ПРИЛОЖЕНИЕ №9
УТВЕРЖДЕНО
Приказом «О вводе в действие комплекта организационно-распорядительной документации по организации обработки и защиты персональных данных» МБОУ Сокольская СШ
от «____» _____ 20 _____ г.
№ _____
(М.П.)

Инструкция
по идентификации и аутентификации
пользователей информационных систем персональных данных

Оглавление

1. Общие положения

1.1. Муниципальное бюджетное общеобразовательное учреждение Сокольская средняя школа (далее – Организация) настоящей Инструкции по идентификации и аутентификации пользователей информационных систем персональных данных (далее - Инструкция) определяет порядок идентификации и аутентификации пользователей информационных систем персональных данных «Управление сферой образования в Нижегородской области», «Сведения ГИА», «Сведения о документах об образовании» (далее – информационная система), являющихся работниками Организации, порядок идентификации и аутентификации внешних пользователей информационных систем, порядок управления аппаратными средствами аутентификации, порядок идентификации и аутентификации устройств, а также обязанности пользователей информационных систем и администратора безопасности информационных систем.

1.2. Сокращения, термины и определения:

В настоящей Инструкции используются сокращения, термины и определения, приведенные в таблицах 1 и 2 соответственно.

Таблица 1 – Перечень сокращений

Сокращение	Расшифровка сокращения
ФСТЭК России	Федеральная служба по техническому и экспортному контролю
ПДн	Персональные данные

Таблица 2 – Перечень терминов и определений

Термин	Определение	Источник
Администратор безопасности информационной системы персональных данных (администратор безопасности)	Работник, ответственный за обеспечение безопасности персональных данных в информационной системе персональных данных	
Аутентификация	Действия по проверке подлинности субъекта доступа и/или объекта доступа, а также по проверке принадлежности субъекту доступа и/или объекту доступа предъявленного идентификатора доступа и аутентификационной информации	ГОСТ Р 58833-2020
Аутентификационная информация	Информация, используемая при аутентификации субъекта доступа или объекта доступа.	ГОСТ Р 58833-2020

Термин	Определение	Источник
Идентификация	Действия по присвоению субъектам и объектам доступа идентификаторов и/ или по сравнению предъявляемого идентификатора с перечнем присвоенных идентификаторов	ГОСТ Р 58833-2020
Идентификатор	Признак субъекта доступа или объекта доступа в виде строки знаков (символов), который используется при идентификации и однозначно определяет (указывает) соотнесенную с ними идентификационную информацию	ГОСТ Р 58833-2020
Идентификационная информация	Совокупность значений идентификационных атрибутов, которая связана с конкретным субъектом доступа или конкретным объектом доступа	ГОСТ Р 58833-2020
Информация	Сведения (сообщения, данные) независимо от формы их представления	ГОСТ Р 50922-2006
Информационная система	Совокупность, содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств	ГОСТ Р 51583-2014
Инцидент информационной безопасности	Одно или несколько нежелательных или не ожидаемых событий информационной безопасности, которые со значительной вероятностью приводят к компрометации бизнес-операций и создают угрозы для информационной безопасности	ГОСТ Р ИСО/МЭК 27000
Многофакторная аутентификация	Аутентификация, при выполнении которой используется не менее двух различных факторов аутентификации	ГОСТ Р 58833-2020
Персональные данные	Любая информация, относящаяся прямо или косвенно к определенному или определяемому физическому лицу (субъекту персональных данных)	Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»

1.3. Перечень нормативных правовых актов, на основании которых разработана Инструкция:

Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»,

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

Приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

1.4. Пользователи информационных систем должны быть ознакомлены с настоящей Инструкцией до начала работы в информационных системах под роспись. Обязанность по организации ознакомления пользователей с настоящей Инструкцией возлагается на ответственного за организацию обработки ПДн.

2. Порядок идентификации и аутентификации пользователей

2.1. К работе в информационных системах допускается только определенный круг пользователей.

К внутренним пользователям информационных систем относятся работники Организации, допуск которых осуществляется в минимальном объеме, необходимом для выполнения должностных обязанностей, в соответствии с утвержденными Организацией Перечнями лиц, доступ которых к персональным данным, обрабатываемым в информационных системах в Организации, необходим для выполнения ими служебных (трудовых) обязанностей.

Пользователю информационных систем присваивается уникальная символьная последовательность в виде персонального идентификатора (логин, имя пользователя), которая однозначно его идентифицирует. Идентификаторы определяют доступ к техническим средствам и информационным ресурсам информационных систем и их системам защиты информации.

2.2. Персональный идентификатор (учетная запись) пользователя создается администратором безопасности и сообщается пользователю. Персональному идентификатору пользователя соответствуют определенные полномочия в информационных системах и пароль, обеспечивающий аутентификацию в информационных системах.

Права пользователя по доступу к информационным ресурсам информационных систем, определяются в соответствии со служебной запиской начальника структурного подразделения на имя руководителя Организации и матрицей доступа.

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 информационных систем при увольнении работника Организации немедленно по окончании последнего сеанса работы работника, а уволенный работник должен быть исключен из числа пользователей информационных систем.

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

Исключается повторное использование идентификатора в течение времени не менее 1 года.

2.5. Первичные пароли генерируются администратором безопасности в момент создания идентификаторов и выдаются пользователю под подпись в журналах учета выдачи первичных паролей информационных систем персональных данных в Организации (Приложение №1, №2, №3 к настоящей Инструкции).

Ведение и надежное хранение журналов учета выдачи первичных паролей информационных систем в Организации (далее - Журнал) осуществляет администратор безопасности.

Срок хранения завершенного Журнала определяется утвержденной номенклатурой Организации.

Уничтожение Журнала по истечении срока хранения (не менее 3-х лет) осуществляется в установленном порядке в Организации.

2.6. Идентификация и аутентификация пользователя информационных систем осуществляется при доступе в информационные системы. Авторизация пользователей информационных систем производится на основании положительных результатов аутентификации.

При первом доступе к информационной системе пользователь обязан изменить выданный первичный пароль, руководствуясь требованиями к сложности пароля, указанными в настоящей Инструкции (пункт 2.8).

2.7. В случаях, предусмотренных нормативными документами по защите персональных данных, обрабатываемых в информационных системах, 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:

– длина пароля должна быть не менее 6 символов;

– алфавит пароля не менее 70 символов;

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

– 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.) и другие данные, которые могут быть подобраны путем анализа информации о пользователе);

– в качестве пароля не может быть использован один и тот же повторяющийся символ либо повторяющаяся комбинация из нескольких символов;

– при смене пароля новое значение должно отличаться от предыдущего не менее чем в 3 символах;

– новое значение пароля не должно совпадать с 5 предыдущими значениями пароля.

2.9. Пароль действует не более 90 дней, по истечении которых пользователь обязан заменить его новым.

2.10. Администратор безопасности осуществляет настройку в информационных системах:

– политики паролей в соответствии с п.2.8, п.2.9;

– параметров количества неуспешных попыток аутентификации (ввода неправильного пароля) до блокировки до 5 попыток;

– блокирование программно-технического средства или учетной записи пользователя информационных систем в случае достижения установленного максимального количества неуспешных попыток аутентификации в течение не более 30 минут;

– блокирование сеанса доступа в информационных системах после установленного времени бездействия (неактивности) пользователя 30 минут или по запросу пользователя.

2.11. Разблокирование пароля осуществляет администратор безопасности при обращении к нему пользователя с заблокированным паролем.

2.12. Администратор безопасности контролирует настройку защиты обратной связи при вводе аутентификационной информации (исключение отображения для пользователя действительного значения пароля, когда вводимые символы отображаются условными знаками «*».

3. Управление аппаратными средствами аутентификации

3.1. В случае использования 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 Организации (Приложение №4 к настоящей Инструкции).

Ведение и надежное хранение журнала учета аппаратных средств аутентификации Организации осуществляет администратор безопасности.

Срок хранения завершенного журнала учета аппаратных средств аутентификации Организации определяется утвержденной номенклатурой Организации.

Уничтожение журнала учета аппаратных средств аутентификации Организации по истечении срока хранения (не менее 3-х лет) осуществляется в установленном порядке в Организации.

4. Обязанности пользователя

4.1. Пользователь информационных систем является частью системы защиты ПДн и обязан соблюдать следующие правила информационной безопасности:

– знать, помнить свой идентификатор и пароль для доступа к информационным системам;

– не разглашать, не сообщать или любым другим способом не доводить до кого-либо, включая работников Организации, в т.ч. руководителей, администратора безопасности и системного администратора, значения действующих паролей;

– не записывать значения паролей на бумагу, электронные носители, иные предметы;

– осуществлять ввод паролей в условиях, исключающих просмотр;

– осуществлять смену пароля не реже, чем через 90 дней;

– надежно хранить индивидуальный аппаратный идентификатор,

– не передавать индивидуальный аппаратный идентификатор другим лицам;

– немедленно сообщать администратору безопасности о фактах компрометации паролей, об утере либо повреждении индивидуального аппаратного идентификатора. В этих случаях не использовать информационных систем до специального разрешения администратора безопасности.

5. Обязанности администратора безопасности

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

5.2. Администратор безопасности обязан:

– создавать, присваивать, уничтожать, вести учет и осуществлять выдачу пользователям персональных идентификаторов и паролей доступа к техническим средствам и информационным ресурсам информационных систем;

– хранить, выдавать, инициализировать, блокировать средства аутентификации (пароли, аппаратные идентификаторы) и принимать меры в случае утраты или компрометации средств аутентификации;

– вести и надежно хранить Журналы учета выдачи первичных паролей информационных систем в Организации;

– надежно хранить и вести учет аппаратных средств аутентификации по Журналу учета аппаратных средств аутентификации Организации;

– обеспечивать смену паролей пользователей с периодичностью не реже 1 раза в 90 дней с момента очередной смены;

– изменять свой собственный пароль не реже 1 раза в месяц;

– принимать меры по обеспечению внеплановой смены паролей в случае их компрометации или утере аппаратных идентификаторов;

– сообщать ответственному за организацию обработки ПДн о инцидентах, связанных с компрометацией или утерей паролей, аппаратных идентификаторов;

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

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

– заблокировать доступ пользователя, владельца скомпрометированного пароля и (или) утраченного идентификатора, к информационным системам.

– выявить действия, произведенные в информационных системах с использованием скомпрометированных персональных идентификаторов и паролей доступа.

– доложить ответственному за организацию обработки ПДн об инциденте.

– создать и выдать пользователю новый персональный идентификатор и пароль (при необходимости аппаратный идентификатор) доступа к информационным системам.

6. Ответственность

6.1. Пользователи информационных систем должны быть предупреждены об ответственности за действия с персональными идентификаторами и паролями доступа, нарушающие требования настоящей Инструкции.

6.2. Работники Организации несут ответственность за ненадлежащее исполнение или неисполнение своих обязанностей, предусмотренных настоящей

Инструкцией, в пределах, определенных действующим законодательством Российской Федерации.

Приложение № 1
к Инструкции по идентификации и аутентификации пользователей
информационных систем в МБОУ Сокольская СШ, утвержденной приказом
МБОУ Сокольская СШ
от «__» _____20__г. № ___

ЖУРНАЛ

учета выдачи первичных паролей
информационной системы персональных данных
«Управление сферой образования в Нижегородской области» в МБОУ Сокольская СШ

Учетный №_____

Журнал начат _____
Журнал окончен _____
Листов (_____)

№ п/п	Ф.И.О. работника	Должность	Подразделение	Тип доступа	Первичный пароль	Дата выдачи/блокирования	Подпись	Примечание
1	2	3	4	5	6	7	8	9
1	И.В. Титова	Директор	Администрация	Пользователь				
2	И.В. Миронова	Заместитель директора		Пользователь				
3	И.В. Миронова	Заместитель директора		Администратор				
4								
5								
6								
7								

Приложение № 2
к Инструкции по идентификации и аутентификации пользователей
информационных систем в МБОУ Сокольская СШ, утвержденной приказом
МБОУ Сокольская СШ
от «__» _____20__г. № ___

ЖУРНАЛ

учета выдачи первичных паролей
информационной системы персональных данных
«Сведения ГИА» в МБОУ Сокольская СШ

Учетный №_____

Журнал начат _____
Журнал окончен _____
Листов (_____)

№ п/п	Ф.И.О. работника	Должность	Подразделение	Тип доступа	Первичный пароль	Дата выдачи/блокирования	Подпись	Примечание
1	2	3	4	5	6	7	8	9
1	И.В. Титова	Директор	Администрация	Пользователь				
2	И.В. Миронова	Заместитель директора		Пользователь				
3	И.В. Миронова	Заместитель директора		Администратор				
4								
5								
6								
7								

Лист ___

Приложение № 3
к Инструкции по идентификации и аутентификации пользователей
информационных систем в МБОУ Сокольская СШ, утвержденной приказом
МБОУ Сокольская СШ
от «__» _____20__г. № ___

ЖУРНАЛ

учета выдачи первичных паролей
информационной системы персональных данных
«Сведения о документах об образовании» в МБОУ Сокольская СШ

Учетный №_____

Журнал начат _____

Журнал окончен _____

Листов (_____)

№ п/п	Ф.И.О. работника	Должность	Подразделение	Тип доступа	Первичный пароль	Дата выдачи/блокирования	Подпись	Примечание
1	2	3	4	5	6	7	8	9
1	И.В. Титова	Директор	Администрация	Пользователь				
2	И.В. Миронова	Заместитель директора		Пользователь				
3	И.В. Миронова	Заместитель директора		Администратор				
4								
5								
6								
7								

Лист ___

Правила

по формированию и ведению
журнала учета выдачи первичных паролей
информационной системы персональных данных

1. Формирование журнала

Журнал ведется на бумажном носителе (формируется из листов формата А4, ориентация листа – альбомная).

Титульный лист журнала изготавливается на отдельном листе.

Все листы журнала (за исключением титульного) нумеруются.

Весь журнал прошнуровывается (сшивается), подписывается с обратной стороны руководителем Организации с указанием количества прошитых и пронумерованных листов в журнале.

2. Ведение журнала

Перед началом использования журнала на лицевой стороне титульного листа указывается номер журнала по номенклатуре дел Организации и дата начала ведения журнала.

Графы журнала заполняются следующим образом:

- Графа 1 – порядковый номер записи;
- Графа 2 – Ф.И.О. работника;
- Графа 3 – занимаемая должность в организации;
- Графа 4 – подразделение организации (если есть);
- Графа 5 – тип доступа (пользователь или администратор);
- Графа 6 – пароль, назначаемый администратором безопасности;
- Графа 7 – дата выдачи или блокирования пароля;
- Графа 8 – подпись работника (при выдаче) или администратора безопасности (при блокировании);
- Графа 9 **–** Примечание (любая информация, относящаяся к пользователю).

Все записи в журнале делаются четко и разборчиво. В случае если вносимые данные не помещаются на одной строке (в одной ячейке), то используется необходимое количество строк.

Приложение № 4
к Инструкции по идентификации и аутентификации пользователей
информационных персональных данных в МБОУ Сокольская СШ,
утвержденной приказом МБОУ Сокольская СШ
от «__» _____20__г. № ___

Журнал

учета аппаратных средств аутентификации
МБОУ Сокольская СШ

Учетный № _____

Журнал начат _____
Журнал окончен _____
Листов (_____)

№ п/п	Наименование устройства	Инвентарный номер	Информационные системы	Дата периодического осмотра и подпись администратора безопасности	Отметка о выдаче			Отметка о возврате		Примечание
					Дата получения	ФИО, должность пользователя	Подпись пользователя за получение	Дата возврата	ФИО и подпись пользователя	
1	2	3	4	5	6	7	8	9	10	11
1	*ESMART Token USB 64K Metal*	*инв. № 000011*	*«Управление сферой образования в Нижегородской области»*	*01.01.2022 АБ _____ И.В. Миронова*	*12.06.2022*	*И.В. Миронова*	*_____/*	*30.12.2022*	*_____ И.В. Миронова*	*Пример заполнения*
2			*«Сведения ГИА»*	*01.01.2022 АБ _____ И.В. Миронова*		*И.В. Миронова*	*_____/*		*_____ И.В. Миронова*	
4			*«Сведения о документах об образовании»*	*01.01.2022 АБ _____ И.В. Миронова*		*И.В. Миронова*	*_____/*		*_____ И.В. Миронова*	
5										
6										
7										
8										

Правила
по формированию и ведению
журнала учета аппаратных средств аутентификации

1. Формирование журнала

Журнал ведется на бумажном носителе (формируется из листов формата А4, ориентация листа – альбомная).

Титульный лист журнала изготавливается на отдельном листе.

Все листы журнала (за исключением титульного) нумеруются.

Весь журнал прошнуровывается (сшивается) и подписывается с обратной стороны руководителем Организации с указанием количества прошитых и пронумерованных листов в журнале.

2. Ведение журнала

Перед началом использования журнала на лицевой стороне обложки указывается номер журнала по номенклатуре дел (журналов) на текущий год и дата начала ведения журнала.

Графы журнала заполняются следующим образом:

- Графа 1 – порядковый номер записи;
- Графа 2 – наименование устройства;
- Графа 3 – инвентарный (серийный) номер устройства;
- Графа 4 – название информационных систем;
- Графа 5 – дата последнего осмотра и подпись администратора безопасности;
- Графа 6 – дата передачи пользователю;
- Графа 7 – Ф.И.О. работника, занимаемая должность в организации;
- Графа 8 – подпись работника за получение устройства;
- Графа 9 – дата возврата работником устройства администратору безопасности;
- Графа 10 – Ф.И.О. работника, подпись за возврат устройства;
- Графа 10 – Примечание. Любая информация, относящаяся к записанному устройству.

Все записи в журнале делаются четко и разборчиво. В случае если вносимые данные не помещаются на одной строке (в одной ячейке), то используется необходимое количество строк.