МУНИЦИПАЛЬНОЕ КАЗЕННОЕ УЧРЕЖДЕНИЕ
«ЦЕНТР БУХГАЛТЕРСКОГО
ОБЕСПЕЧЕНИЯ МУНИЦИПАЛЬНЫХ УЧРЕЖДЕНИЙ ГОРОДА
ПЯТИГОРСКА»

ПРИКАЗ

29.12.2017 № 44

Об утверждении Регламента
учета средств защиты информации,
эксплуатационной и технической
документации к ним, электронных
носителей персональных данных

В целях исполнения Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» и в соответствии с пунктом 14 «Требований к защите персональных данных при их обработке в информационных системах персональных данных», утвержденных постановлением Правительства РФ от 1 ноября 2012 г. № 1119,-

ПРИКАЗЫВАЮ:

1. Утвердить Регламент учета средств защиты информации, эксплуатационной и технической документации к ним, электронных носителей персональных данных.

2. Контроль исполнения настоящего приказа оставляю за собой.

3. Настоящий приказ вступает в силу с момента его подписания.

Начальник Н.С. Даниелян

УТВЕРЖДАЮ

Начальник МКУ «ЦБО»

Н.С. Даниелян

РЕГЛАМЕНТ
учета средств защиты информации, эксплуатационной и технической документации к ним, электронных носителей персональных данных МКУ «ЦБО»

1. Общие положения

Регламент учета СЗИ, эксплуатационной и технической документации к ним, электронных носителей персональных данных устанавливает:

- порядок учета, ввода в эксплуатацию и изъятия из употребления средств, используемых для обеспечения безопасности ПДн при их обработке в ИСПДн;
- порядок учета и хранения электронных носителей информации, содержащих ПДн.

Требования настоящего Регламента распространяются на всех должностных лиц, допущенных к обработке ПДн.

2. Порядок учета и хранения средств защиты информации

Используемые или хранимые оператором СЗИ, эксплуатационная и техническая документация к ним подлежат учету в журнале поэкземплярного учета СЗИ, эксплуатационной и технической документации к ним (см. приложение к настоящему Регламенту).

Учет СЗИ, эксплуатационной и технической документации к ним осуществляется ответственным за обеспечение безопасности ПДн.

Программные средства учитываются совместно с аппаратными средствами, с которыми осуществляется их штатное функционирование. Если аппаратные или аппаратно-программные СЗИ подключаются к системной шине или к одному из внутренних интерфейсов аппаратных средств, то такие СЗИ учитываются также совместно с соответствующими аппаратными средствами.

Все экземпляры СЗИ, эксплуатационная и техническая документация к ним должны выдаваться пользователям СЗИ, несущим персональную ответственность за их сохранность под роспись в соответствующем журнале.

Эксплуатационная и техническая документация, а также электронные носители с инсталляционными файлами СЗИ должны содержаться в хранилищах

(шкафах, ящиках, сейфах и др.), исключающих бесконтрольный доступ к ним, а также их непреднамеренное уничтожение.

Аппаратные средства, с которыми осуществляется штатное функционирование СЗИ, должны быть оборудованы средствами контроля за их вскрытием (опечатаны, опломбированы). Место опечатывания (опломбирования) должно быть таким, чтобы его можно было визуально контролировать.

СЗИ изымаются из употребления по решению ответственного за обеспечение безопасности ПДн, при этом вносятся необходимые изменения в журнал поэкземплярного учета средств защиты информации, эксплуатационной и технической документации к ним.

СЗИ считаются изъятыми из употребления, если исполнена предусмотренная эксплуатационной и технической документацией процедура удаления программного обеспечения СЗИ, и они полностью отключены от аппаратных средств.

3. Порядок учета электронных носителей персональных данных

Учет носителей ПДн осуществляется ответственным за обеспечение безопасности ПДн.

При смене ответственного за обеспечение безопасности ПДн, составляется акт приема-сдачи носителей ПДн и всех журналов учета, который утверждается начальником управления образования.

Ответственный за обеспечение безопасности ПДн выдает носители ПДн только сотрудникам, имеющим допуск к ПДн.

Перед записью ПДн на носитель, пользователь передает его ответственному за обеспечение безопасности ПДн

При получении носителей ПДн из сторонних организаций они передаются ответственному за обеспечение безопасности ПДн для учета, после чего могут быть выданы пользователям для работы.

На носителях ПДн проставляются следующие реквизиты:

- регистрационный номер;
- дата и роспись ответственного за обеспечение безопасности ПДн.

Учет носителей ПДн производится в «Журнале учета электронных носителей персональных данных».

Движение (выдача и возврат) носителей с ПДн должно отражаться в соответствующем «Журнале учета выдачи и возврата электронных носителей персональных данных». Выдача носителей ПДн сотруднику производится под его личную роспись.

Передача носителей с ПДн другим сотрудникам, имеющим допуск к ПДн, производится только через ответственного за обеспечение безопасности ПДн с обязательной записью в «Журнале учета выдачи и возврата электронных носителей персональных данных».

Листы журналов нумеруются, прошиваются и опечатываются.

4. Порядок хранения электронных носителей персональных данных

Носители информации с ПДн должны храниться в служебных помещениях, в надежно запираемых и опечатываемых шкафах (сейфах). При этом должны быть созданы надлежащие условия, обеспечивающие их физическую сохранность.

Запрещается выносить носители с ПДн из служебных помещений без согласования с ответственным за обеспечение безопасности ПДн.

Сотрудники должны после окончания работы запирать полученные носители ПДн в личный сейф, в случае его отсутствия сдавать ответственным за обеспечение безопасности ПДн д.

Проверка наличия носителей ПДн проводится один раз в год комиссией. В ходе ревизии комиссия определяет перечень носителей ПДн, которые (информацию на которых) можно уничтожить.

Проверка наличия носителей ПДн при необходимости может проводиться ответственным за обеспечение безопасности ПДн или специально уполномоченным лицом.

Уничтожение носителей ПДн (информации на них), утративших свое практическое значение и не имеющих исторической ценности, производится по акту. В учетных журналах об этом делается отметка со ссылкой на соответствующий акт.

5. Ответственность за выполнение регламента

На пользователей ИСПДн, ответственных за обеспечение безопасности ПДн, возлагается персональная ответственность за выполнение всех обязанностей, возложенных на них в настоящем Регламенте.

За правонарушения, совершенные в процессе своей деятельности должностные лица несут ответственность в пределах, определенных действующим законодательством Российской Федерации.

Приложение №1
к Регламенту учета средств защиты информации, эксплуатационной и технической документации к ним, электронных носителей персональных данных

Форма журнала поэкземплярного учета средств защиты информации, эксплуатационной и технической документации к ним

№ п/п	Наименование средства защиты информации/ эксплуатационной, технической документации	Регистрационные номера средства защиты информации/ эксплуатационной, технической документации	Отметка о подключении (установке) средства защиты информации		Отметка об изъятии средства защиты информации из аппаратных средств		Примечание
			Ф.И.О. лица, производившего подключение (установку) средства защиты информации, дата, подпись	Номера аппаратных средств, в которые установлены или к которым подключены средства защиты информации	Ф.И.О. лица, производившего изъятие средства защиты информации, дата, подпись	Номер акта или расписка об уничтожении	
1	2	3	4	5	6	7	8

УТВЕРЖДАЮ
Начальник МКУ «ЦБО»

Н.С.Даниелян

Инструкция пользователя информационной системы персональных данных

1. Общие положения

1.1. Настоящая инструкция определяет основные обязанности, права и ответственность пользователей информационной системы персональных данных в МКУ «ЦБО» (далее – Организация или Оператор).

1.2. Пользователями информационной системы персональных данных, являются работники Организации, допущенные к работе в информационной системе персональных данных в установленном порядке на основании приказа Организации (далее – Пользователь).

1.3. Пользователь в своей работе должен руководствоваться настоящей инструкцией и следующими основными законодательными и нормативными правовыми актами Российской Федерации:

– Трудовой кодекс Российской Федерации (ст. 65, ст.85-90);

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

– Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» (далее – Федеральный закон № 152-ФЗ);

– Постановление Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

– локальные акты Организации в сфере обработки персональных данных.

1.4. Основные понятия и термины, используемые в настоящей инструкции, применяются в значениях, определенных статьей 3 Федерального закона № 152-ФЗ.

1.5. Пользователь получает указания от своего непосредственного руководителя и подотчетно ему.

2. Обязанности пользователя.

2.1. Знать и выполнять требования действующих нормативных правовых актов Российской Федерации, а также локальных актов, правил и инструкций Организации, регламентирующих деятельность по обработке и защите персональных данных в том числе:

– Правил обработки персональных данных;

– Порядка доступа работников в помещения, в которых ведется обработка персональных данных;

– Правил организации режима обеспечения безопасности помещений, в которых размещена информационная система;

– Правил доступа к персональным данным, обрабатываемым в информационной системе.

2.2. Знать и выполнять установленные требования по учету, хранению и использованию носителей персональных данных, обеспечению безопасности персональных данных.

2.3. Соблюдать установленную технологию обработки персональных данных.

2.4. Обеспечивать конфиденциальность персональных данных, ставших известными в результате обработки персональных данных.

2.5. Соблюдать требования парольной политики.

2.6. При возникновении внештатных и аварийных ситуаций незамедлительно докладывать непосредственному руководителю и системному администратору информационных систем для приятия необходимых мер с целью ликвидации их последствий и возможного ущерба.

2.7. Пользователю ЗАПРЕЩАЕТСЯ:

– подключать к техническим средствам информационной системы персональных данных (далее – ИС) нештатные устройства (флэш-диски, карты памяти, жесткие диски и др.);

– самостоятельно вносить изменения в состав, конфигурацию и размещение технических средств ИС;

– самостоятельно вносить изменения в состав, конфигурацию и настройку программного обеспечения, установленного в ИС;

– разрешать работу со средствами ИС лицам, не допущенным к обработке персональных данных в установленном порядке;

– оставлять незаблокированными автоматизированные рабочие места при отсутствии на рабочем месте;

– сообщать и передавать третьим лицам личные пароли и атрибуты доступа к ресурсам ИС.

3. Права пользователя.

3.1. Пользователь имеет право обращаться к ответственному за организацию обработки персональных данных по любым организационным вопросам, касающимся обработки и защиты персональных данных в ИС (выполнение режимных мер, установленной технологии обработки информации, инструкций и других документов по обеспечению информационной безопасности персональных данных).

3.2. Пользователь имеет право обращаться к системному администратору информационных систем с просьбой об оказании консультаций и технической помощи по обеспечению безопасности обрабатываемой в ИС информации, а также по вопросам эксплуатации установленных средств защиты информации.

3.3. Пользователь имеет право обращаться к системному администратору с просьбой об оказании консультаций и технической помощи по использованию установленных в ИС программных и технических средств, в том числе средств защиты информации.

4. Ответственность пользователя.

Пользователь информационной системы персональных данных несет ответственность за ненадлежащее исполнение или неисполнение своих обязанностей, предусмотренных настоящей инструкцией, в пределах, определенных действующим законодательством Российской Федерации.

С инструкцией ознакомлены

подпись	фамилияи инициалы	дата