



Инструкция
по порядку учета, хранения и уничтожения съёмных носителей
информации в муниципальном автономном учреждении
дополнительного образования «Детско-юношеский центр»

Общие положения

1.1. Администратор безопасности информации – пользователь, уполномоченный выполнять некоторые действия (имеющий полномочия) по администрированию (управлению) системой защиты информации в соответствии с установленной ролью.

1.2. Безопасность информации [данных] – состояние защищенности информации [данных], при котором обеспечены ее [их] конфиденциальность, доступность и целостность.

1.3. Защищаемая информация – информация, для которой обладателем информации определены характеристики ее безопасности.

1.4. Информационная система – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.

1.5. Информация – сведения (сообщения, данные) независимо от формы их представления.

1.6. Конфиденциальность информации – обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя.

1.7. Несанкционированный доступ (несанкционированные действия) – доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых информационной системой.

1.8. Носитель информации – физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.

1.9. Персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

1.10. Пользователь – лицо, которому разрешено выполнять некоторые действия (операции) по обработке информации в информационной системе или использующее результаты ее функционирования.

1.11. Средство защиты информации – техническое, программное, программно-техническое средство, предназначенное или используемое для защиты информации.

1.12. Техническое средство – аппаратное или программно-аппаратное устройство, осуществляющее формирование, обработку, передачу или прием информации в информационной системе.

2. Общие положения

2.1. Настоящая Инструкция разработана в соответствии с Конституцией Российской Федерации, Трудовым кодексом Российской Федерации, Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», Указом Президента Российской Федерации от 06.03.1997 №188 «Об утверждении перечня сведений конфиденциального характера», Постановлением Правительства Российской Федерации от 01.11.2012 г. № 1119 г. «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

2.2. Настоящая Инструкция устанавливает порядок использования съемных носителей информации при работе в «Сетевой Город. Образование» и Е-услуги. Образование» (далее – информационная система; ИС) Муниципального автономного учреждения дополнительного образования «Детско-юношеский центр» (далее – Организация).

2.3. Действие настоящей Инструкции распространяется на сотрудников Организации, в рамках выполнения своих должностных обязанностей участвующих в обработке информации ограниченного доступа.

2.4. Контроль исполнения требований настоящей Инструкции возлагается на ответственного за защиту информации.

3. Порядок использования носителей информации

3.1. Под использованием носителей информации в ИС понимается их подключение к инфраструктуре ИС с целью обработки, приема/передачи информации между ИС и носителями информации.

3.2. В ИС допускается использование только учтенных носителей информации, которые являются собственностью и подвергаются регулярной ревизии и контролю.

3.3. Носители информации предоставляются сотрудникам по инициативе руководителей структурных подразделений в случаях:

- необходимости выполнения вновь принятым работником своих должностных обязанностей;
- возникновения у сотрудника производственной необходимости.

4. Порядок учета съемных носителей информации

4.1. Все находящиеся на хранении и в обращении съемные носители информации подлежат учёту.

4.2. Каждый съемный носитель с записанной на нем информацией ограниченного доступа должен иметь этикетку, на которой указывается его уникальный учетный номер.

4.3. Учет и выдачу съемных носителей информации осуществляют сотрудники структурных подразделений, на которых возложены функции хранения носителей информации. Факт выдачи съемного носителя фиксируется в журнале учета съемных носителей информации (Приложение № 1) и журнале приема-выдачи защищаемых носителей информации (Приложение № 2).

4.4. Сотрудники получают учтенный съемный носитель от уполномоченного сотрудника для выполнения работ на конкретный срок. При получении делаются соответствующие записи в журнале учета. По окончании работ пользователь сдает съемный носитель для хранения уполномоченному сотруднику, о чем делается соответствующая запись в журнале учета.

5. Порядок обращения со съёмными носителями информации

5.1. При использовании сотрудниками носителей ПДн необходимо:

- 5.1.1.** Соблюдать требования настоящей Инструкции.
- 5.1.2.** Использовать носители информации исключительно для выполнения своих служебных обязанностей.
- 5.1.3.** Ставить в известность администратора безопасности о любых фактах нарушения требований настоящей Инструкции.
- 5.1.4.** Бережно относиться к носителям информации.
- 5.1.5.** Обеспечивать физическую безопасность носителей информации всеми разумными способами.

5.1.6. Извещать администратора безопасности информации о фактах утраты (кражи) носителей информации.

5.2. При использовании носителей информации запрещено:

5.2.1. Использовать носители информации в личных целях.

5.2.2. Передавать носители информации другим лицам (за исключением администраторов ИС).

5.2.3. Хранить съемные носители с информацией ограниченного доступа вместе с носителями открытой информации, на рабочих столах, либо оставлять их без присмотра или передавать на хранение другим лицам;

5.2.4. Выносить съемные носители с информацией ограниченного доступа из служебных помещений для работы с ними на дому и т. д.

5.3. Любое взаимодействие (обработка, прием/передача информации) инициированное сотрудником между ИС и неучтенными (личными) носителями информации, рассматривается как несанкционированное (за исключением случаев, оговоренных с администратором безопасности информации заранее). Администратор безопасности информации оставляет за собой право блокировать или ограничивать использование носителей информации.

5.4. Информация об использовании сотрудником носителей информации в ИС протоколируется и, при необходимости, может быть предоставлена администратором безопасности информации.

5.5. В случае выявления фактов несанкционированного и/или нецелевого использования носителей информации инициализируется служебная проверка, проводимая комиссией, состав которой определяется ответственным за защиту информации.

5.6. По факту выясненных обстоятельств составляется акт расследования инцидента и передается администратору безопасности информации для принятия мер согласно локальным нормативным актам и действующему законодательству.

5.7. Информация, хранящаяся на носителях информации, подлежит обязательной проверке на отсутствие вредоносного ПО.

5.8. При отправке или передаче информации ограниченного доступа адресатам на съемные носители записываются только предназначенные адресатам данные. Отправка информации ограниченного доступа адресатам на съемных носителях осуществляется в порядке, установленном для документов для служебного пользования.

5.9. Вынос съемных носителей информации для непосредственной передачи адресату осуществляется только с письменного разрешения администратора безопасности информации.

5.10. В случае утраты или уничтожения съемных носителей информации либо разглашении содержащихся в них сведений немедленно ставится в известность администратор безопасности информации. На утраченные носители составляется акт. Соответствующие отметки вносятся в журналы учета бумажных и съемных носителей информации.

5.11. Съемные носители информации, пришедшие в негодность, или отслужившие установленный срок, подлежат уничтожению. Уничтожение съемных носителей с персональными данными осуществляется уполномоченной комиссией. По результатам уничтожения носителей составляется акт (Приложение № 3).

5.12. В случае увольнения или перевода работника в другое структурное подразделение, предоставленные носители информации изымаются.

6. Ответственность

6.1. Работники, нарушившие требования настоящей Инструкции, несут ответственность в соответствии с действующим законодательством и локальными нормативными актами.

Регистрационный № _____

ЖУРНАЛ УЧЕТА ЗАЩИЩАЕМЫХ НОСИТЕЛЕЙ ИНФОРМАЦИИ

Начат «___» _____ 20__ г.

Окончен «___» _____ 20__ г.

На _____ листах

(должность руководителя)

(подпись)
М.П.

(Фамилия И.О.)

№ п/п	Регистрационный номер	Тип защищаемого носителя информации	Дата	Назначение (содержимое) носителя	Сведения об уничтожении носителя	Ответственное должностное лицо (ФИО)
1						
2						
3						
4						
5						
6						
7						
8						
9						
10						
11						

Приложение № 2
к Инструкции по порядку учета, хранения и уничтожения съёмных носителей информации

ЖУРНАЛ ПРИЕМА-ВЫДАЧИ ЗАЩИЩАЕМЫХ НОСИТЕЛЕЙ ИНФОРМАЦИИ

Начат «___» _____ 20__ г.

Окончен «___» _____ 20__ г.

На _____ листах

(должность руководителя)

(подпись)
М.П.

(Фамилия И.О.)

№ п/п	Регистрационный номер/дата	Расписка в получении (ФИО, подпись, дата)	Расписка о возврате (ФИО, подпись, дата)
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			
11			

Приложение № 3
к Инструкции
по порядку учета,
хранения и уничтожения
съёмных носителей информации

УТВЕРЖДАЮ

«__» _____ 20__ г.

**Типовая форма акта
об уничтожении носителей персональных данных**

В связи с достижением цели обработки персональных данных (ПДн) к уничтожению отобраны следующие бумажные носители персональных данных:

№ п/п	Учетный номер носителя	Цель обработки ПДн	Дата начала обработки ПДн	Дата окончания обработки ПДн
1				
2				
3				

ПДн должны быть уничтожены со следующих материальных носителей:

№ п/п	Учетный номер носителя	Цель обработки ПДн	Дата начала обработки ПДн	Дата окончания обработки ПДн
1				
2				
3				

Всего подлежит уничтожению _____ бумажных носителей ПДн.

Уничтожение информации необходимо с _____ материальных носителей.

Проверка правильности включения материальных носителей ПДн в Акт проведена.

Бумажные носители ПДн полностью уничтожены путем

_____ ПДн с материальных носителей уничтожены путем

СОГЛАСОВАНО

Ответственный за организацию обработки и обеспечение безопасности
ПДн

_____	_____	_____
(ФИО)	(подпись)	(дата)

ОТМЕТКА О ВЫПОЛНЕНИИ

Ответственный за выполнение

_____	_____	_____
(ФИО, должность)	(подпись)	(дата)