках обеспечения безопасности ПДн выполняет следующие функции:

– разрабатывает и согласует формы договоров или соглашений ГОУ ЯО ЦДЮТурЭк и третьими лицами, в рамках которых предполагается передача ПДн, предоставление доступа к ПДн либо совместная обработка ПДн;

– анализирует законность целей обработки ПДн ГОУ ЯО ЦДЮТурЭк;

– определяет необходимость взимания согласия с субъектов ПДн на обработку их ПДн в ГОУ ЯО ЦДЮТурЭк, передачу их ПДн третьим лицам, поручение обработки их ПДн сторонним организациям;

– анализирует правомерность запросов от субъектов ПДн, иных лиц, органов, учреждений и организаций к ГОУ ЯО ЦДЮТурЭк;

– обеспечивает предоставление доступа к защищаемым ресурсам ГОУ ЯО ЦДЮТурЭк в соответствии с матрицей доступа, обеспечивает возможность доступа работников ГОУ ЯО ЦДЮТурЭк к необходимым им для выполнения служебных обязанностей ресурсам сети Интернет;

– обеспечивает безотказную работу и восстановление работоспособности ИСПДн и иных информационных систем ГОУ ЯО ЦДЮТурЭк в случае сбоя.

3.4 Ответственность за своевременность и качество выполнения требований законодательства РФ о ПДн возлагается на руководителя ГОУ ЯО ЦДЮТурЭк.

3.5 Ответственность за выполнение требований настоящего Положения возлагается на всех лиц, указанных в данном разделе.

4 Общий порядок организации работ по обеспечению безопасности персональных данных

4.1 Организация работ по обеспечению безопасности ПДн подразумевает:

– разработку плана проведения работ с указанием ожидаемого результата на каждом этапе;

– определение ресурсов, необходимых на каждом этапе проведения работ, и сроков реализации каждого этапа;

– определение лиц, ответственных за реализацию каждого этапа, и лиц, непосредственно участвующих в проведении работ на каждом этапе;

– определение порядка контроля проведения работ на каждом этапе.

4.2 Разработку плана проведения работ по обеспечению безопасности ПДн, обрабатываемых в ГОУ ЯО ЦДЮТурЭк, осуществляет лицо, ответственное за организацию обработки ПДн. План проведения работ составляется сроком на один год и утверждается директором ГОУ ЯО ЦДЮТурЭк.

4.3 Определение необходимого уровня материального, технического и научно-методического обеспечения деятельности на каждом этапе работ и сроков реализации каждого этапа осуществляется совместно лицом, ответственным за обеспечение безопасности ПДн в ИСПДн, лицом, ответственным за организацию обработки ПДн, и директором ГОУ ЯО ЦДЮТурЭк.

4.4 Решением директора ГОУ ЯО ЦДЮТурЭк определяются лица, ответственные за реализацию каждого этапа работ по обеспечению безопасности ПДн, обрабатываемых в ГОУ ЯО ЦДЮТурЭк.

4.5 Директор ГОУ ЯО ЦДЮТурЭк определяет лиц, участвующих в проведении работ на каждом этапе, и их задачи, в том числе, принимает решение о необходимости привлечения сторонних организаций для проведения соответствующих работ.

4.6 Директор ГОУ ЯО ЦДЮТурЭк определяет требования к представлению лицами, ответственными за реализацию соответствующих этапов работ, отчетов о ходе реализации и результатах каждого этапа работ по обеспечению безопасности ПДн. На основании данных отчетов директор ГОУ ЯО ЦДЮТурЭк принимает решение о корректировке сроков реализации соответствующих этапов проведения работ, о необходимости привлечения дополнительных ресурсов, лиц, подразделений или организаций.

5 Порядок проведения работ по созданию системы защиты персональных данных

5.1 Обеспечение безопасности ПДн, обрабатываемых в ГОУ ЯО ЦДЮТурЭк, должно достигаться скоординированным применением различных по своему характеру методов противодействия угрозам безопасности ПДн: правовых, организационных, экономических, инженерно-технических, программно-аппаратных.

5.2 Безопасность ПДн, обрабатываемых с помощью технических средств, обеспечивается системой защиты персональных данных и дополняющими ее мерами нетехнического характера.

5.3 Предусматриваются следующие стадии создания СЗПДн:

- предпроектная стадия;
- стадия проектирования;
- стадия реализации проектных решений;
- стадия ввода СЗПДн в действие;
- стадия сопровождения СЗПДн.

5.4 Предпроектная стадия создания СЗПДн включает в себя:

- обследование ИСПДн (определение перечня обрабатываемых ПДн; перечня технических средств, входящих в состав ИСПДн; круга лиц, имеющих доступ к ИСПДн и техническим средствам ИСПДн; технологического процесса обработки

информации в ИСПДн и взаимодействия со сторонними организациями, связанного с передачей обрабатываемых ПДн; условий хранения носителей ПДн и размещения технических средств ИСПДн и линий (каналов) связи);

– определение и оценку угроз безопасности обрабатываемых ПДн;

– классификацию ИСПДн;

– выбор методов и способов противодействия угрозам безопасности обрабатываемых ПДн;

– разработку технического задания на создание СЗПДн или общих требований к СЗПДн в соответствии с перечнем угроз безопасности ПДн, для противодействия которым представляется целесообразным применение программно-аппаратных методов.

5.5 Стадия проектирования СЗПДн подразумевает:

– разработку проектных решений по СЗПДн;

– разработку проектной документации на СЗПДн.

5.6 На стадии реализации проектных решений осуществляется:

– закупка, установка и настройка средств защиты информации в соответствии с проектной документацией на СЗПДн;

– разработка эксплуатационной документации на СЗПДн;

– реализация необходимых мероприятий организационного характера.

5.7 Стадия ввода СЗПДн в действие предусматривает:

– опытную эксплуатацию СЗПДн;

– приемо-сдаточные испытания СЗПДн;

– аттестацию ИСПДн по требованиям безопасности информации (оценку соответствия ИСПДн требованиям безопасности информации).

5.8 Стадия сопровождения СЗПДн подразумевает:

– поддержание в актуальном состоянии документов, регламентирующих обеспечение безопасности ПДн;

– контроль актуальности аттестационных документов;

– контроль конфигурации средств и систем защиты информации;

– ежегодный инструментальный контроль состояния защищенности системы;

– проведение аттестационных работ в случае изменения конфигурации или замены оборудования, изменения состава используемого программного обеспечения.

5.9 Работы на различных этапах создания СЗПДн могут проводиться как силами сотрудников и подразделений ГОУ ЯО ЦДЮТурЭк, так и сторонними организациями. При этом лицензированию подлежат следующие виды работ и услуг:

– контроль защищенности конфиденциальной информации от утечки по техническим каналам;

– контроль защищенности конфиденциальной информации от несанкционированного доступа и ее модификации в средствах и системах информатизации;

– сертификационные испытания на соответствие требованиям по безопасности информации продукции, используемой в целях защиты конфиденциальной информации;

– аттестационные испытания и аттестация на соответствие требованиям по защите информации;

– проектирование в защищенном исполнении средств и систем информатизации, помещений со средствами (системами) информатизации, подлежащими защите, защищаемых помещений;

– установка, монтаж, испытания, ремонт средств защиты информации (технических средств защиты информации, защищенных технических средств обработки информации, технических средств контроля эффективности мер защиты информации, программных (программно-технических) средств защиты информации, защищенных программных (программно-технических) средств обработки информации, программных (программно-технических) средств контроля защищенности информации).

6 Порядок организации доступа к информационным системам персональных данных и их элементам сторонних организаций

6.1 При взаимодействии со сторонними организациями в случаях, когда сотрудникам этих организаций предоставляется доступ к ИСПДн или ее элементам, с этими организациями заключается соглашение о соблюдении режима безопасности информации при выполнении работ, предусматривающее процедуру определения прав и условий доступа сторонних лиц к защищаемым объектам, и разграничение между сторонами соглашения зон ответственности за нарушение требований безопасности. Данное соглашение может быть включено в договор, заключаемый со сторонними организациями.

6.2 Доступ посторонних лиц к ИСПДн и ее элементам в обязательном порядке осуществляется в присутствии лица, ответственного за эксплуатацию ИСПДн, и (или) лица, ответственного за обеспечение безопасности ПДн в ИСПДн. Указанные лица организуют доступ сотрудников сторонних организаций к ИСПДн и ее элементам так, чтобы исключить возможность несанкционированного доступа к ПДн или их носителям, в том числе, возможность хищения носителя ПДн. При невозможности исключить доступ к ПДн, обрабатываемым в ИСПДн, стороннее лицо, осуществляющее доступ, должно быть под роспись уведомлено о необходимости соблюдать конфиденциальность ПДн и ответственности за нарушение заданных характеристик безопасности информации.

7 Порядок организации работ по эксплуатации информационных систем персональных данных

7.1 Ввод в эксплуатацию и вывод из эксплуатации ИСПДн осуществляются по акту при непосредственном участии работника, ответственного за эксплуатацию ИСПДн, и лица, ответственного за обеспечение безопасности ПДн в ИСПДн.

7.2 Перечень лиц, допущенных к эксплуатации ИСПДн, утверждается директором ГОУ ЯО ЦДЮТурЭк по представлению лица, ответственного за организацию обработки ПДн.

7.3 Лица, ответственные за эксплуатацию ИСПДн, определяются приказом директора ГОУ ЯО ЦДЮТурЭк.

7.4 Подготовка перечня лиц, допущенных к эксплуатации ИСПДн, и перечня защищаемых ресурсов ИСПДн, определение функций лиц, допущенных к эксплуатации ИСПДн, предоставление доступа к ИСПДн осуществляется в соответствии с установленным в ГОУ ЯО ЦДЮТурЭк порядком.

7.5 При выводе из эксплуатации (либо передаче сторонним организациям в целях ремонта) отдельных элементов ИСПДн лицо, ответственное за обеспечение безопасности ПДн в ИСПДн, обеспечивает удаление из запоминающих устройств ПДн и технологической (служебной, конфигурационной, управляющей и т.д.) информации способом, предусмотренным технологией записи в запоминающее устройство.

7.6 Эксплуатация ИСПДн и ее элементов должна осуществляться в соответствии с эксплуатационной документацией, утвержденными инструкциями и правилами.

7.7 По решению директора ГОУ ЯО ЦДЮТурЭк обработка ПДн может быть поручена сторонней организации на основании заключенного с данной организацией договора (соглашения) или контракта. Поручение обработки ПДн сторонней организации может происходить либо в форме предоставления доступа к ИСПДн ГОУ ЯО ЦДЮТурЭк для выполнения определенных функций по обработке ПДн, либо путем создания сторонней организацией собственной ИСПДн для выполнения переданных ей функций по обработке ПДн.

7.8 При принятии решения о поручении обработки ПДн сторонней организации лицо, ответственное за организацию обработки ПДн, определяет необходимость взимания согласия субъектов ПДн на поручение обработки их ПДн третьему лицу, обеспечивает соответствие формы договора (соглашения) или контракта на поручение обработки ПДн требованиям Федерального закона РФ от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

8 Порядок организации внутреннего контроля процесса обработки и обеспечения безопасности персональных данных

8.1 Внутренний контроль процесса обработки и обеспечения безопасности ПДн заключается в проверке выполнения установленных законодательством РФ и внутренними документами ГОУ ЯО ЦДЮТурЭк требований по обработке, хранению и обеспечению безопасности ПДн. Целью проведения внутренних проверок является выявление и своевременное устранение нарушений требований по обеспечению безопасности ПДн, в том числе, путем принятия дополнительных мер по обеспечению безопасности ПДн.

8.2 Мероприятия по осуществлению внутреннего контроля процесса обработки и обеспечения безопасности ПДн направлены на решение следующих задач:

– обеспечение соблюдения работниками ГОУ ЯО ЦДЮТурЭк требований настоящего Положения и других внутренних документов ГОУ ЯО ЦДЮТурЭк, а также нормативных правовых актов, регулирующих сферу обработки ПДн;

– оценка компетентности персонала, задействованного в обработке ПДн, и определение необходимости его обучения по вопросам обработки ПДн и (или) обеспечения безопасности ПДн;

– обеспечение соответствия условий эксплуатации технических средств ИСПДн и средств защиты информации требованиям технической и эксплуатационной документации;

– выявление изменений технологического процесса обработки ПДн, новых угроз безопасности ПДн и их источников, иных факторов, влияющих на оценку угроз безопасности ПДн;

– сбор информации, необходимой для анализа выявленных нарушений требований по обработке, хранению и обеспечению безопасности ПДн, выработки предложений и принятия решений по совершенствованию порядка обработки и обеспечения безопасности ПДн.

8.3 Лица, ответственные за эксплуатацию ИСПДн, обеспечивают текущий контроль соблюдения лицами, имеющими доступ к ИСПДн, требований по эксплуатации ИСПДн.

8.4 Лицо, ответственное за организацию обработки ПДн, совместно с лицом, ответственным за обеспечение безопасности ПДн в ИСПДн, проводит регулярные проверки соблюдения требований по обеспечению безопасности ПДн. Порядок, формы и план проведения внутреннего контроля соблюдения требований по обеспечению безопасности ПДн могут быть закреплены отдельными документами, утвержденными директором ГОУ ЯО ЦДЮТурЭк, либо определяться лицом, ответственным за организацию обработки ПДн, совместно с лицом, ответственным за обеспечение безопасности ПДн в ИСПДн, самостоятельно.

8.5 Результаты контрольных мероприятий должны быть документально зафиксированы. Лицо, ответственное за организацию обработки ПДн, ежеквартально (либо по требованию) представляет директору ГОУ ЯО ЦДЮТурЭк сводный отчет о результатах проведения мероприятий по внутреннему контролю процесса обработки и обеспечения безопасности ПДн.

9 Документальное сопровождение обработки персональных данных

9.1 В случае изменения сведений, указанных в уведомлении уполномоченного органа по защите прав субъектов ПДн о намерении осуществлять обработку ПДн, в частности, принятия дополнительных (иных) мер по обеспечению безопасности ПДн, лицо, ответственное за организацию обработки ПДн (при необходимости - совместно с лицом, ответственным за обеспечение безопасности ПДн в ИСПДн) в недельный срок подготавливает информационное письмо о внесении изменений в уведомление о намерении осуществлять обработку ПДн, по форме и в соответствии с требованиями, установленными уполномоченным органом по защите прав субъектов ПДн.

9.2 При принятии решения о создании ИСПДн, определении новых целей обработки ПДн, возникновении необходимости обработки ПДн (в том числе, законодательно обусловленной) лицо, ответственное за организацию обработки ПДн, определяет необходимость взимания согласия субъектов ПДн на обработку их ПДн в ГОУ ЯО ЦДЮТурЭк. Лицо, ответственное за организацию обработки ПДн, органи-

зует взимание согласия субъектов ПДн на обработку их ПДн при принятии решения о необходимости взимания согласия.

9.3 В случае если ГОУ ЯО ЦДЮТурЭк получает ПДн не от субъекта ПДн, лицо, ответственное за организацию обработки ПДн, определяет необходимость уведомления субъекта ПДн об обработке его ПДн. Лицо, ответственное за организацию обработки ПДн, организует уведомление субъектов ПДн об обработке их ПДн при принятии решения о необходимости такого уведомления.

10 Трансграничная передача персональных данных

10.1 В рамках функционирования ИСПДн ГОУ ЯО ЦДЮТурЭк трансграничная передача обрабатываемых ПДн не осуществляется.

10.2 Решение о необходимости трансграничной передачи ПДн директор ГОУ ЯО ЦДЮТурЭк. При этом лицо, ответственное за организацию обработки ПДн, определяет правомерность передачи ПДн и устанавливает, является ли иностранное государство, на территорию которого предполагается передача ПДн, стороной Конвенции Совета Европы о защите физических лиц при автоматизированной обработке ПДн, или входит в перечень иностранных государств, обеспечивающих адекватную защиту прав субъектов ПДн, утвержденный уполномоченным органом по защите прав субъектов ПДн.

11 Порядок взаимодействия с государственными органами

11.1 По запросу уполномоченного органа по защите прав субъектов ПДн лицо, ответственное за организацию обработки ПДн, оценивает правомерность запроса и обеспечивает подготовку ответа в течение семи рабочих дней с даты получения запроса. Если запрос связан с выявлением неточных ПДн или неправомерной обработки ПДн, то лицо, ответственное за организацию обработки ПДн (при необходимости – совместно с лицом, ответственным за обеспечение безопасности ПДн в ИСПДн), обеспечивает блокирование соответствующих ПДн на период проведения проверки.

11.2 При получении правомерного запроса на исправление выявленных нарушений лицо, ответственное за организацию обработки ПДн, устраняет нарушение собственными силами, если нарушение касается содержания таких документов, как согласие на обработку ПДн, уведомления, договоры, соглашения и т. п. В том случае, если нарушения связаны с удалением, уточнением ПДн, а также с техническими вопросами обеспечения безопасности ПДн, обязанность устранения нарушения возлагается на лицо, ответственное за обеспечение безопасности ПДн в ИСПДн.

11.3 В установленных федеральным законодательством случаях ГОУ ЯО ЦДЮТурЭк обязано предоставлять информацию, содержащую ПДн, по мотивированному запросу уполномоченных органов государственной власти по вопросам их компетенции либо судебных органов. При поступлении соответствующего запроса его правомерность оценивается лицом, ответственным за организацию обработки ПДн. В случае правомерного запроса подготовку ответа на запрос обеспечивает лицо, ответственное за организацию обработки ПДн.