



УТВЕРЖДАЮ

Директор школы

 И.В. Абрамова

Приказ № 104 от 30.12.2020 г.

## ИНСТРУКЦИЯ

по управлению программным обеспечением

### 1. Введение.

1.1. Настоящая инструкция предназначена для обеспечения защиты информации, содержащейся в автоматизированной информационной системе МБОУСОШ № 8 (далее – АИС), в том числе персональных данных (далее – ПДн), при установке и обновлении программного обеспечения (далее – ПО) АИС, в том числе ПО средств защиты информации (далее – СЗИ).

1.2. Настоящая инструкция определяет порядок действий **администратора безопасности** и администраторов системных АИС при установке и обновлении программного обеспечения АИС, в том числе ПО СЗИ.

### 2. Порядок установки и обновления программного обеспечения.

2.1. Установку (обновление) ПО АИС осуществляет администратор системной АИС, имеющий необходимые полномочия в соответствии с **матрицей доступа** согласно «Инструкции по управлению доступом к информации».

2.2. Установку (обновление) ПО системы защиты информации АИС, осуществляет **администратор безопасности**.

2.3. **ЗАПРЕЩЕНО** устанавливать (обновлять) ПО, не включенное в **список программного обеспечения, разрешенного к применению в АИС**.

2.4. Установка ПО производится с рабочих копий оригинальных лицензионных дистрибутивных носителей (дискет, компакт дисков и т.п.), полученных законным порядком (путем). Устанавливаемое ПО должно иметь необходимую эксплуатационную документацию и Руководство пользователя.

2.5. Учет дистрибутивных носителей на разрешенное ПО осуществляет **администратор безопасности**. Учет дистрибутивных носителей ПО, разрешенного к применению, производится в **журнале учета дистрибутивных носителей ПО**.

2.6. Устанавливаемое ПО должно быть предварительно проверено (протестировано) **администратором безопасности** на работоспособность, отсутствие опасных функций, а также на совместимость с установленными в АИС программными и техническими средствами, в том числе СЗИ.

2.7. После установки (обновления) программного обеспечения администратор системной АИС и администратор безопасности, каждый в своей части, выполняют необходимые настройки, выполняют тестирование работоспособности и вносят необходимые изменения в эксплуатационную документацию на АИС и ее систему защиты информации.

2.8. Администратор безопасности и администраторы системных АИС, каждый в своей части, проводят оценку изменений в ПО на условия отклонения технологического процесса обработки информации в АИС от ранее принятого. При обнаружении отклонений **администратор безопасности** и администраторы системных АИС, каждый в своей части, докладывают об обнаруженных отклонениях **ответственному за защиту информации**. На основании полученной

информации **ответственный за защиту информации** действует в соответствии с разделами 3 и 4 «Положения о защите информации».

2.9. После обновления ПО **администратор безопасности** заменяет носители с дистрибутивом неактуального программного обеспечения на носители с дистрибутивом обновленного ПО.

### **3. Заключительные положения.**

3.1. Администратор безопасности и администраторы системные АИС должны быть предупреждены об ответственности за действия с программным обеспечением, нарушающие требования настоящей инструкции.

3.2. Администратор безопасности и администраторы системные АИС должны быть ознакомлены с настоящей инструкцией до начала работы с АИС под роспись. Обязанность ознакомления администратора безопасности и администраторов системных АИС с настоящей инструкцией лежит на **ответственном за защиту информации.**

### **4. 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 Составы 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».