

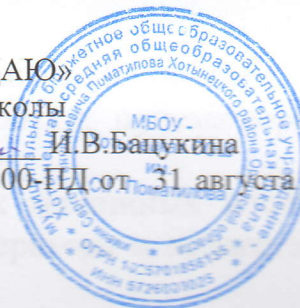
Принят
на заседании педагогического совета
Протокол №1 от 30 августа 2022 года

«УТВЕРЖДАЮ»

Директор школы

И.В. Бабукина И.В. Бабукина

Приказ № 500-ПД от 31 августа 2022
года



Порядок
учета машинных носителей информации с
персональными данными
муниципального бюджетного
общеобразовательного учреждения –
Хотынецкой средней общеобразовательной школы
имени Сергея Геннадьевича Поматилова
Хотынецкого района Орловской области

1. Общие положения

1.1. Настоящий Порядок разработан в соответствии с Федеральным законом № 149-ФЗ от 27.07.2006 г. «Об информации, информационных технологиях и о защите информации», Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных», ГОСТ Р ИСО/МЭК 17799-2005 «Практические правила управления информационной безопасностью» и другими нормативными правовыми актами, и устанавливает порядок учета и использования машинных носителей информации для обработки персональных данных.

2. Основные термины, сокращения и определения

Администратор информационной системы – технический специалист, обеспечивает ввод в эксплуатацию, поддержку и последующий вывод из эксплуатации программного обеспечения (ПО) и оборудования вычислительной техники.

АРМ – автоматизированное рабочее место пользователя (персональный компьютер (ПК) с прикладным ПО) для выполнения определенной производственной задачи.

ИБ – информационная безопасность – комплекс организационно-технических мероприятий, обеспечивающих конфиденциальность, целостность и доступность информации.

ИС – информационная система – система, обеспечивающая хранение, обработку, преобразование и передачу информации с использованием компьютерной и другой техники.

Машинный носитель информации – материальный носитель, используемый для хранения и передачи электронной информации.

ПК – персональный компьютер.

ПО – программное обеспечение вычислительной техники.

ПО вредоносное – ПО или изменения в ПО, приводящие к нарушению конфиденциальности, целостности и доступности критичной информации.

Пользователь – работник Оператора, использующий ПК и носители информации для выполнения своих служебных обязанностей.

3. Порядок использования машинных носителей информации

- 3.1. Под использованием машинных 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 машинных носителей информации, которые являются собственностью Оператора и подвергаются регулярной ревизии и контролю.
- 3.3. К машинным носителям конфиденциальной информации предъявляются те же требования ИБ, что и для стационарных АРМ (целесообразность дополнительных мер обеспечения ИБ определяется администраторами ИС).
- 3.4. Машинные носители конфиденциальной информации предоставляются по инициативе Руководителей структурных подразделений в случаях: необходимости выполнения вновь принятым Пользователем своих должностных обязанностей; возникновения у Пользователя производственной необходимости.

4. Порядок учета, хранения и обращения со съемными машинными носителями конфиденциальной информации (персональных данных)

- 4.1. Все находящиеся на хранении и в обращении съемные машинные носители с конфиденциальной информацией (персональными данными) подлежат учёту.
- 4.2. Каждый съемный машинный носитель с записанной на нем конфиденциальной информацией (персональными данными) должен иметь этикетку, на которой указывается его уникальный учетный номер.
- 4.3. Учет и выдачу съемных машинных носителей конфиденциальной информации (персональных данных) осуществляют уполномоченные сотрудники структурных подразделений, на которых возложены функции хранения машинных носителей персональных данных. Факт выдачи съемного машинного носителя исполнителю фиксируется в журнале учета съемных машинных носителей конфиденциальной информации.
- 4.4. Пользователи 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 Пользователями машинных носителей с конфиденциальной информацией (персональными данными) необходимо: соблюдать требования настоящего Порядка; использовать машинные носители информации исключительно для выполнения своих служебных обязанностей; ставить в известность администраторов ИС о любых фактах нарушения требований настоящего Порядка; бережно относиться к машинным носителям конфиденциальной информации (персональных данных); обеспечивать физическую безопасность машинных носителей информации всеми разумными способами; извещать администраторов ИС о фактах утраты (кражи) машинных носителей конфиденциальной информации (персональных данных).
- 4.6. При использовании машинных носителей конфиденциальной информации (персональных данных) запрещается:

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

- 4.7. Любое взаимодействие (обработка, прием/передача информации), инициированное сотрудником между ИС и неучтенными (личными) носителями информации, рассматривается как несанкционированное (за исключением случаев, согласованных с администраторами ИС заранее). Администратор ИС оставляет за собой право блокировать или ограничивать использование машинных носителей информации.
- 4.8. В случае выявления фактов несанкционированного и/или нецелевого использования машинных носителей конфиденциальной информации (персональных данных) инициализируется служебная проверка, проводимая комиссией, состав и полномочия которой определяется приказом Оператора. По факту выясненных обстоятельств составляется акт расследования инцидента и передается руководителю структурного подразделения для принятия мер согласно локальным нормативным актам Оператора и действующему законодательству.
- 4.9. Информация, хранящаяся на машинных носителях конфиденциальной информации (персональных данных), подлежит обязательной проверке на отсутствие вредоносного ПО.
- 4.10. При отправке или передаче конфиденциальной информации (персональных данных) адресатам на съемные машинные носители записываются только предназначенные адресатам данные. Отправка конфиденциальной информации (персональных данных) адресатам на съемных машинных носителях осуществляется в порядке, установленном для документов для служебного пользования.
- 4.11. Вынос съемных машинных носителей конфиденциальной информации (персональных данных) для непосредственной передачи адресату осуществляется только с письменного разрешения руководителя структурного подразделения.
- 4.12. В случае утраты или уничтожения съемных машинных носителей конфиденциальной информации (персональных данных) либо разглашении содержащихся в них сведений немедленно ставится в известность руководитель соответствующего структурного подразделения. 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 в соответствии с «Порядком уничтожения документов и машинных носителей информации, содержащих персональные данные».

- 4.14. В случае увольнения или перевода работника в другое структурное подразделение, предоставленные ему машинные носители конфиденциальной информации (персональных данных) изымаются уполномоченным сотрудником структурных подразделений, на которого возложены функции хранения машинных носителей персональных данных.

5. Ответственность

Пользователи и администраторы информационной системы, нарушившие требования настоящего порядка, несут ответственность в соответствии с действующим законодательством и локальными нормативными актами Оператора.