ПРИНЯТО
на заседании
Общего собрания
работников Учреждения
Протокол № 5 от 11.08.2017

УТВЕРЖДАЮ
Директор МАОУ СШ № 59
«Перспектива» г. Липецка
_____ Д.А. Гладышев
«_18_» августа_2017 г.

**Описание технологического процесса обработки информации, содержащей персональные данные, в информационных системах персональных данных в МАОУ СШ № 59 «Перспектива» г. Липецка**

1. В процессе обработки информации на объекте вычислительной техники – информационной системы персональных данных (ИСПДн) на базе АРМ ПЭВМ участвуют следующие группы пользователей:

– системный администратор ИСПДн – обладает всей полнотой доступа к ресурсам объекта вычислительной техники, организует и контролирует работу ОВТ объектов информатизации, других пользователей.

– пользователи ИСПДн – имеющие доступ к ИСПДн объектов информатизации на основании приказа о допуске к ИСПДн.

2. Перечень объектов доступа: жесткие магнитные диски (ЖМД), гибкие магнитные диски (ГМД), CD-диски, штатное программное обеспечение (ПО).

3. Перечень субъектов доступа: системный администратор, пользователи. К работе в автоматизированной системе объектов вычислительной техники (ОВТ) допускаются только сотрудники в соответствии с утвержденным Списком пользователей ИСПДн, допущенных к обработке персональных данных и зарегистрированные в установленной системе защиты информации от несанкционированного доступа (далее - СЗИ НСД) Etoken Network Logon 5, eToken PRO, ViPNeT for Windows 4 (в зависимости от типа ИСПДн) после изучения организационно-распорядительной документации ИСПДн.

4. Подготовка персонального компьютера (далее – ПК) к работе:

– включить источник бесперебойного питания, включить системный блок и монитор. Подключить аппаратное устройство идентификации eToken или ViPNeT for Windows 4 (в зависимости от ИСПДн). После запроса системы необходимо набрать персональные логин и пароль на клавиатуре;

– запустить программу антивирусного контроля и проверить жесткий диск и используемые съемные носители на наличие вирусов.

– при нарушении или сбое системы защиты от НСД, при отказе загрузки операционной системы или подключения защищенного хранилища - прекратить работу и пригласить администратора информационной безопасности.

5. Если во время работы на ПК появилась необходимость временно покинуть рабочее место, исполнитель обязан заблокировать ПК. Разблокирование ПК производится набором пароля разблокировки, который был создан при настройке системы блокировки.

6. Описание реализованных правил разграничения доступа.

6.1. Обработка персональных данных осуществляется только на предварительно учтенных носителях информации (защищаемых ресурсах – ЖМД, гибкие магнитные дисков (ГМД), CD-дисков прошедших антивирусный контроль, причем каждый исполнитель для обработки информации использует только свой профиль пользователя, в котором администратором закреплены правила разграничения доступа: возможность доступа к дискам, папкам и файлам, возможность записи и чтения информации и т.д.

6.2. Запись производится только на учтенные магнитные носители информации.

6.3. Администратор организует и контролирует доступ пользователей к доступным ресурсам ИСПДн и состояние информации на носителях.

6.4. По окончании рабочего дня все съемные носители информации, документы и материалы должны находиться в сейфе.

6.5. Исполнители обязаны предъявлять, по требованию ответственного за защиту информации, для проверки все числящиеся за ними документы и носители информации.

9. Исполнителю запрещается:

– обрабатывать информацию в присутствии посторонних лиц;

– записывать информацию на неучтенных носителях информации;

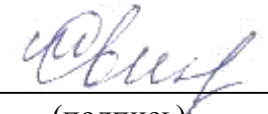
– использовать в работе пароли, если есть подозрение на их компрометацию;

– разглашать сведения о применяемой системе защиты и содержании информации;

– изменять и тиражировать программное обеспечение;

– вводить персональные данные под диктовку;

– производить передачу персональных данных по каналам связи без использования средств криптографической защиты.

Разработал: инженер  М.Г. Свинцова

(подпись)