

Положение
о защите информации, содержащейся в автоматизированной информационной
системе «Сетевой город. Образование» МБОУ СОШ с.Леонидово

1. Общие положения

1.1. Данное Положение о защите информации (далее Положение) разработано в соответствии с Федеральным законом от 27.07.2006 N 149-ФЗ «Об информации, информационных технологиях и о защите информации», приказом ФСТЭК России от 18 февраля 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».

1.2. Ограничение доступа к информации

1.2.1. Ограничение доступа к информации устанавливается федеральными законами в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства.

1.2.2. Обязательным является соблюдение конфиденциальности информации, доступ к которой ограничен федеральными законами.

1.2.3. Защита информации осуществляется в соответствии с **законодательством** Российской Федерации.

1.2.4. Федеральными законами устанавливаются условия отнесения информации к сведениям, составляющим служебную тайну и иную тайну, обязательность соблюдения конфиденциальности такой информации, а также ответственность за ее разглашение.

1.2.5. Информация, полученная гражданами (физическими лицами) при исполнении ими профессиональных обязанностей или организациями при осуществлении ими определенных видов деятельности (профессиональная тайна), подлежит защите в случаях, если на эти лица федеральными законами возложены обязанности по соблюдению конфиденциальности такой информации.

1.2.6. Информация, составляющая профессиональную тайну, может быть предоставлена третьим лицам в соответствии с федеральными законами и (или) по решению суда.

1.2.7. Срок исполнения обязанностей по соблюдению конфиденциальности информации, составляющей профессиональную тайну, может быть ограничен только с согласия гражданина (физического лица), предоставившего такую информацию о себе.

1.2.8. Запрещается требовать от гражданина (физического лица) предоставления информации о его частной жизни, в том числе информации, составляющей личную или семейную тайну, и получать такую информацию помимо воли гражданина (физического лица), если иное не предусмотрено федеральными законами.

1.2.9. Порядок доступа к персональным данным граждан (физических лиц) устанавливается федеральным законом о персональных данных.

2. Понятие о защите информации:

Разделение в информационной системе функций по управлению (администрированию) информационной системой, управлению (администрированию) системой защиты персональных данных, функций по обработке персональных данных и иных функций ИС

Обеспечение доверенных канала, маршрута между администратором, пользователем и средствами защиты информации (функциями безопасности средств защиты информации)

Контроль целостности программного обеспечения, включая программное обеспечение средств защиты информации.

Контроль целостности персональных данных, содержащихся в базах данных информационной системы
Обеспечение возможности восстановления программного обеспечения, включая программное обеспечение средств защиты информации, при возникновении внештатных ситуаций
Обнаружение и реагирование на поступление в информационную систему незапрашиваемых электронных сообщений (писем, документов) и иной информации, не относящихся к функционированию информационной системы
Контроль содержания информации, передаваемой из информационной системы (контейнерный, основанный на свойствах объекта доступа, и (или) контентный, основанный на поиске запрещенной к передаче информации с использованием сигнатур, масок и иных методов), и исключение неправомерной передачи информации из информационной системы
Ограничение прав пользователей по вводу информации в информационную систему
Исключение возможности отрицания пользователем факта отправки персональных данных другому пользователю
Контроль точности, полноты и правильности данных, вводимых в информационную систему по вводу и (или) передаче персональных данных и предупреждение пользователей об ошибочных действиях.
Меры по защите машинных носителей персональных данных (средств обработки (хранения) персональных данных, съемных машинных носителей персональных данных) должны исключать возможность несанкционированного доступа к машинным носителям и хранящимся на них персональным данным, а также несанкционированное использование съемных машинных носителей персональных данных.
Меры по антивирусной защите должны обеспечивать обнаружение в информационной системе компьютерных программ либо иной компьютерной информации, предназначенной для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты информации, а также реагирование на обнаружение этих программ и информации.

3. В школе имеется утвержденный директором перечень должностей, имеющих доступ к персональным данным. Данный доступ необходим им для полноценного исполнения их трудовых обязанностей. Документы и информация избирательно и обоснованно распределены между работниками.

4. При уходе в отпуск, служебной командировке и иных случаях длительного отсутствия работника на рабочем месте, он обязан передать документы и иные носители лицам, имеющим доступ к персональным данным.

5. Персональные данные работников, учащихся учреждения хранятся в шкафу и несгораемом сейфе, а также в электронном виде на локальной компьютерной сети.

Дверь оборудована надежным замком. Доступ к электронным базам данных, содержащих персональные данные работников, обеспечиваются системой паролей. Пароли устанавливаются руководителем школы и сообщаются лишь узкому кругу лиц.