

УТВЕРЖДЕНО:

Заведующий МБДОУ «Детский сад
общеразвивающего вида №47»



Кашапова З.Г.
201 8 года

Инструкции по порядку учета и хранению съемных носителей конфиденциальной информации (персональных данных)

в МБДОУ «Детский сад общеразвивающего вида №47» НМР РТ

1. Общие положения

1.1. Настоящее Положение разработано в соответствии с Федеральным законом № 149-ФЗ от 27.07.2006 г. «Об информации, информационных технологиях и о защите информации», ГОСТ Р ИСО/МЭК 17799-2005 «Практические правила управления информационной безопасностью» и другими нормативными правовыми актами, и устанавливает порядок использования носителей информации.

1.2. Действие настоящего Положения распространяется на сотрудников МБДОУ «Детский сад общеразвивающего вида №47» НМР РТ (далее-ДОУ) и третью сторону.

2. Основные термины, сокращения и определения

1. **Администратор ИС** – технический специалист, обеспечивает ввод в эксплуатацию, поддержку и последующий вывод из эксплуатации ПО и оборудования вычислительной техники.
2. **АРМ** – автоматизированное рабочее место пользователя (ПК с прикладным ПО) для выполнения определенной производственной задачи.
3. **ИБ** – информационная безопасность – комплекс организационно-технических мероприятий, обеспечивающих конфиденциальность, целостность и доступность информации.
4. **ИС** – информационная система – система, обеспечивающая хранение, обработку, преобразование и передачу информации с использованием компьютерной и другой техники.
5. **Носитель информации** – любой материальный объект, используемый для хранения и передачи электронной информации.
6. **Паспорт ПК** – документ, содержащий полный перечень оборудования и программного обеспечения АРМ.

7. **ПК** – персональный компьютер.
8. **ПО** – Программное обеспечение вычислительной техники.
9. **ПО вредоносное** – ПО или изменения в ПО, приводящие к нарушению конфиденциальности, целостности и доступности критичной информации.
10. **ПО коммерческое** – ПО сторонних производителей (правообладателей). Предоставляется в пользование на возмездной (платной) основе.
11. **Пользователь** – работник Организации, использующий мобильные устройства и носители информации для выполнения своих служебных обязанностей.

3. Порядок использования носителей информации

3.1. Под использованием носителей информации в ИС ДОУ 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 ДОУ и подвергаются регулярной ревизии и контролю.

3.3. К предоставленным носителям конфиденциальной информации предъявляются те же требования ИБ, что и для стационарных АРМ (целесообразность дополнительных мер обеспечения ИБ определяется администраторами ИС).

3.4. Носители конфиденциальной информации предоставляются сотрудникам ДОУ в случаях:

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

4. Порядок учета, хранения и обращения со съемными носителями конфиденциальной информации (персональных данных), твердыми копиями и их утилизации

4.1. Все находящиеся на хранении и в обращении съемные носители с конфиденциальной информацией (персональными данными) в ДОУ подлежат учёту.

4.2. Каждый съемный носитель с записанными на нем конфиденциальной информацией (персональными данными) должен иметь этикетку, на которой указывается его уникальный учетный номер.

4.3. Учет и выдачу съемных носителей конфиденциальной информации (персональных данных) осуществляют сотрудники структурных подразделений, на

которых возложены функции хранения носителей персональных данных. Факт выдачи съемного носителя фиксируется в журнале учета съемных носителей конфиденциальной информации.

4.4. Сотрудники ДОУ 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.

4.5. При использовании сотрудниками носителей конфиденциальной информации необходимо:

- соблюдать требования настоящей Инструкции.
- использовать носители информации исключительно для выполнения своих служебных обязанностей.
- ставить в известность администратора ИС о любых фактах нарушения требований настоящей Инструкции.
- бережно относиться к носителям конфиденциальной информации.
- обеспечивать физическую безопасность носителей информации всеми разумными способами.
- извещать администратора ИС о фактах утраты (кражи) носителей конфиденциальной информации.

4.6. При использовании носителей конфиденциальной информации запрещено:

- использовать носители конфиденциальной информации в личных целях.
- передавать носители конфиденциальной информации другим лицам (за исключением администраторов ИС).
- хранить съемные носители с конфиденциальной информацией (персональными данными) вместе с носителями открытой информации, на рабочих столах, либо оставлять их без присмотра или передавать на хранение другим лицам;
- выносить съемные носители с конфиденциальной информацией (персональными данными) из служебных помещений для работы с ними на дому и т. д.

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

4.6. Информация об использовании сотрудником носителей информации в ИС протоколируется и, при необходимости, может быть предоставлена Руководителю ДОУ.

4.7. В случае выявления фактов несанкционированного и/или нецелевого использования носителей конфиденциальной информации инициализируется служебная проверка, проводимая комиссией, состав которой определяется Руководителем органа исполнительной власти.

4.8. По факту выясненных обстоятельств составляется акт расследования инцидента и передается Руководителю ДОУ для принятия мер согласно локальным нормативным актам дошкольного учреждения и действующему законодательству.

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

4.10. При отправке или передаче конфиденциальной информации (персональных данных) адресатам на съемные носители записываются только предназначенные адресатам данные. Отправка конфиденциальной информации (персональных данных) адресатам на съемных носителях осуществляется в порядке, установленном для документов для служебного пользования.

4.11. Вынос съемных носителей конфиденциальной информации (персональных данных) для непосредственной передачи адресату осуществляется только с письменного разрешения руководителя ДОУ.

4.12. В случае утраты или уничтожения съемных носителей конфиденциальной информации (персональных данных) либо разглашении содержащихся в них сведений немедленно ставится в известность заведующий ДОУ. На утраченные носители составляется акт. Соответствующие отметки вносятся в журналы учета съемных носителей конфиденциальной информации (персональных данных).

4.13. Съемные носители конфиденциальной информации (персональных данных), пришедшие в негодность, или отслужившие установленный срок, подлежат уничтожению. Уничтожение съемных носителей с конфиденциальной информацией осуществляется «уполномоченной комиссией». По результатам уничтожения носителей составляется акт по прилагаемой форме

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

5. Ответственность

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

