Приложение к Положению о защите персональных данных МБОУ «Северский лицей»

**Существующие меры защиты ИСПД в МБОУ «Северский лицей»**

Существующие в ИСПДн технические меры защиты представлены в таблице ниже.

Таблица 1 – Меры защиты

|  |  |  |
| --- | --- | --- |
| Элемент ИСПДн | Программное средство обработки ПДн | Установленные средства защиты |
| АРМ пользователя | ОС Windows XP, ОС Windows 7БраузерInternet Explorer$Mozilla, Google Chrome | Средства ОС:- управление и разграничение доступа пользователей;- регистрацию и учет действий с информацией.Антивирус *Kaspersky*- регистрацию и учет действий с информацией; - обеспечивать целостность данных; - производить обнаружений вторжений. |
| АРМ администратора | ОС Windows XP, ОС Windows 7БраузерInternet Explorer$Mozilla, Google ChromeПрограммный комплекс ViPNet Client (Клиент) | Средства ОС:- управление и разграничение доступа пользователей;- регистрацию и учет действий с информацией.Антивирус *Kaspersky*- регистрацию и учет действий с информацией; - обеспечивать целостность данных; - производить обнаружений вторжений.Программный комплекс, выполняющий на рабочем месте пользователя или сервере с прикладным ПО функции VPN-клиента, персонального экрана, клиента защищенной почтовой системы, а также криптопровайдера для прикладных программ, использующих функции подписи и шифрования. |

В ИСПДн введены следующие организационные меры защиты:

* В Учреждении осуществляется контроль доступа в контролируемую зону, двери закрываются на замок, установлены камеры на входах в здание.
* Разработаны и внедрены инструкции пользователей ИСПДн и администратора ИСПДн, инструкция пользователя по обеспечению безопасности обработки персональных данных, при возникновении внештатных ситуаций в которых отражены порядок безопасной работы с ИСПДн;
* организовано разграничение прав пользователей на установку стороннего ПО, установку аппаратных средств, подключения мобильных устройств и внешних носителей, установку и настройку элементов ИСПДн и средств защиты.
* Ведется учет носителей информации.
* В Учреждении существует ответственный сотрудник за обеспечение безопасности ПДн.
* В учреждение проводятся периодические внутренние проверки режима безопасности ПДн.
* Введена парольная политика, устанавливающая сложность ключей и атрибутов доступа (паролей), а так же их периодическую смену.
* Пользователи осведомлены и проинструктированы о порядке работы и защиты персональных данных.
* Осуществляется резервное копирование защищаемой информации.
* В помещениях, где расположены элементы ИСПДн, установлена пожарная сигнализация.