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

Должностная инструкция ответственного за обеспечение безопасности конфиденциальной информации, в том числе персональных данных

1. Общие положения

1.1. Настоящая должностная инструкция определяет основные обязанности, права и ответственность лица, ответственного за обеспечение безопасности конфиденциальной информации, в том числе персональных данных (далее – КИ), в информационной системе (далее – ИС) МБУ ДО «Центр внешкольной работы с детьми и подростками».

1.2. Лицо, ответственное за обеспечение безопасности КИ, в ИС МБУ ДО «Центр внешкольной работы с детьми» (далее – Организация или Оператор) назначает руководитель и оно подотчетно ему.

1.3. Лицо, ответственное за обеспечение безопасности КИ в ИС МБУ ДО «Центр внешкольной работы с детьми и подростками» (далее – Ответственный) в своей работе должен руководствоваться настоящей инструкцией и следующими основными законодательными и нормативными правовыми актами Российской Федерации:

- Федеральный закон Российской Федерации от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и защите информации»;

- Федеральный закон Российской Федерации от 27.07.2006 № 152-ФЗ «О персональных данных»;

- Постановление Правительства Российской Федерации от 01 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

- Постановление Правительства Российской Федерации от 15 сентября 2008 года № 687 «Об утверждении Положения об особенностях обработки персональных

данных, осуществляемой без использования средств автоматизации»;

- Приказ ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;

- Приказ ФСБ России от 10 июля 2014 г. N 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности»;

- локальные акты Организации.

1.4. Основные понятия и термины, используемые в настоящей Инструкции, применяются в значениях, определенных статьей 3 Федерального закона Российской Федерации от 27.07.2006 № 152-ФЗ «О персональных данных».

1.5. Ответственный – лицо, выполняющее функции по установке, настройке и сопровождению программных и технических средств, входящих в состав ИС, в том числе средств защиты информации (далее – СЗИ).

1.6. Ответственный получает указания непосредственно от руководителей отделов, в которых обрабатываются КИ.

2. Обязанности:

1) знать и выполнять требования действующих нормативных правовых актов, Российской Федерации, а также локальных актов Организации, регламентирующих деятельность по защите КИ;

2) знать требования к защите КИ, организационные и технические меры по обеспечению безопасности КИ при их обработке в ИС;

3) устанавливать, настраивать и сопровождать СЗИ ИС;

4) управлять СЗИ ИС и поддерживать их функционирование;

5) резервировать СЗИ ИС или осуществлять контроль за их резервированием, восстанавливать СЗИ ИС;

6) участвовать в приемке в эксплуатацию новых СЗИ ИС;

7) назначать права доступа пользователей к объектам доступа (программам, файлам, каталогам, портам и устройствам ввода-вывода) согласно надлежащим образом оформленным разрешениям;

8) генерировать ключи, личные идентификаторы для пользователей ИС;

9) формировать и управлять списком необходимых реквизитов и значениями атрибутов объектов и субъектов доступа;

10) контролировать целостность эксплуатируемого в ИС программного обеспечения, в том числе самих СЗИ, их параметров и режимов с целью недопущения и выявления несанкционированных модификаций;

11) контролировать физическую сохранность оборудования ИС, СЗИ ИС, эксплуатационной и технической документации СЗИ ИС, носителей информации, носителей программных СЗИ ИС;

12) не допускать установку, использование, хранение и распространение в ИС программных средств, не связанных с выполнением пользователями ИС трудовых (служебных) обязанностей;

13) осуществлять текущий, после сбоев, и периодический (не реже 3 раз в год) контроль работоспособности СЗИ ИС;

14) контролировать работу пользователей в сетях общего пользования и (или) международного информационного обмена;

15) выявлять подозрительные действия пользователей и попытки несанкционированного доступа к КИ, обрабатываемой в ИС, путем анализа системных журналов безопасности в ИС. В случае обнаружения или выявления таких попыток, немедленно докладывать ответственному за организацию обработки КИ;

16) консультировать пользователей ИС в части правил работы с СЗИ, вопросов защиты информации в ИС;

17) осуществлять ведение журналов:

– Журнал учета машинных носителей конфиденциальной информации, в том числе персональных данных;

– Журнал учета СЗИ (приложение № 1 к настоящей инструкции);

– Журнал учета СКЗИ (приложение № 2 к настоящей инструкции).

18) принимать меры по реагированию, в случае возникновения внештатных и аварийных ситуаций, с целью ликвидации их последствий;

19) предоставлять ответственному за организацию обработки КИ, отчет о состоянии защиты ИС, своевременно докладывать о внештатных ситуациях, выявленных нарушениях требований по защите КИ;

20) в случае отказа технических средств или программного обеспечения ИС, в том числе средств защиты принимать меры по их своевременному восстановлению и выявлению причин, приведших к отказу.

21) периодически (раз в месяц) контролировать ведение электронного журнала безопасности и соответствие отраженных в нем полномочий сотрудников оператора их должностным обязанностям (для 1-го уровня защищенности).

3. Права:

1) требовать от пользователей ИС выполнения законодательных, нормативных правовых актов Российской Федерации, а также локальных актов Организации в части обработки и защиты КИ;

2) приостанавливать обработку КИ в ИС в случаях угрозы их безопасности при нарушении установленной технологии обработки КИ и нарушения работы СЗИ ИС;

3) вносить предложения по изменению содержания локальных актов Организации с целью соответствия реальным условиям или в случае изменения законодательных и нормативных правовых актов;

4) докладывать непосредственному руководителю о нарушениях или невыполнении пользователями требований по обеспечению безопасности КИ.

4. Ответственность

Лицо, ответственное за обеспечение безопасности КИ в ИС несет ответственность за ненадлежащее исполнение или неисполнение своих обязанностей, предусмотренных настоящей Инструкцией, в пределах, определенных действующим законодательством Российской Федерации.

С инструкцией ознакомлен:

Лицо, ответственное за обеспечение безопасности конфиденциальной информации, в том числе персональных данных

_____ _____

(подпись) (фамилия и инициалы)

Приложение № 1
к должностной инструкции
ответственного за обеспечение
безопасности конфиденциальной
информации, в том числе

_____

(наименование организации)

ЖУРНАЛ
учета средств защиты информации

Дата начала **«___» _____ 201__**
Дата окончания **«___» _____ 201__**

ПОРЯДОК ЗАПОЛНЕНИЯ ЖУРНАЛА УЧЕТА

1. Журнал учета заполняется шариковой ручкой синего цвета.

2. Не допускается написание более одной строчки текста в строке журнала, т.е. текст переносится на следующую строку журнала.

3. № пункта, номера – необходимо проставлять арабскими цифрами без точки на конце.

4. Наименование средств писать полностью без сокращений.

5. Формат даты: ЧЧ. ММ. ГГ.

6. Для исправления ошибок необходимо перечеркнуть (одной чертой) неправильное написание, вписать правильное и поставить подпись должностного лица организации, заверив ее печатью организации, с указанием даты исправления. Не допускается исправления ошибок с помощью корректирующего средства.

№ п/п	Регистрационный номер	Наименование	Сведения об установке средства защиты информации			Сведения об изъятии/удалении средства защиты информации			Примечание
			Дата установки	Место установки (использования)	Ф.И.О. производившего установку, подпись	Дата изъятия/ удаления	Ф.И.О. производившего изъятие/удаление, подпись	Причина изъятия/ удаления	

№ п/п	Регистрационный номер	Наименование	Сведения об установке средства защиты информации			Сведения об изъятии/удалении средства защиты информации			Примечание
			Дата установки	Место установки (использования)	Ф.И.О. производившего установку, подпись	Дата изъятия/ удаления	Ф.И.О. производившего изъятие/удаление, подпись	Причина изъятия/ удаления	

Приложение № 2
к должностной инструкции
ответственного за обеспечение
безопасности конфиденциальной
информации, в том числе персональных
данных

Экз. №___

_____

(наименование организации)

ЖУРНАЛ
поэкземплярного учета средств криптографической защиты информации (СКЗИ), эксплуатационной и технической документации к ним, ключевых документов

Ответственный за ведение Журнала /_____/

Дата начала «___» _____ 201__
Дата окончания «___» _____ 201__

№ п/п	Наименование СКЗИ, эксплуатационной и технической документации к ним, ключевых документов	Серийные номера СКЗИ, эксплуатационной и технической документации к ним, номера серий ключевых документов	Номера экземпляров (криптографические номера) ключевых документов	Отметка о получении		Отметка о выдаче	
				От кого получены	Дата и номер сопроводи-тельного письма	Ф.И.О. пользователя СКЗИ	Дата и расписка в получении
1	2	3	4	5	6	7	8

Отметка о подключении (установке СКЗИ)			Отметка об изъятии СКЗИ из аппаратных средств, уничтожении ключевых документов			Примечание
Ф.И.О. сотрудников органа криптографической защиты, пользователя СКЗИ, произведших подключение (установку)	Дата подключения (установки) и подписи лиц, произведших подключение (установку)	Номера аппаратных средств, в которые установлены или к которым подключены СКЗИ	Дата изъятия (уничтожения)	Ф.И.О. сотрудников органа криптографической защиты, пользователя СКЗИ, производивших изъятие (уничтожение)	Номер акта или расписка об уничтожении	
9	10	11	12	13	14	15