ПРИЛОЖЕНИЕ № 9
К ПРИЗАЗУ МАОУ «СОШ № 2»
«ОБ УТВЕРЖДЕНИИ ПОЛИТИКИ
ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ»
ОТ 03.10.2023 № 390

ИНСТРУКЦИЯ
ПО ИДЕНТИФИКАЦИИ И АУТЕНТИФИКАЦИИ

1. Введение.

1.1. Настоящая инструкция определяет в организации «наименование» (далее – Организация) порядок идентификации и аутентификации пользователей информационной системы (далее ИС) «Государственная итоговая аттестация», являющихся сотрудниками Организации, порядок управления аппаратными средствами аутентификации, порядок идентификации/аутентификации внешних пользователей ИС, порядок идентификации/аутентификации устройств, а также обязанности пользователя ИС и администратора безопасности. Настоящая инструкция определяет в организации «наименование» (далее – Организация) порядок идентификации и аутентификации пользователей информационной системы (далее ИС) «Государственная итоговая аттестация», являющихся сотрудниками Организации, порядок управления аппаратными средствами аутентификации, порядок идентификации/аутентификации внешних пользователей ИС, порядок идентификации/аутентификации устройств, а также обязанности пользователя ИС и администратора безопасности.

2. Порядок идентификации и аутентификации пользователя.

2.1. Всем пользователям ИС, являющимся сотрудниками Организации, допущенным в установленном порядке к работе с ИС, присваиваются учетные записи в виде персональных идентификаторов (логины, имена пользователей). Идентификаторы определяют доступ к техническим средствам и информационным ресурсам ИС и системам защиты информации ИС.

2.2. Персональный идентификатор (учетная запись) пользователя создается администратором безопасности и сообщается пользователю. Персональному идентификатору пользователя соответствуют определенные полномочия в ИС и пароли, обеспечивающие аутентификацию (проверку подлинности) в ИС. Права пользователя по доступу к информационным ресурсам ИС, определяется должностью пользователя и матрицей доступа.

Персональные идентификаторы должны быть заблокированы администратором безопасности при превышении времени неиспользования более 90 дней подряд с момента присвоения. Персональные идентификаторы должны быть удалены из ИС при увольнении сотрудника Организации немедленно по окончании последнего сеанса работы сотрудника, а уволенный сотрудник должен быть исключен из числа пользователей ИС.

2.3. Персональные идентификаторы должны быть заблокированы администратором безопасности при превышении времени неиспользования более 90 дней подряд с момента присвоения. Персональные идентификаторы должны быть удалены из ИС при увольнении сотрудника Организации немедленно по окончании последнего сеанса работы сотрудника, а уволенный сотрудник должен быть исключен из числа пользователей ИС.

2.4. При приеме (увольнении) на работу сотрудника Организации или изменении полномочий (временное или бессрочное) действующего сотрудника Организации, изменения в его доступе к информационным ресурсам ИС и генерацию (уничтожение) идентификаторов и паролей, производит администратор безопасности.

2.5. Первичные пароли генерируются администратором безопасности в момент создания идентификаторов и выдаются пользователю под роспись в журнале учета выдачи первичных паролей (приложение № 1 к настоящей Инструкции).

2.6. При первом доступе к ИС пользователь обязан изменить выданный первичный пароль, руководствуясь требованиями к сложности пароля, указанными в настоящей Инструкции (п. 2.8).

В случаях, предусмотренных нормативными документами по защите информации, обрабатываемой в ИС, либо по решению руководителя при особой ценности для Организации сведений, к которым необходимо обеспечить безопасный доступ, помимо паролей используются дополнительные атрибуты доступа – аппаратные идентификаторы (смарт-карты, электронные ключи), которые обеспечивают более надежную многофакторную аутентификацию.

2.7. В случаях, предусмотренных нормативными документами по защите информации, обрабатываемой в ИС, либо по решению руководителя при особой ценности для Организации сведений, к которым необходимо обеспечить безопасный доступ, помимо паролей используются дополнительные атрибуты доступа – аппаратные идентификаторы (смарт-карты, электронные ключи), которые обеспечивают более надежную многофакторную аутентификацию.

2.8. Требования к сложности пароля:

2.8.1. длина пароля должна быть не менее шести символов;

2.8.2. в числе символов пароля обязательно должны присутствовать строчные и прописные буквы, цифры и специальные символы;

2.8.3. пароль не должен включать в себя легко вычисляемые значения символов (имена, фамилии, имена детей или домашних животных, наименования информационных систем, типичных для организации профессиональных терминов, номера телефонов, номера или марки автомобилей, адреса и т. д.), а также общепринятые сокращения (ЭВМ, ЛВС, USER и т.п.); при смене пароля новое значение должно отличаться от предыдущего не менее чем в трех символах; пароль действует не более 90 дней, по истечении которых пользователь обязан заменить его новым.

2.9. Администратор безопасности осуществляет настройку в ИС параметров количества вводов неправильного пароля. Количество вводов неправильного пароля устанавливается равным 3. Разблокирование пароля осуществляет администратор безопасности при обращении к нему пользователя с заблокированным паролем. Администратор безопасности организует настройку в ИС параметров блокирования сеанса доступа при времени бездействия пользователя более 1 часа или по запросу пользователя.

3. Управление аппаратными средствами аутентификации.

3.1. При использовании аппаратных средств аутентификации пользователей (смарт-карты, электронные ключи) выдачу, инициализацию, блокирование и утилизацию аппаратных средств аутентификации организует администратор безопасности.

3.2. Учет выдачи аппаратных средств аутентификации осуществляет администратор безопасности в журнале учета аппаратных средств аутентификации (приложение № 2 к настоящей Инструкции).

4. Идентификация и аутентификация внешних пользователей.

4.1. Присвоение идентификатора и выдача атрибутов аутентификации внешним пользователям ИС, осуществляется администратором безопасности. Учет внешних пользователей, допущенных к обработке информации, осуществляет администратор безопасности.

4.2. Выдачу и смену паролей, учет паролей, учет аппаратных средств аутентификации внешних пользователей, допущенных к обработке информации, организует администратор безопасности по правилам п.2, п.3 настоящей инструкции.

5. Обязанности пользователя.

5.1. Пользователь ИС является частью системы защиты информации и обязан соблюдать следующие правила информационной безопасности:

5.1.1. Помнить свой идентификатор и пароль для ИС.

5.1.2. Обеспечивать сохранность полученных аппаратных идентификаторов. Не предоставлять доступ к личному аппаратному идентификатору никому, кроме администратора безопасности.

5.1.3. Держать свои пароли в тайне, а именно не сообщать, не разглашать и любым другим способом не доводить до чьего-либо сведения (в том числе других сотрудников Организации, в т.ч. руководителей) личные пароли.

5.1.4. Осуществлять ввод паролей только в условиях, исключающих их просмотр.

5.1.5. Не хранить записки-памятки с личными паролями на видном и/или легкодоступном месте: на столе, на мониторе, под клавиатурой, в верхнем ящике стола и т.п.

5.1.6. Своевременно сообщать администратору безопасности о фактах компрометации паролей (когда пароли стали или может быть станут известны еще кому-либо кроме его владельца), об утере или повреждении аппаратного идентификатора и в этих случаях не использовать ИС до специального разрешения администратора безопасности.

6. Обязанности администратора безопасности.

6.1. Администратор безопасности осуществляет организационное и техническое обеспечение процессов создания, использования, изменения и прекращения действия персональных идентификаторов и паролей доступа в ИС, контроль действий пользователей ИС при их работе с персональными идентификаторами и паролями доступа.

6.2. Администратор безопасности обязан:

6.2.1. Создавать, вести учет, закрепление и выдачу пользователям персональных идентификаторов и паролей доступа к техническим средствам и информационным ресурсам ИС.

6.2.2. Обеспечивать смену паролей пользователей с периодичностью не реже одного раза в 90 дней с момента очередной смены.

6.2.3. Свой собственный пароль администратор безопасности должен изменять не реже одного раза в месяц.

6.2.4. Принимать меры по обеспечению внеплановой смены паролей в случае их компрометации или утере аппаратных идентификаторов.

6.2.5. Выявлять и пресекать действия пользователей, которые могут привести к компрометации паролей и (или) утрате аппаратных идентификаторов.

6.3. Действия администратора безопасности при компрометации паролей и утрате аппаратных идентификаторов.

6.3.1. Заблокировать доступ пользователя, владельца скомпрометированного пароля и (или) утраченного идентификатора.

6.3.2. Выявить действия, произведенные в ИС с использованием скомпрометированных персональных идентификаторов и паролей доступа.

6.3.3. Создать и выдать пользователю новый персональный идентификатор и пароль доступа к ИС.

7. Заключительные положения.

7.1. Пользователи ИС должны быть предупреждены об ответственности за действия с персональными идентификаторами и паролями доступа, нарушающие требования настоящей инструкции.

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

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

8. Нормативные и правовые документы.

8.1. 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».

8.2. 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».

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