УТВЕРЖДАЮ

Директор школы _____ И.В. Абрамова

Приказ № 104 от 30.12.2020 г.

ИНСТРУКЦИЯ

по управлению доступом пользователей к информации

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 разграничении доступа пользователей к ресурсам и информации АИС.

1.2. Настоящая инструкция определяет порядок действий **администратора безопасности** и пользователей информационной системы при разграничении доступа пользователей к ресурсам и информации АИС.

2. Матрица доступа.

2.1. Разграничение доступа к ресурсам и информации АИС осуществляет и контролирует **администратор безопасности** путем настройки программно – технических средств АИС и средств защиты информации (далее – СЗИ) на основании **журнала учета выдачи паролей** и **матрицы доступа**.

2.2. Матрицу доступа и все ее изменения утверждает руководитель МБОУ СОШ № 8 (далее – Организация). Сохранность, конфиденциальность и актуальность матрицы доступа обеспечивает **ответственный за защиту информации**.

2.3. Актуализацию доступа пользователей к ресурсам и информации АИС, а также соответствующие настройки программно – технических средств АИС и СЗИ осуществляет администратор безопасности **периодически, один раз в месяц** или на основании приказов по предоставлению (запрету) доступа пользователям к ресурсам и информации АИС.

3. Порядок предоставления пользователям доступа к ресурсам АИС до прохождения процедур идентификации, аутентификации.

3.1. Вход в АИС и действия с ресурсами АИС до прохождения процедур идентификации, аутентификации разрешен **администратору безопасности** и **администраторам системным** для восстановления АИС после сбоев и отказов технических средств АИС только с письменного разрешения **ответственного за защиту информации**. В разрешении должны быть кратко описаны необходимые действия с ресурсами АИС. Срок действия разрешения заканчивается в момент запуска АИС после восстановления.

3.2. Доступ к ресурсам АИС до момента прохождения процедур идентификации, аутентификации остальным пользователям запрещен.

4. Порядок предоставления удаленного доступа к ресурсам АИС.

4.1. Удаленный доступ пользователей к информационным ресурсам АИС возможен только с помощью технических средств (персональный компьютер, ноутбук, планшет, сотовый телефон) являющихся собственностью Организации и внесенных в журнал **разрешенных устройств удаленного доступа**.

4.2. Выдачу, учет, хранение, настройку программного обеспечения, в том числе СЗИ, установку программного обеспечения и его обновление, антивирусную защиту технических средств удаленного доступа осуществляет администратор безопасности. Все данные по конфигурации и настройкам должны быть записаны в журнал разрешенных устройств удаленного доступа.

4.3. Ограничения для пользователей на использование технических средств удаленного доступа отражены в **матрице доступа**.

4.4. При настройке средств удаленного доступа к ресурсам АИС **администратор безопасности** осуществляет возможность удаленного доступа к ресурсам АИС с автоматической аутентификацией средств удаленного доступа.

4.5. Периодически, не реже одного раза в месяц **администратор безопасности** контролирует состояние средств удаленного доступа и их использование. При обнаружении нарушений в исходной конфигурации и при обнаружении попыток доступа к ресурсам АИС, не включенных в разрешенные для пользователя, устройство и пользователь блокируются, администратор безопасности инициирует расследование инцидента в соответствии с «Положением по защите информации».

4.6. При удаленном доступе к ресурсам АИС должна обеспечиваться безопасность информации, передаваемой по сетям связи общего пользования (международного информационного обмена).

5. Порядок использования в АИС мобильных технических средств.

5.1. К мобильным техническим средствам Организации отнесены все переносные технические устройства, на которые может быть записана и с которых может быть считана информация, содержащаяся в АИС.

5.2. Все мобильные технические средства Организации должны быть учтены и идентифицированы. Учет мобильных технических средств осуществляет **администратор безопасности** в **журнале учета разрешенных мобильных технических средств**.

5.3. Ограничения для пользователей на использование мобильных технических средств отражены в **матрице доступа**.

5.4. Контроль исправности и назначения использования мобильных технических средств, производит **администратор безопасности**. В случае обнаружения неисправности или использования не по назначению, мобильное устройство изымается у пользователя и администратором безопасности предпринимаются действия по устранению инцидента.

5.5. При передаче мобильных технических средств на ремонт или техническое обслуживание **администратор безопасности** полностью очищает их от информации.

6. Порядок взаимодействия с внешними информационными системами.

6.1. Пользователям внешних информационных систем (внешним пользователям) доступ к ресурсам АИС определен **журналом учета выдачи паролей** и **матрицей доступа**.

6.2. **Администратор безопасности** осуществляет процедуру доступа внешних пользователей к ресурсам АИС в соответствии с п.2 настоящей Инструкции.

7. Заключительные положения.

7.1. Все пользователи АИС должны быть предупреждены об ответственности за действия с информационными ресурсами АИС, нарушающие требования настоящей инструкции.

7.2. Пользователи АИС должны быть ознакомлены с настоящей инструкцией до начала работы с АИС под роспись. Обязанность ознакомления сотрудников Организации с настоящей инструкцией лежит на **ответственном за защиту информации**.

8. 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».