ПРИЛОЖЕНИЕ № 11
К ПРИЗАЗУ МАОУ «СОШ № 2»
«ОБ УТВЕРЖДЕНИИ ПОЛИТИКИ
ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ»
ОТ 03.10.2023 № 390

ИНСТРУКЦИЯ
ПО ЗАЩИТЕ МАШИННЫХ НОСИТЕЛЕЙ ИНФОРМАЦИИ

1. Введение.

1.1. Настоящая инструкция определяет порядок учета, хранения, выдачи, уничтожения и ограничения использования машинных носителей информации в организации МАОУ «Средняя общеобразовательная школа № 2» (далее – Организация).

1.2. Машинный носитель информации (далее МНИ) – это материальный носитель, используемый для передачи и хранения защищаемой информации (в том числе персональных данных) в электронном виде. Машинные носители информации делятся на съемные и несъемные носители.

1.2.1. Несъемные машинные носители информации являются частью автоматизированного рабочего места (далее АРМ) или сервера и в процессе эксплуатации не предполагают демонтаж.

1.2.2. К съемным носителям относятся любые технические устройства, предназначенные для запоминания информации, оперативно подключаемые к АРМ или серверу в целях записи на них информации из памяти АРМ (или сервера) или считывания с них информации в память АРМ (или сервера).

2. Учет машинных носителей информации.

2.1. Все используемые в информационной системе (далее ИС) машинные носители информации подлежат учёту.

2.2. Учет, хранение и выдачу носителей информации осуществляет администратор безопасности. При увольнении администратора безопасности составляется акт приема-сдачи учетных документов и носителей.

2.3. Учет всех видов и типов носителей информации производится в журнале учета машинных носителей информации (приложение № 1 к настоящей Инструкции).

2.4. На несъемную часть носителей ИС наносится уникальный в пределах Организации учетный номер.

3. Выдача машинных носителей информации.

3.1. Пользователи ИС получают учтенный носитель от администратора безопасности, для выполнения работ на конкретный срок.

3.2. При получении пользователем носителя информации делается соответствующая запись в журнале учета машинных носителей информации.

3.3. По окончании работ или установленного срока использования пользователь ИС сдает носитель информации администратору безопасности, о чем делается соответствующая запись в журнале учета машинных носителей информации.

4. Использование машинных носителей информации.

4.1. На машинные носители информации записываются исключительно информация и программные средства обработки информации, содержащейся в ИС.

4.2. Носители информации, допускающие повторную запись информации, проходят процедуру многократной перезаписи общедоступной информации перед повторным использованием или ремонтом с целью гарантированного уничтожения остаточной информации. Процедуру перезаписи организует и контролирует администратор безопасности.

4.3. Вынос учтенных носителей информации за пределы установленных мест обработки информации допустим только с письменного разрешения администратора безопасности.

4.4. Передача носителей, содержащих информацию, которая обрабатывается в ИС

сторонним организациям или третьим лицам производится по приказу руководителя Организации через администратора безопасности. Администратор безопасности производит в этом случае необходимые отметки в журнале учета машинных носителей информации.

5. Хранение машинных носителей информации.

5.1. Хранение МНИ осуществляется в условиях, препятствующих несанкционированному ознакомлению с информацией, копированию, изменению или уничтожению информации, содержащейся на машинных носителях.

5.2. МНИ хранятся в служебных помещениях, в отведенных для этих целей хранилищах, исключающих несанкционированный доступ к ним.

5.3. Запрещается хранить носители информации на рабочих столах, оставлять их без присмотра, передавать на хранение третьим лицам.

6. Действия при утрате и порче машинных носителей информации.

6.1. В случае утраты или порчи пользователем МНИ, содержащих обрабатываемую в ИС информацию, немедленно ставится в известность администратор безопасности. Администратор безопасности вносит соответствующую запись в журнал учета машинных носителей информации.

6.2. По факту утраты или порчи машинных носителей информации администратор безопасности проводит служебное расследование в установленном порядке.

6.3. Носители, пришедшие в негодность или с истекшим сроком эксплуатации, подлежат уничтожению в установленном порядке.

7. Уничтожение машинных носителей информации.

7.1. Уничтожение машинных носителей информации организует администратор безопасности с составлением Акта уничтожения машинных носителей информации.

7.2. Уничтожение носителей информации производится способом, гарантирующим невозможность восстановления информации, содержавшейся на носителе. Такими способами являются: механическое, электрическое, электромагнитное, химическое или термическое воздействие на носитель, применение специального программного обеспечения для уничтожения информации на носителе. Способ уничтожения выбирается администратором безопасности в зависимости от типа носителя и возможностей Организации.

8. Ограничения и ответственность.

8.1. Всем пользователям ИС запрещено использовать учтенные машинные носители информации для личных целей.

8.2. Пользователям запрещено передавать носители информации кому-либо, осуществлять учет, хранение и выдачу носителей информации, обрабатываемой в ИС. Передача носителей информации осуществляется в порядке, предусмотренном п. 4.5 и п. 4.6 настоящей Инструкции.

8.3. Любое взаимодействие (чтение, запись информации, запуск программного обеспечения) между техническими средствами ИС, СЗИ и неучтенными носителями информации запрещено.

8.4. В случае выявления фактов утраты, несанкционированного и (или) нецелевого использования учтенных носителей информации, использования неучтенных (личных) носителей информации в ИС назначается служебное расследование. По результату расследования и по представлению администратора безопасности, руководитель Организации принимает решение о привлечении пользователя ИС к ответственности согласно локальным нормативным актам Организации и действующему законодательству.

8.5. Сотрудники Организации, несут ответственность за ненадлежащее исполнение или неисполнение своих обязанностей предусмотренных настоящей Инструкцией, в пределах, определенных действующим законодательством Российской Федерации.

9. Заключительные положения.

9.1. Пользователи ИС должны быть предупреждены об ответственности за невыполнение требований настоящей Инструкции и ознакомлены с Инструкцией до начала работы в ИС.

9.2. Обязанность ознакомления пользователей ИС с настоящей Инструкцией лежит на администраторе безопасности.

10. Нормативные и правовые документы.

10.1. Приказ ФСТЭК России от 18.02.2013 года № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

10.2. Приказ ФСТЭК России от 23.03.2017 года № 49 «О внесении изменений в состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденные приказом федеральной службы по техническому и экспортному контролю от 18 февраля 2013 г. № 21, и в требования к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды, утвержденные приказом федеральной службы по техническому и экспортному контролю от 14 марта 2014 г. № 31».

10.3. Постановление Правительства РФ от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».