Утверждаю директор

МАОУ СШ №55 г. Липецка «Лингвист»

Т.Д. Тихонова

Положение МАОУ СШ №55 г. Липецка «Лингвист» о структурном подразделении, ответственном за обеспечение безопасности персональных данных при их обработке в информационных системах персональных данных.

1. Общие положения

1.1. Настоящее «Положение МАОУ СШ №55 г. Липецка «Лингвист» о структурном подразделении, ответственном за обеспечение безопасности персональных данных при их обработке в информационных системах персональных данных» (далее – Положение) определяет правовое положение, функции и ответственность структурного подразделения МАОУ СШ №55 г. Липецка «Лингвист» (далее – Оператор), на которого руководителем Оператора возложена роль Структурного подразделения, ответственного за обеспечение безопасности персональных данных в информационных системах персональных данных (далее – СПОБПДн).

1.2. Настоящее Положение разработано в соответствии с действующим законодательством Российской Федерации в области обработки и защиты персональных данных.

1.3. Настоящее Положение вступает в силу после его утверждения руководителем Оператора. Все изменения в Положение вносятся на основании решения руководителя Оператора в установленном порядке.

2. Основные понятия.

2.1. В настоящих Правилах используются основные понятия, приведенные в пункте 2 «Положения МАОУ СШ №55 г. Липецка «Лингвист» об организации обработки персональных данных».

3. Правовое положение СПОБПДн.

3.1. СПОБПДнв лице своего руководителя и своих представителей несёт ответственность за обеспечение безопасности персональных данных в соответствии с требованиями статьи 19 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

3.2. СПОБПДн в лице своего руководителя и своих представителей наделяется следующими правами:

3.2.1. Требовать от обеспечивающих информационную безопасность и применение информационных технологий должностных лиц и представителей иных подразделений Оператора отчёта о выполнении своих должностных обязанностей, связанных с построением и поддержанием в актуальном состоянии

системы защиты персональных данных, в частности, выполнения ими следующих задач, но не ограничиваясь ими:

(1) осуществление регулярного обнаружения уязвимостей и угроз безопасности персональных данных;

(2) участие в определении актуальных угроз безопасности персональных данных;

(3) проведение работ по проработке технических решений по защите персональных данных, внедрению и эксплуатации программных и аппаратных средств защиты, а также инфраструктуры информационных систем персональных данных;

(4) участие в разработке и поддержании в актуальном состоянии организационно-распорядительной документации системы защиты персональных данных;

(5) участие в реализации разрешительной системы доступа к персональным данным (для владельцев ИСПДн и процессов обработки персональных данных).

3.2.2. Запрашивать и получать от сотрудников Оператора информацию для исполнения своих прав и обязанностей, приведенных в настоящем Положении.

3.2.3. Выступать с ходатайством к руководителю Оператора о внесении изменений в технологические процессы, связанные с обработкой персональных данных, а также в ИСПДн, если это обусловлено необходимостью обеспечения безопасности персональных данных в соответствии с требованиями законодательства Российской Федерации;

3.2.4. Выступать с ходатайством к руководителю Оператора о необходимости проведения организационных и технических мероприятий с целью обеспечения безопасности персональных данных в соответствии с требованиями законодательства Российской Федерации.

3.2.5. Выступать с ходатайством к руководителю Оператора о поощрении или наложении взысканий на работников Оператора в связи с исполнением ими обязанностей, связанных с обработкой персональных данных.

3.2.6. Выступать с ходатайством к руководителю Оператора о привлечении организации, обладающей лицензией ФСТЭК России на осуществление деятельности по технической защите конфиденциальной информации, для разработки Частной модели угроз и нарушителя, а также для проведения организационных и технических мероприятий по обеспечению безопасности персональных данных.

4. Функции СПОБПДн.

4.1. СПОБПДн запрашивает у каждой организации, поручающей Оператору обработку персональных данных в ИСПДн Оператора, результат оценки возможного вреда субъектам персональных данных.

4.2. С учётом предоставленных Оператору результатов оценки возможного вреда, СПОБПДн самостоятельно или с привлечением внешней организации, обладающей лицензией ФСТЭК России на деятельность по технической защите конфиденциальной информации, разрабатывает Модель угроз и нарушителя безопасности персональных данных и утверждает её у руководителя Оператора.

4.3. По результатам разработки Модели угроз и нарушителя безопасности СПОБПДн делает вывод о типе угроз, актуальных для ИСПДн, при этом под

актуальными угрозами безопасности персональных данных понимается совокупность условий и факторов, создающих актуальную опасность несанкционированного, в том числе случайного, доступа к персональным данным при их обработке в ИСПДн, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия.

4.4. СПОБПДн самостоятельно или с привлечением организации, обладающей лицензией ФСТЭК России на деятельность по технической защите конфиденциальной информации, определяет и обеспечивает организационные и технические мероприятия, которые должны выполняться Оператором для нейтрализации угроз, признанных актуальными.

4.5. СПОБПДн разрабатывает Требования к организационным и техническим мероприятиям, которые распространяются на все организации, поручающие Оператору обработку персональных данных в ИСПДн Оператора.

4.6. СПОБПДн контролирует выполнение мероприятий по обеспечению безопасности персональных данных в ИСПДн, в том числе:

4.6.1. Организацию режима обеспечения безопасности помещений, в которых размещена ИСПДн, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения.

4.6.2. Обеспечение сохранности носителей персональных данных.

4.6.3. Актуальность утвержденного руководителем Оператора документа, определяющего перечень лиц, доступ которых к персональным данным, обрабатываемым в ИСПДн, необходим для выполнения ими служебных (трудовых) обязанностей.

4.6.4. Использование средств защиты информации, прошедших процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации, в случае, когда применение таких средств необходимо для нейтрализации актуальных угроз, при этом сертификаты на средства защиты информации должны быть действительными.

4.6.5. Назначение Ответственного лица для каждой ИСПДн Оператора (для ИСПДн, для которой установлена необходимость обеспечения 2 уровня защищённости).

4.6.6. Ограничения доступа к содержанию электронного журнала сообщений: доступ должен быть возможен исключительно для должностных лиц (работников) Оператора или уполномоченного лица, которым сведения, содержащиеся в указанном журнале, необходимы для выполнения служебных (трудовых) обязанностей (для ИСПДн, для которой установлена необходимость обеспечения 3 уровня защищённости).

4.6.7. Автоматическую регистрацию в электронном журнале безопасности изменений полномочий работника Оператора по доступу к персональным данным, содержащимся в ИСПДн.

Утверждаю директор

МАОУ СШ №55 г. Липецка «Лингвист»

_____ Т.Д. Тихонова

Правила доступа служащих (работников) МАОУ СШ № 55 г. Липецка «Лингвист» в помещения, в которых ведется обработка персональных данных.

1. Общие положения

1.1. Настоящие «Правила доступа служащих (работников) МАОУ СШ №55 г. Липецка «Лингвист» в помещения, в которых ведется обработка персональных данных» (далее – Правила) устанавливают единые требования к доступу государственных гражданских служащих (работников) МАОУ СШ №55 г. Липецка «Лингвист» (далее – Оператор) в помещения, в которых осуществляется обработка персональных данных (далее – Помещения).

1.2. Настоящие Правила разработаны в соответствии с действующим законодательством Российской Федерации в области обработки и защиты персональных данных.

1.3. Правила обязательны для применения и исполнения всеми служащими (работниками) Оператора. Нарушение порядка обработки персональных данных, определённого Правилами, влечёт материальную, дисциплинарную, гражданскую, административную и уголовную ответственность в соответствии с нормами действующего законодательства Российской Федерации.

1.4. Настоящие Правила вступают в силу после их утверждения руководителем Оператора. Все изменения в Правила вносятся на основании решения руководителя Оператора в установленном порядке.

2. Основные понятия

2.1. В настоящих Правилах используются основные понятия, приведенные в пункте 2 «Положения МАОУ СШ №55 г. об организации обработки персональных данных».

2.2. В настоящих Правилах используется дополнительное понятие:

2.2.1. Помещение – часть объема здания или сооружения, имеющая определенное назначение и ограниченная строительными конструкциями.

3. Доступ в Помещения

3.1. Обеспечение безопасности персональных данных от уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных достигается, в том числе, установлением правил доступа в помещения, в которых ведется обработка персональных данных как с использованием средств автоматизации, так и без использования средств автоматизации.

3.2. Размещение ИСПДн осуществляется в охраняемых помещениях. Для Помещений организуется режим обеспечения безопасности, при котором обеспечивается сохранность носителей персональных данных и средств защиты информации, а также исключается возможность неконтролируемого проникновения и пребывания в этих помещениях посторонних лиц.
3.3. При хранении материальных носителей персональных данных в Помещениях должны соблюдаться условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный доступ к ним.
3.4. В помещения, где размещены технические средства, позволяющие осуществлять обработку персональных данных, а также хранятся носители информации, допускаются только служащие (работники) Оператора, уполномоченные осуществлять обработку и (или) защиту персональных данных.
3.5. Ответственными за организацию доступа в Помещения являются начальники структурных подразделений, использующих Помещения.
3.6. Нахождения лиц, не уполномоченных осуществлять обработку и (или) защиту персональных данных, в Помещениях возможно только в сопровождении уполномоченного служащего (работника) Оператора на время, ограниченное служебной необходимостью.
3.7. Внутренний контроль за соблюдением порядка доступа в Помещения, проводится лицом, ответственным за организацию обработки персональных данных.

4. Требования к Помещениям

4.1. В целях обеспечения соблюдения требований к ограничению доступа в Помещения Оператором обеспечивается:
4.1.1. Использование Помещений строго по назначению.
4.1.2. Наличие на входах в Помещения дверей, оборудованных запорными устройствами, уплотняющими прокладками.
4.1.3. Содержание дверей Помещений в нерабочее время в закрытом на запорное устройство состоянии.
4.1.4. Содержание окон в Помещениях в нерабочее время в закрытом состоянии.