

ПРИНЯТО
Протокол педагогического совета
№ 1 от 29.02. 2016 г.

УТВЕРЖДЕНО
Приказ
№ 33 от 09.03. 2016 г.

**Правила
разграничения доступа к защищаемым информационным
ресурсам, обрабатываемым с использованием средств вычислительной
техники в МОУ «СОШ №5» г. Всеволожска**

1. Общие положения

1.1. Настоящие правила предназначены для установления правомерного порядка доступа должностных лиц к защищаемым информационным ресурсам, обрабатываемым в электронном виде с использованием средств вычислительной техники.

**2. Предоставление прав доступа к защищаемым
информационным ресурсам**

2.1. Предоставление прав доступа к информационным ресурсам реализуется в форме разрешительной системы доступа и основывается на функциональных обязанностях, выполняемых должностными лицами, связанных с обработкой защищаемых информационных ресурсов, с учетом требований, предъявляемых к безопасности информации.

2.2. Реализация разрешительной системы доступа обеспечивается определением перечня должностных лиц, имеющих право доступа к защищаемым информационным ресурсам и предоставлением или ограничением такого доступа с помощью технических и программных средств защиты информации.

2.3. Перечень должностных лиц, имеющих право доступа к защищаемым информационным ресурсам (Приложение №1) утверждается директором школы.

2.4. Предоставление или ограничение доступа к информационным ресурсам реализуется с помощью технических и программных средств защиты информации, прошедших установленным порядком процедуру оценки

соответствия в форме обязательной сертификации по требованиям безопасности информации (далее — технические средства).

2.5. С помощью технических средств осуществляется заведение, активация, блокирование или уничтожение соответствующих типов учетных записей (внутреннего пользователя, внешнего пользователя: системная, приложения; гостевая (анонимная), временная и (или) иные типы записей) и управление предоставлением прав доступа.

2.6. Управление правами доступа реализуется администратором безопасности информации на основании заявки должностного лица, в приложения; гостевая (анонимная), временная и (или) иные типы записей) и управление предоставлением прав доступа.

2.7. Управление правами доступа реализуется администратором безопасности информации на основании заявки должностного лица, в отношении которого принимаются меры по разграничению доступа к информационным ресурсам.

3. Ответственность

3.1. Администратор безопасности информации несёт ответственность за правильность настроек параметров технических средств разграничения доступа.

3.2. Пользователи, допущенные к защищаемым информационным ресурсам, несут ответственность за нарушение требований безопасности информации, в соответствии с действующим законодательством.