

МУНИЦИПАЛЬНОЕ БЮДЖЕТНОЕ ОБЩЕОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
«СРЕДНЯЯ ОБЩЕОБРАЗОВАТЕЛЬНАЯ ШКОЛА п. ДОЛИНСКИЙ
ГРОЗНЕНСКОГО МУНИЦИПАЛЬНОГО РАЙОНА»
(МБОУ «СОШ п. Долинский»)
МУНИЦИПАЛЬНИ БЮДЖЕТАН ЮКЪАРАДЕШАРАН ХЪУКМАТ
«ГРОЗНЕНСКИ МУНИЦИПАЛЬНИ КЮШТАН ДОЛИНСКИЙ ПОСЕЛКЕРА
ЮККЪЕРА ЮКЪАРАДЕШАРАН ШКОЛА»

ПРИНЯТО:

Педагогический совет школы
Протокол № 1 "25" 08 2018 г.

УТВЕРЖДАЮ:

Директор МБОУ «СОШ п. Долинский»

И.И. Успаев

Приказ № 101 "25" 08 2018 г.



СВЕДЕНИЯ

о реализуемых требованиях к защите персональных данных в МБОУ «СОШ п. Долинский»

Основные понятия и определения:

- 1) Информационная система персональных данных - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств (далее - ИСПДн);
- 2) Автоматизированная обработка персональных данных - обработка персональных данных с помощью средств вычислительной техники;
- 3) Угроза безопасности персональных данных - совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия при их обработке в информационной системе персональных данных;
- 4) Уровень защищенности персональных данных - комплексный показатель, характеризующий требования, исполнение которых обеспечивает нейтрализацию определенных угроз безопасности персональных данных при их

обработке в информационных системах персональных данных.

В соответствии с действующим законодательством в МБОУ «СОШ п. Долинский» создана нормативная база и реализованы мероприятия по защите персональных данных: – назначен ответственный (в соответствии с приказом) за организацию обработки персональных данных;

– изданы документы, регламентирующие обработку персональных данных, а также документы, устанавливающие процедуры, направленные на предотвращение и выявление нарушений законодательства РФ и устранение последствий таких нарушений

– определены угрозы безопасности персональных данных;

– реализованы требования к защите персональных данных исходя из уровня защищенности персональных данных.

– применяются средства защиты информации, прошедшие в установленном порядке процедуру оценки соответствия;

– произведена оценка эффективности принимаемых мер по обеспечению безопасности персональных данных;

– производится учет машинных носителей персональных данных;

– приняты соответствующие меры по защите от несанкционированного доступа к персональным данным;

– осуществляется резервное копирование баз данных содержащих персональные данные, для возможности их восстановления при модификации или уничтожения вследствие несанкционированного доступа к ним;

– проводятся периодические внутренние проверки состояния системы защиты персональных данных;

– произведена оценка вреда, который может быть причинен субъектам персональных данных в случае нарушения законодательства в сфере защиты персональных данных и соотношение причиненного вреда с принятыми мерами; – все работники, осуществляющие обработку персональных данных, ознакомлены под роспись с требованиями к защите персональных данных, положениями законодательства Российской Федерации о персональных данных, локальными актами по вопросам обработки персональных данных.

Все программные средства, используемые для защиты информации, имеют соответствующие сертификаты

