УТВЕРЖДАЮ
Директор Центра

А. В. Жигайлов
«28» декабря 2018 г.

Р Е Г Л А М Е Н Т

проведения контрольных мероприятий в государственном автономном образовательном учреждении дополнительного образования «Центр для одаренных детей «Поиск»

1. Общие положения

1.1. Регламент проведения контрольных мероприятий в государственном автономном образовательном учреждении дополнительного образования «Центр для одаренных детей «Поиск» (далее – Регламент) разработан в соответствии с Федеральным законом от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», с Федеральным законом Российской Федерации от 27.06.2006 г. N 152-ФЗ "О персональных данных", Доктриной информационной безопасности Российской Федерации», утвержденной Президентом Российской Федерации от 09.09.2000 г. № Пр-1895.

1.2. Настоящий Регламент определяет последовательность проведения контрольных внутренних мероприятий по соответствию требованиям законодательства в области персональных данных и последовательность действий при возникновении инцидентов информационной безопасности. В регламенте указывается последовательность действий по обновлению и актуализации внутренних локальных актов, касающихся обработки и защиты персональных данных в государственном автономном образовательном учреждении

дополнительного образования «Центр для одаренных детей «Поиск» (далее – Центр «Поиск»).

2. Цели и задачи Контроля

2.1. Цели контроля

2.1.1. Формализация состава и периодичности проведения контрольных мероприятий, порядка их проведения и планирования.

2.1.2. Формализация порядка проведения оценки соответствия обработки и защиты персональных данных в Центре «поиск» требованиям законодательства РФ в области персональных данных и локальных нормативных актов Центра «Поиск».

2.1.3. Формализация порядка проведения оценки эффективности и достаточности принимаемых мер по обеспечению безопасности персональных данных в соответствии с оценкой вреда, который может быть причинен субъектам персональных данных в случае нарушения их законных прав.

2.1.4. Обеспечение своевременного выявления и предотвращения угроз безопасности персональных данных при их обработке в информационных системах персональных данных Центра «Поиск».

2.2. Основные задачи Контроля

2.2.1. проверка соответствия принятых и принимаемых мер по защите ПДн требованиям законодательства РФ и локальным актам Центра «Поиск»;

2.2.2. проверка своевременности и полноты выполнения требований нормативных документов, регламентирующих организацию и порядок осуществления мероприятий по защите ПДн.

2.3. Все лица, назначенные приказом директора в состав постоянно действующей комиссии по защите персональных данных, а также лица, на которых локальными нормативными актами Центра «Поиск» возлагается ответственность за проведение мероприятий по контролю обеспечения защиты

персональных данных, в обязательном порядке должны быть ознакомлены с настоящим регламентом.

2.4. Регламент вступает в силу с момента утверждения директором Центра «Поиск». Действует бессрочно до замены или отмены. Все изменения вносятся приказом директора.

2.5. Полный плановый пересмотр Регламента осуществляется регулярно, не реже одного раза в три года, с целью проверки соответствия положений реальным условиям обработки и защиты персональных данных в Центре «Поиск».

2.6. Частичный пересмотр осуществляется по мере необходимости постоянно действующей комиссией по защите персональных данных в следующих случаях:

- при изменении приоритетов угроз безопасности персональных данных;
- при изменении процессов обработки персональных данных, местонахождения объектов защиты, условий их содержания, хранения и использования;
- при определении такой необходимости по результатам проведения внутреннего контроля обеспечения защиты персональных данных, в целях повышения эффективности мероприятий, определенных в настоящем регламенте;
- при изменении состава, обязанностей и полномочий должностных лиц Центра «Поиск», задействованных в вводимых настоящим регламентом мероприятиях.

2.7. Результат проведения контрольных мероприятий служит подтверждением того, что:

- СЗПДн обеспечивают выполнение требований законодательства РФ в области защиты ПДн при эксплуатации ИСПДн;
- меры, средства и мероприятия, проводимые в целях защиты ПДн, обеспечивают необходимый уровень защищенности ПДн при их обработке в ИСПДн;

- СЗИ настроены и используются в соответствии с техническими условиями, правилами эксплуатации и требованиями формуляров;
- рекомендации предшествующих проверок реализованы в полной мере.

2.8. Постоянный внутренний Контроль осуществляется Комиссией в рамках исполнения ею своих обязанностей.

2.9. Результаты Контроля оформляются актами и доводятся до сведения директора и должностных лиц.

2.10. Полная внутренняя проверка условий обработки и защиты ПДн проводится Комиссией не реже 1 раза в 3 года в сроки, определяемые Комиссией, и санкционируется приказом директора.

2.11. По инициативе Комиссии может проводиться аудит обеспечения безопасности ПДн с привлечением третьей стороны – юридических лиц или индивидуальных предпринимателей, имеющих лицензию ФСТЭК России на осуществление деятельности по технической защите конфиденциальной информации, заключающийся в оценке соответствия текущего состояния информационной безопасности в Центре «Поиск» требованиям правовых и нормативных документов в области защиты ПДн.

3. Организация Контроля

3.1. Виды Контроля

3.1.1. Комиссия проводит как плановый (периодический), так и внеплановый Контроль. Время проведения внепланового Контроля проверяемым не сообщается. Порядок проведения Контроля определяется локальными нормативными актами Центра «Поиск», включая настоящий Регламент, и соответствующими методиками.

3.1.2. Повседневный (оперативный) Контроль над выполнением требований по защите ПДн осуществляют лица, ответственные за эксплуатацию ИСПДн, обработку ПДн, а также члены Комиссии и другие уполномоченные приказами директора лица.

3.2. Состав контрольных мероприятий

3.2.1. Основными составляющими Контроля являются:

3.2.1.1. Автоматизированный контроль на основе мониторинга событий информационной безопасности.

3.2.1.2. Проверка правильности и полноты проводимых мероприятий по обеспечению соответствия обработки и защиты ПДн требованиям законодательства РФ.

3.2.1.3. Проверка работоспособности и эффективности средств защиты информации. Проверка работоспособности средств защиты информации в рамках контрольных мероприятий проводится в соответствии с программой проведения контроля состояния СЗПДн.

3.2.1.4. Проверка своевременности внесения изменений в проектную, техническую и нормативно-техническую документацию по обеспечению безопасности ПДн.

3.2.1.5. Принятие на основе результатов Контроля мер по устранению последствий нарушений требований безопасности ПДн, вплоть до полного или частичного приостановления эксплуатации ИСПДн, если иными мерами невозможно устранить нарушения требований безопасности ПДн.

3.2.1.6. Проведение в ходе мероприятий по государственному контролю разъяснительной работы по применению требований законодательства РФ и нормативных документов в области защиты ПДн в ИСПДн.

3.2.2. Основные контрольные мероприятия и периодичность их проведения приведены в таблице 1.

Таблица 1

Перечень основных контрольных мероприятий

Мероприятие	Периодичность
Контроль соответствия полномочий пользователей ИСПДн матрицам доступа	Ежемесячно

Контроль соблюдения порядка и требований обработки ПДн	Еженедельно
Контроль соблюдения требований парольной защиты	Ежемесячно
Контроль соблюдения требований антивирусной защиты	Еженедельно
Контроль соблюдения требований ИБ в сфере информационного обмена	Еженедельно
Контроль соблюдения требований работы с машинным носителем информации	Ежемесячно
Контроль соблюдения порядка доступа в выделенные помещения	Ежеквартально
Контроль соблюдения порядка проведения резервного копирования, хранения и корректности создаваемых резервных копий	Ежемесячно
Контроль соблюдения порядка использования СЗИ	Еженедельно
Контроль соблюдения требований хранения материальных носителей ПДн (бумажных и машинных)	Ежеквартально
Контроль соблюдения требований работы в ИСПДн	Ежемесячно
Контроль соответствия состава обрабатываемых ПДн заявленным целям их обработки	Ежегодно
Контроль реагирования на обращения (запросы) субъектов ПДн об исполнении из законных прав	Ежемесячно
Контроль исполнения требований Комиссии	Ежеквартально
Контроль (тестирование) работоспособности и корректной настройки СЗПДн	Ежеквартально
Контроль удаления ПДн и уничтожения их материальных носителей	Ежеквартально
Контроль соблюдения порядка предоставления ПДн и их материальных носителей третьим лицам	Ежемесячно
Выявление изменений порядка и условий обработки и защиты ПДн	Ежегодно
Контроль обновления ПО и соответствия программного и технического состава ИСПДн заявленному (техническому паспорту)	Ежемесячно
Анализ и переоценка УБПДн, предсказание появления новых, еще не известных угроз	Ежегодно
Контроль исполнения требований законодательства РФ в области ПДн	Ежеквартально
Контроль актуальности ЛНА, регламентирующих обработку и защиту ПДн	Ежеквартально
Контроль ведения журнальных форм Ежеквартально Внутренний аудит обеспечения безопасности ПДн	1 раз в 3 года

3.2.3. Периодичность проведения того или иного мероприятия устанавливается по решению Комиссии. Некоторые мероприятия следует проводить внепланово, в случае изменения внешних факторов, например, изменения законодательства РФ в области ПДн.

3.3. Планирование

3.3.1. Внутренние мероприятия по Контролю могут быть плановыми и внеплановыми.

3.3.2. Плановые мероприятия

3.3.2.1. Плановые мероприятия устанавливаются локальными нормативными актами Центра «Поиск», регламентирующими обработку и защиту ПДн, включая настоящий регламент.

3.3.2.2. Перечень плановых мероприятий формируется Комиссией и утверждается директором в виде годового плана.

3.3.3. Внеплановые мероприятия

3.3.3.1. Решение о проведении внеплановых мероприятий принимается председателем Комиссии, и оформляется приказом директора.

3.3.3.2. Внеплановость мероприятий подразумевает максимально короткий срок между выходом приказа о проведении и проведением; минимизацию круга лиц, которые заранее знают о готовящемся мероприятии; отсутствие периодичности в сроках проведения таких мероприятий.

3.3.3.3. Внеплановые мероприятия могут осуществляться, в частности, в случаях изменения законодательства РФ в области ПДн; возникновения инцидента информационной безопасности (например, утечки ПДн); появления жалоб субъектов ПДн; изменения структуры процессов обработки ПДн.

3.3.3.4. Внеплановые мероприятия могут осуществляться, в частности, в целях реагирования на инциденты ИБ и их предупреждения; определения текущего состояния СЗПДн; определения уровня

подготовки работников в области защиты ПДн; тестирования СЗПДн.

3.3.3.5. В качестве внеплановых мероприятий могут выступать любые мероприятия из входящих в состав плановых, а также иные.

4. Проведение Контроля

4.1. Внутренний плановый Контроль проводится Комиссией в соответствии с годовыми планами. Планы, составляются на один календарный год таким образом, чтобы в течение года была проведена проверка выполнения всех требований к обеспечению безопасности ПДн и условиям их обработки.

4.2. При проведении внутреннего планового Контроля Комиссия:

4.2.1. проверяет наличие необходимых локальных нормативных актов и эксплуатационных документов на СЗИ и знание их работниками Центра «Поиск»;

4.2.2. проверяет выполнение требований локальных нормативных актов Центра «Поиск» и эксплуатационных документов на СЗИ работниками Центра «Поиск»;

4.2.3. документирует результаты Контроля;

4.2.4. вырабатывает рекомендации по устранению недостатков в обеспечении ИБ и по совершенствованию СЗПДн.

4.3. Результаты проведения внутренних мероприятий по контролю фиксируются в протоколах проведения внутренних проверок. В случае выявления нарушения, председателем Комиссии в протоколе делается запись о мероприятиях по устранению нарушения и сроке исполнения. Протоколы хранятся у председателя Комиссии до конца текущего года. Уничтожение протоколов проводится Комиссией самостоятельно в январе следующего за проверочным годом.

4.4. По результатам внутреннего планового Контроля разрабатывается план по устранению недостатков в обеспечении ИБ и совершенствованию СЗПДн,

в соответствии с которым в Учреждении разрабатываются и проводятся необходимые мероприятия.

4.5. О результатах внутреннего Контроля и мерах, необходимых для устранения нарушений, директору докладывает председатель Комиссии.

4.6. При повседневном Контроле осуществляется анализ событий, произошедших в ИСПДн, по различным системным журналам. Для расследования инцидентов, связанных с нештатными ситуациями или нарушением безопасности ПДн, в Центре «Поиск» могут создаваться специальные комиссии.

4.7. В случае невозможности проведения того или иного мероприятия в запланированный заранее день, оно может быть проведено ранее или позднее (не более чем на неделю) намеченной даты.

5. Годовой план мероприятий

5.1. Общие сведения

5.1.1. Комиссией ежегодно формируется Годовой план на один (следующий) год. После формирования годовой план утверждается директором не позднее 28 декабря текущего года.

5.1.2. После утверждения годовой план передается председателю Комиссии.

5.1.3. Вопросы пересмотра плана на текущий год решаются на заседании Комиссии.

5.1.4. Выполненные планы хранятся в течение трех лет.

5.2. Структура годового плана

5.2.1. В годовой план включаются все устанавливаемые локальными нормативными актами Центра «Поиск» мероприятия в области защиты ПДн.

5.2.2. Годовой план состоит из двух разделов: еженедельные мероприятия и прочие мероприятия.

5.2.3. В первый раздел годового плана включаются мероприятия, выполнение которых необходимо осуществлять еженедельно или чаще (ежедневно, два раза в неделю и т.п.).

5.2.4. Во второй раздел включаются мероприятия, осуществляемые с периодичностью от одного раза в неделю (не включительно). Каждое такое мероприятие должно быть привязано к конкретной дате, в которую данное мероприятие должно быть проведено. При выборе даты проведения мероприятия необходимо ориентироваться по календарю выходных и праздничных дней на соответствующий год. Даты должны располагаются в порядке от 1 января до 31 декабря.

5.3. Обновление годового плана

5.3.1. Вопросы обновления годового плана на текущий год рассматриваются на заседаниях Комиссии.

5.3.2. При необходимости дополнить годовой план новыми мероприятиями, либо изменить состав или порядок мероприятий в плане на оставшийся период года – годовой план изменяется.

5.3.3. Мероприятия, размещенные в старой версии плана, в новую не переносятся. Новая версия должна содержать только мероприятия, актуальные до конца года. На обложке новой версии плана указывается с какой даты он действует.

5.3.4. Обновленная версия утверждается директором и незамедлительно, в течение одного дня, передается председателю Комиссии, старая версия изымается. На обложке старой версии годового плана делается пометка о его неактуальности, начиная с указанной даты.

5.4. Обращение ответственного с годовым планом

5.4.1. Ответственный за выполнение мероприятий годового плана обязан ежедневно уточнять состав ближайших мероприятий с целью подготовки к ним, а также выполнять все мероприятия, запланированные на текущий день.

5.5. Контроль выполнения плановых мероприятий

5.5.1. Контроль выполнения плановых мероприятий осуществляется ежеквартально Комиссией.

5.5.2. Осуществляется контроль выполнения мероприятий за истекший квартал.

5.5.3. В случае невыполнения без уважительных причин запланированных мероприятий, ответственное лицо может быть подвергнуто дисциплинарному взысканию.

6. Ответственность

6.1. Лица, ответственные за проведение мероприятий по Контролю, несут персональную ответственность за качество и своевременность проведения возложенных на них мероприятий в соответствии с настоящим регламентом и действующим законодательством РФ.