ПРИЛОЖЕНИЕ № 10
К ПРИЗАЗУ МАОУ «СОШ № 2»
«ОБ УТВЕРЖДЕНИИ ПОЛИТИКИ
ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ»
ОТ 03.10.2023 № 390

ИНСТРУКЦИЯ
ПО УПРАВЛЕНИЮ ДОСТУПОМ К ИНФОРМАЦИИ

1. Введение.

1.1. Настоящая инструкция предназначена для обеспечения защиты информации, в том числе персональных данных (далее ПДн), содержащейся в информационной системе (далее ИС) «Государственная итоговая аттестация».

1.2. Настоящая инструкция определяет порядок действий ответственного за защиту информации (далее администратора безопасности) и пользователей ИС при разграничении доступа к ресурсам и информации ИС.

2. Матрица доступа.

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

2.2. В организации разработана и утверждена матрица доступа к ресурсам ИС «Государственная итоговая аттестация».

2.3. Сохранность, конфиденциальность и актуальность матрицы доступа обеспечивает администратор безопасности.

2.4. Контроль и актуализацию доступа пользователей к ресурсам и информации ИС «Государственная итоговая аттестация», а также соответствующие настройки программно – технических средств соответствующих СЗИ осуществляет администратор безопасности периодически, один раз в месяц или на основании приказов руководителя организации.

3. Доступ идентификации и аутентификации.

3.1. Вход в ИС и действия с ресурсами ИС до процедур идентификации и аутентификации разрешен только администратору безопасности для восстановления ИС после сбоев и аварий технических средств ИС.

3.2. Доступ к ресурсам ИС до момента прохождения процедур идентификации и аутентификации остальным пользователям запрещен.

4. Удаленный доступ.

4.1. Указанные в п. 4 требования следует соблюдать только в случае, если организация использует или планирует использовать удаленный доступ (через сеть Интернет) к ресурсам ИС.

4.2. Удаленный доступ пользователей к информационным ресурсам ИС возможен только с помощью технических средств (персональный компьютер, ноутбук, планшет, сотовый телефон) являющихся собственностью Организации и внесенных в журнал разрешенных устройств удаленного доступа (приложение №1 к настоящей Инструкции).

4.3. Выдачу, учет, хранение, настройку программного обеспечения, 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.

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

4.5. Периодически, не реже одного раза в месяц администратор безопасности контролирует состояние средств удаленного доступа к ресурсам ИС «Государственная итоговая аттестация» и их использование. При обнаружении нарушений в исходной конфигурации и при обнаружении попыток доступа к ресурсам ИС, не включенных в разрешенные для пользователя, устройство и пользователь блокируются администратором безопасности.

5. Мобильные технические средства.

5.1. Указанные в п.5 требования следует соблюдать только в случае, если организация использует или планирует использовать мобильные технические средства для доступа к ресурсам ИС.

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

5.3. Все мобильные технические средства Организации должны быть учтены и идентифицированы. Учет мобильных технических средств осуществляет администратор безопасности в журнале учета разрешенных мобильных технических средств (приложение № 2 к настоящей Инструкции).

5.4. Контроль исправности и назначения использования мобильных технических средств для доступа к ресурсам ИС «Государственная итоговая аттестация», 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, имеющей отношение к ИС.

6. Заключительные положения.

6.1. Все пользователи ИС должны быть предупреждены об ответственности за действия с получением доступа к ресурсам ИС, нарушающие требования настоящей инструкции.

6.2. Пользователи ИС должны быть ознакомлены с настоящей инструкцией до начала работы с ИС под роспись. Обязанность ознакомления пользователей информационной системы с настоящей инструкцией лежит на администраторе безопасности.

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

7. Нормативные и правовые документы.

7.1. 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».

7.2. 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».

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