УТВЕРЖДАЮ

Директор школы _____ И.В. Абрамова

Приказ № 104 от 30.12. 2020 г.

ИНСТРУКЦИЯ

по защите машинных носителей информации

1. Введение.

1.1. Настоящая инструкция предназначена для обеспечения защиты информации, содержащейся в автоматизированной информационной системе МБОУ СОШ № 8 (далее – АИС), в том числе персональных данных (далее – ПДн), при работе с машинными носителями информации.

1.2. Настоящая инструкция определяет порядок учета, хранения, выдачи и уничтожения машинных носителей информации в МБОУ СОШ № 8 (далее – Организация).

1.3. Машинный носитель информации – 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.

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

1.3.2. 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 АИС машинные носители информации (далее – носители) подлежат учёту.

2.2. Учет, хранение и выдачу съемных носителей осуществляет **администратор безопасности**. При увольнении администратора безопасности составляется акт приема-сдачи учетных документов и носителей, который утверждается руководителем Организации.

2.3. Учет всех видов и типов носителей производится в **Журнале учета машинных носителей** информации.

2.4. Несъемные носители учитываются по номерам технической документации на носители.

2.5. Съемные носители учитываются по уникальным номерам, присвоенным им внутри Организации. При этом на съемные носители наносятся присвоенные им номера способом, позволяющим их визуальную идентификацию (например, наклеивание этикетки и т.п.).

3. Организация выдачи съемных машинных носителей.

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

3.2. **Администратор безопасности** обязан проверить наличие у пользователя АИС действующего разрешения к использованию съемных носителей информации в соответствии с **матрицей допуска**.

3.3. При получении носителя делается соответствующая запись в **Журнале учета машинных носителей информации**.

3.4. По окончании работ или установленного срока использования пользователь сдает съемный носитель **администратору безопасности**, о чем делается соответствующая запись в **Журнале учета машинных носителей информации**.

4. Использование и передача съемных машинных носителей информации.

4.1. На машинные носители информации записывается исключительно информация, обрабатываемая в АИС, включая персональные данные, и программные средства обработки информации, содержащейся в АИС.

4.2. Носители информации, допускающие повторную запись информации, проходят процедуру многократной перезаписи не конфиденциальной 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 разрешен только с письменного разрешения **ответственного за защиту информации**.

4.4. Передача носителей информации пользователям АИС производится только через **администратора безопасности**, ведущего учет, хранение и выдачу съемных носителей, в порядке, предусмотренном п.2 настоящей Инструкции.

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

5. Организация хранения машинных носителей информации.

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

5.2. Съемные носители информации хранятся в служебных помещениях, в установленных для этих целей хранилищах исключающих несанкционированный доступ к ним. Места хранения съемных носителей информации определены приказом руководителя Организации.

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

5.4. Несъемные машинные носители информации хранятся в составе АРМ и серверов. Доступ к несъемным носителям информации ограничивается наклейкой этикеток (стикеров) на корпуса АРМ и серверов в местах, исключающих сохранность целостности этикеток (стикеров) при попытке физического доступа к несъемным носителям информации. Контроль целостности этикеток (стикеров) осуществляет администратор безопасности.

6. Действия при утрате и порче машинных носителей информации.

6.1. В случае утраты или порче пользователем носителей, немедленно ставится в известность **администратор безопасности**. Администратор безопасности вносит соответствующую запись в Журнал учета машинных

носителей информации и докладывает об инциденте **ответственному за защиту информации**.

6.2. По факту утраты или порчи машинных носителей информации **ответственным за защиту информации** проводится служебная проверка и действия, определенные порядком расследования инцидентов в соответствии с «Положением по защите информации».

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

7. Уничтожение носителей информации.

7.1. Уничтожение машинных носителей информации организует **администратор безопасности** с предоставлением **Акта уничтожения машинных носителей информации** ответственному за защиту информации. Акт подписывает администратор безопасности и утверждает ответственный за защиту 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.

8. Ограничения и ответственность.

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

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

8.3. В случае выявления фактов утраты, несанкционированного и (или) нецелевого использования учтенных носителей информации, использования неучтенных (личных) носителей информации назначается служебная проверка, и осуществляются действия, определенные порядком расследования инцидентов в соответствии с «Положением по защите информации». По результату расследования инцидента и по представлению **ответственного за защиту информации** руководитель Организации принимает решение о привлечении пользователя АИС к ответственности согласно локальным нормативным актам Организации и действующему законодательству.

8.4. Пользователи АИС несут ответственность, предусмотренную законодательством Российской Федерации и нормативными правовыми актами Организации, за невыполнение требований настоящей Инструкции.

9. Заключительные положения.

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

9.2. Обязанность ознакомления пользователей АИС с настоящей Инструкцией лежит на **ответственном за защиту информации**.

10. Нормативные и правовые документы.

1.1. Методический документ, утвержден ФСТЭК России 11 февраля 2014 года «Меры защиты информации в государственных информационных системах».

1.2. 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».

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

1.4. Постановление правительства РФ от 21.03.2012 **№211** «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами».