


УТВЕРЖДАЮ
Директор
МБУ ДО «Центр внешкольной работы с детьми и подростками»
О.А.Пашинцева
«09» января 2018 г.



ПРАВИЛА

**доступа к конфиденциальной информации, в том числе персональным данным,
обрабатываемой в информационной системе**

1. Общие положения

1.1. Настоящие правила определяют порядок доступа к конфиденциальной информации, в том числе персональным данным (далее – КИ), обрабатываемым в информационной системе (далее – ИС) МБУ ДО «Центр внешкольной работы с детьми и подростками», лиц, имеющих доступ к КИ.

1.2. Настоящие правила разработаны в соответствии с Федеральным законом от 27.07.2006 г. № 152-ФЗ «О персональных данных», постановлением Правительства Российской Федерации от 01.11. 2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

1.3. Основные понятия и термины, используемые в настоящих правилах, применяются в значениях, определенных статьей 3 Федерального закона № 152-ФЗ.

1.4. Перечень персональных данных (далее – ПДн), обрабатываемых в ИС, а также перечень ИС утверждаются МБУ ДО «Центр внешкольной работы с детьми и подростками» (далее – Организация или Оператор).

1.5. Безопасность ПДн при их обработке в ИС обеспечивается с помощью системы информационной безопасности (далее – СИБ), нейтрализующей актуальные угрозы.

1.6. Управление СИБ осуществляет ответственный за обеспечение безопасности КИ (администратор сети), назначаемый Оператором.

2. Организация доступа к КИ

2.1. Перечень лиц, доступ которых к КИ, обрабатываемым в ИС и на материальных (бумажных) носителях, необходим для выполнения ими служебных (трудовых) обязанностей (далее – лица, допущенные к КИ) утверждает Оператор.

2.2. На основании и в соответствии с утвержденным Перечнем лиц, допущенных к КИ, ответственный за обеспечение безопасности разрабатывает Таблицу разграничения доступа к КИ, форма которой приведена в Приложении № 1 к настоящим правилам.

2.3. Таблица (матрица) разграничения доступа составляется как на электронном, так и на бумажном носителях.

2.4. Ответственный за обеспечение безопасности КИ на основании таблицы доступа предоставляет пользователям доступ к КИ, проверяет на его автоматизированном рабочем месте (далее - АРМ) заданные возможности доступа и выдает под расписку персональный идентификатор.

3. Обязанности лиц, допущенных к КИ:

- не сообщать конфиденциальную информацию лицам, не имеющим права доступа к ней;

- обеспечивать сохранность материалов с КИ;

- не делать неучтенных копий на бумажных и электронных носителях;

- не оставлять включенными АРМ с предоставленными правами доступа, после окончания работы (в перерывах) не оставлять материалы с КИ на рабочих столах. Покидая рабочее место, пользователь обязан убрать документы и электронные носители с КИ в закрываемые на замок шкафы (сейфы);

- при работе с документами, содержащими КИ, исключить возможность ознакомления, просмотра этих документов лицами, не допущенными к работе с ними;

- не выносить документы и иные материалы с КИ из служебных помещений, предназначенных для работы с ними;

- не вносить изменения в настройку средств защиты информации (далее – СЗИ);

- немедленно сообщать непосредственному руководителю об утрате, утечке или искажении КИ, об обнаружении неучтенных материалов с указанной информацией;

- не допускать действий, способных повлечь утечку КИ;

- предъявлять для проверки лицам, наделенным необходимыми полномочиями в соответствии с законодательством Российской Федерации, числящиеся и имеющиеся

в наличии документы касающиеся КИ только по согласованию с руководителем Оператора.

4. Порядок доступа должностных лиц органов государственной власти, должностных лиц Оператора и субъектов персональных данных к КИ

4.1. Право доступа к КИ имеют должностные лица органов государственной власти, иных государственных органов, органов местного самоуправления, которым доступ к такой информации предусмотрен Федеральными законами.

4.2. Право доступа к КИ имеют должностные лица Оператора, которым доступ к такой информации предусмотрен Федеральными законами и (или) локальными актами Оператора.

4.3. Доступ к КИ субъектов персональных данных осуществляется на основании направленного оператору запроса.

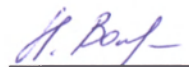
4.4. Порядок учета (регистрации), рассмотрения запросов осуществляется в соответствии с утвержденными Оператором Правилами рассмотрения запросов субъектов персональных данных или их представителей.

4.5. При работе с документами, связанными с предоставлением КИ, должен обеспечиваться режим ограниченного доступа к соответствующим документам.

5. Лица, допущенные к КИ, должны ознакомиться с настоящими Правилами под роспись.

6. Лица, виновные в нарушении требований настоящих Правил и иных документов, регламентирующих вопросы защиты КИ, несут ответственность в соответствии с действующим законодательством Российской Федерации.

Лицо, ответственное за организацию
обработки конфиденциальной информации,
в том числе персональных данных



Приложение № 1
к Правилам доступа к конфиденциальной информации, в том числе персональным данным, обрабатываемым в информационной системе

ТАБЛИЦА

разграничения доступа к конфиденциальной информации, в том числе персональным данным, обрабатываемым в информационной системе «Электронное дополнительное образование» МБУ ДО «Центр внешкольной работы с детьми и подростками»

Наименование информационных ресурсов информационной системы	Тип доступа	Уровень доступа субъектов доступа			
		Системный администратор	Ответственный за безопасность	Пользователь АРМ-1	Пользователь АРМ-2
Программные средства	выполнение	+	+	+	
	инсталляция	+			
	изменение	+			
АРМ 1	Операционная система	+	+		
	Kaspersky Endpoint Security 10		+		
	VIPNet Client 4		+		
	Secret Net 7		+		
	БАРС.Образование – Электронное дополнительное образование	выполнение запись			
Принтер	выполнение настройка		+		

Где: доступ разрешен – «+»

Лицо, ответственное за безопасность

конфиденциальной информации, в том числе персональных данных _____

