

ПРИЛОЖЕНИЕ №10

УТВЕРЖДЕНО

Приказом

МДОБУ «Кудровский ДСКВ №4»

«О вводе в действие комплекта организационно-
распорядительной документации по организации обработки и защиты
персональных данных»

Заведующий

Михайлова Марина Тайфиковна

(подпись, печать)

«24» февраля 2025 г.

ИНСТРУКЦИЯ

по управлению доступом

к информационным системам персональных данных

в МДОБУ «Кудровский ДСКВ №4»

Оглавление

1. Общие положения	3
2. Порядок предоставления допуска к обработке информации в информационных системах	5
3. Матрица доступа	5
4. Общий порядок предоставления доступа к информационным системам.....	6
5. Порядок предоставления удаленного доступа (при наличии).....	8
6. Порядок использования мобильных технических средств (в случае использования).	9
7. Взаимодействие с внешними информационными системами (при наличии).	10
8. Ответственность	10
Приложение № 1	11
Приложение № 2	14

1. Общие положения

1.1. Настоящая Инструкция по управлению доступом к информационным системам персональных данных в МДОБУ «Кудровский ДСКВ №4» (далее – Инструкция) определяет в МДОБУ «Кудровский ДСКВ №4» порядок действий администратора безопасности информационных системы персональных данных (далее – информационные системы) и пользователей информационных систем при разграничении доступа к ресурсам и информации 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
СЗИ	Средства защиты информации

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
Идентификация	Действия по присвоению субъектам и объектам доступа идентификаторов	ГОСТ Р 58833-2020

Термин	Определение	Источник
	и/ или по сравнению предъявляемого идентификатора с перечнем присвоенных идентификаторов	
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
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»
Средство защиты информации	Техническое, программное, программно-техническое средство, вещество и (или) материал, предназначенные или используемые для защиты информации	ГОСТ Р 50922-2006

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

- Федеральный закон от 27.07.2006 года № 152-ФЗ «О персональных данных»,
- постановление Правительства Российской Федерации от 01.11.2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»,
- 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».

1.4. Пользователи информационных систем должны быть ознакомлены с настоящей Инструкцией до начала работы в информационных системах. Обязанность по организации ознакомления пользователей с настоящей Инструкцией возлагается на ответственного за организацию обработки ПДн в МДОБУ «Кудровский ДСКВ №4» (далее – ответственный за организацию обработки ПДн).

2. Порядок предоставления допуска к обработке информации в информационных системах

2.1. Допуск работников МДОБУ «Кудровский ДСКВ №4» к обработке информации в информационных системах осуществляется в минимальном объеме, необходимом для выполнения должностных обязанностей.

2.2. Работники МДОБУ «Кудровский ДСКВ №4» допускаются к обработке ПДн в информационных системах в соответствии с утвержденными МДОБУ «Кудровский ДСКВ №4» Перечнями лиц, доступ которых к персональным данным, обрабатываемым в информационных системах в МДОБУ «Кудровский ДСКВ №4», необходим для выполнения ими трудовых (служебных) обязанностей, матрицей доступа.

2.3. Допуск работников МДОБУ «Кудровский ДСКВ №4» непосредственно к обработке персональных данных в информационных системах предоставляется исключительно после прохождения инструктажа по вопросам обработки и защиты персональных данных при их обработке в информационной системе персональных данных.

3. Матрица доступа

3.1. Разграничение доступа к ресурсам и информации информационных систем осуществляет и контролирует администратор безопасности путем настройки программно-технических средств и средств защиты информации информационных систем на основании журналов учета выдачи первичных паролей информационных систем в МДОБУ «Кудровский ДСКВ №4» и матриц доступа.

3.2. Предоставление доступа к информационным ресурсам информационных систем осуществляется в соответствии с приказами МДОБУ «Кудровский ДСКВ №4» .

3.3. В МДОБУ «Кудровский ДСКВ №4» разработаны и утверждены Матрицы доступа к ресурсам информационных систем.

3.4. Сохранность, конфиденциальность и актуальность Матриц доступа обеспечивает администратор безопасности.

4. Общий порядок предоставления доступа к информационным системам

4.1. Каждому лицу, имеющему доступ к информационным системам, присваивается учетная запись. Все действия, совершаемые с использованием учетной записи пользователя информационных систем, рассматриваются как совершаемые лично им.

Учетные записи пользователей информационных систем персонифицированы, то есть однозначно определяют своего владельца.

4.2. Заведение, активацию, блокирование и уничтожение учетных записей в информационных системах осуществляет администратор безопасности.

4.3. Управление учетными записями, реализация необходимых методов, типов и правил разграничения доступа осуществляется в соответствии с Матрицей доступа.

4.4. Гостевые учетные записи в информационных системах не используются.

4.5. Заведение учетных записей администраторов осуществляется в соответствии с утвержденными приказами МДОБУ «Кудровский ДСКВ №4» об администраторах информационных систем и Матрицами доступа. Контроль использования учетных записей администраторов осуществляется ответственным за организацию обработки ПДн.

4.6. Администратор безопасности осуществляет настройку в информационных системах:

- блокирование учетной записи при превышении времени неиспользования более 90 дней;
- блокирование сеанса доступа в информационной системе после установленного времени бездействия (неактивности) пользователя 30 минут или по его запросу;

– блокирование учетной записи в случае достижения установленного максимального количества неуспешных попыток аутентификации в течение не более 30 минут (максимальное количество неуспешных попыток аутентификации до блокировки - 5).

4.7. Вход в информационные системы и действия с ресурсами информационных систем до процедур идентификации и аутентификации разрешены администратору безопасности для восстановления информационных систем после сбоев и аварий технических средств информационных систем. Срок действия разрешения заканчивается в момент запуска информационных систем после восстановления.

Доступ к ресурсам информационных систем до момента прохождения процедур идентификации и аутентификации остальным пользователям запрещен.

4.8. При предоставлении прав доступа к информационным системам используются встроенные функции контроля доступа системного и прикладного программного обеспечения, требующие перед получением доступа обязательного прохождения аутентификации с минимально возможными требованиями использования механизмов аутентификации на основе учетной записи и пароля.

4.9. В случае утраты и (или) компрометации средств аутентификации пользователи информационных систем немедленно обязаны уведомить администратора безопасности, который незамедлительно предпринимает действия по блокированию учетной записи.

4.10. Управление информационными потоками обеспечивается разрешенным маршрутом прохождения информации между пользователями, устройствами в рамках информационных систем, а также между информационными системами или при взаимодействии с сетью Интернет. Управление информационными потоками блокирует передачу защищаемой информации через информационно-телекоммуникационную сеть Интернет (или другие информационно-телекоммуникационные сети международного информационного обмена) по незащищенным линиям связи, сетевые запросы и трафик, несанкционированно исходящие из информационных систем и (или) входящие в информационные системы.

4.11. Процедура предоставления удаленного доступа пользователей информационных систем (при наличии) осуществляется с порядком предоставления доступа, определенного в разделе 5 настоящей Инструкции.

4.12. Процедура использования мобильных технических средств (в случае использования) осуществляется в соответствии с порядком использования, определенного в разделе 6 настоящей Инструкции.

5. Порядок предоставления удаленного доступа (при наличии)

Указанные в пункте 5 требования следует соблюдать только в случае, если организация использует или планирует использовать удаленный доступ (через сеть Интернет) к ресурсам информационных систем.

5.1. Удаленный доступ пользователей к информационным ресурсам информационных систем возможен только с помощью технических средств (персональный компьютер, ноутбук, планшет, сотовый телефон) являющихся собственностью МДОБУ «Кудровский ДСКВ №4» и внесенных в журнал разрешенных устройств удаленного доступа в МДОБУ «Кудровский ДСКВ №4» (Приложение №1 к настоящей Инструкции).

Ведение и надежное хранение журнала разрешенных устройств удаленного доступа в МДОБУ «Кудровский ДСКВ №4» осуществляет администратор безопасности.

Срок хранения завершенного журнала учета разрешенных устройств удаленного доступа в МДОБУ «Кудровский ДСКВ №4» определяется утвержденной номенклатурой МДОБУ «Кудровский ДСКВ №4».

Уничтожение журнала учета разрешенных устройств удаленного доступа в МДОБУ «Кудровский ДСКВ №4» по истечении срока хранения (не менее 3-х лет) осуществляется в установленном порядке в МДОБУ «Кудровский ДСКВ №4» .

5.2. 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 в МДОБУ «Кудровский ДСКВ №4».

5.3. При настройке средств удаленного доступа к ресурсам информационных систем администратор безопасности осуществляет возможность удаленного доступа к

ресурсам информационных систем с автоматической аутентификацией средств удаленного доступа.

5.4. Контроль использования технических средств удаленного доступа к информационным системам возлагается на администратора безопасности.

6. Порядок использования мобильных технических средств (в случае использования)

Указанные в пункте 6 требования следует соблюдать только в случае, если организация использует или планирует использовать мобильные технические средства для доступа к ресурсам информационных систем.

6.1. К мобильным техническим средствам МДОБУ «Кудровский ДСКВ №4» отнесены все переносные технические устройства, на которые может быть записана и с помощью которых может быть осуществлена обработка информации, содержащейся в информационных системах.

6.2. Все мобильные технические средства МДОБУ «Кудровский ДСКВ №4» должны быть учтены и идентифицированы. Учет мобильных технических средств осуществляет администратор безопасности в журнале учета разрешенных мобильных технических средств в МДОБУ «Кудровский ДСКВ №4» (Приложение №2 к настоящей Инструкции).

6.3. Ведение и надежное хранение журнала разрешенных устройств мобильных технических средств в МДОБУ «Кудровский ДСКВ №4» осуществляет администратор безопасности.

6.4. Срок хранения завершеного журнала учета разрешенных мобильных технических средств в МДОБУ «Кудровский ДСКВ №4» определяется утвержденной номенклатурой МДОБУ «Кудровский ДСКВ №4».

6.5. Уничтожение журнала учета разрешенных мобильных технических средств в МДОБУ «Кудровский ДСКВ №4» по истечении срока хранения (не менее 3-х лет) осуществляется в установленном порядке в МДОБУ «Кудровский ДСКВ №4».

6.6. При передаче мобильных технических средств на ремонт или техническое обслуживание администратор безопасности полностью очищает их от персональных данных и информации, имеющей отношение к информационным системам, в соответствии с Инструкцией по защите машинных носителей персональных данных в МДОБУ «Кудровский ДСКВ №4» . .

6.7. Контроль использования мобильных технических средств для доступа к информационным системам возлагается на администратора безопасности.

7. Взаимодействие с внешними информационными системами (при наличии)

7.1. Пользователям внешних информационных систем (внешним пользователям) доступ к ресурсам информационных систем устанавливают в Матрице доступа.

7.2. Администратор безопасности осуществляет процедуру доступа внешних пользователей к ресурсам информационных систем в соответствии с пунктом 4 настоящей Инструкции.

8. Ответственность

8.1. Работники МДОБУ «Кудровский ДСКВ №4» несут ответственность за ненадлежащее исполнение или неисполнение своих обязанностей, предусмотренных настоящей Инструкцией, в соответствии с действующим законодательством Российской Федерации.

Приложение № 1
к Инструкции по управлению доступом к информационным системам
персональных данных в МДОБУ «Кудровский ДСКВ №4»
от «__» _____ 20__ г. № ____

ЖУРНАЛ
учета разрешенных средств удаленного доступа
в МДОБУ «Кудровский ДСКВ №4»

Учетный № _____
Журнал начат _____
Журнал окончен _____
Листов (_____)

№ п/п	Наименование	Инвентарный номер	Состояние	Отметка о выдаче			Отметка о возврате		Примечание
				Дата получения	ФИО, должность пользовате- ля	Подпись пользо- вателя за получение	Дата возврата	ФИО и подпись пользователя	
1	2	3	4	5	6	7	8	9	10
1	ноутбук Lenovo B590	инв. № 1000013	исправен	12.06.2021	И.О. Фамилия , должность ответственно го за организацию обработки ПДн	____/	30.10.2021	____[И.О. Фамилия ответственно- го за организацию обработки ПДн]	Пример заполнения
2									
3									
4									
5									
6									
7									
8									
9									
10									

Правила

по формированию и ведению
журнала учета разрешенных средств удаленного доступа
в МДОБУ «Кудровский ДСКВ №4»

1. Формирование журнала

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

Титульный лист изготавливается на отдельном листе.

Все листы журнала (за исключением титульного) нумеруются.

Весь журнал прошнуровывается (сшивается) и подписывается с обратной стороны руководителем МДОБУ «Кудровский ДСКВ №4» с указанием количества прошитых и пронумерованных листов в журнале.

2. Ведение журнала

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

Графы журнала заполняются следующим образом:

- Графа 1 – учетный порядковый номер записи;
- Графа 2 – наименование оборудования или программного средства;
- Графа 3 – инвентарный или серийный номер;
- Графа 4 – указывается техническое состояние устройства.
- Графа 5 – дата передачи пользователю;
- Графа 6 – Ф.И.О. работника, занимаемая должность в организации;
- Графа 7 – подпись работника за получение устройства (средства);
- Графа 8 – дата возврата работником устройства администратору безопасности;
- Графа 9 – Ф.И.О. работника, подпись за возврат устройства;
- Графа 10 – любая информация, относящаяся к записанному устройству или программному средству.

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

Приложение № 2
к Инструкции по управлению доступом к информационным системам
персональных данных в МДОБУ «Кудровский ДСКВ №4»
от «__» _____ 20__ г. № ____

ЖУРНАЛ
учета разрешенных мобильных технических средств
в МДОБУ «Кудровский ДСКВ №4»

4

Учетный № _____
Журнал начат _____
Журнал окончен _____
Листов (_____)

№ п/п	Наименование оборудования	Инвентарный номер	Состояние	Отметка о выдаче			Отметка о возврате		Примечание
				Дата получения	ФИО, должность пользовател я	Подпись пользовате- ля за получение	Дата возврата	ФИО и подпись пользователя	
1	2	3	4	5	6	7	8	9	10
1	ноутбук Lenovo B590	инв. № 1000013	исправен	12.06.2021	И.О. Фамилия , должность ответственно го за организацию обработки ПДн	_____/	30.10.2021	_____[И.О. Фамилия ответственно- го за организацию обработки ПДн]	Пример заполнения
2									
3									
4									
5									
6									
7									
8									
9									
10									

Правила

по формированию и ведению
журнала учета разрешенных мобильных технических средств
в МДОБУ «Кудровский ДСКВ №4»

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.

Все листы журнала, вместе с обложкой сшиваются.

2. Ведение журнала

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

Графы журнала заполняются следующим образом:

- Графа 1 – учетный порядковый номер записи;
- Графа 2 – наименование оборудования;
- Графа 3 – инвентарный или серийный номер;
- Графа 4 – указывается техническое состояние оборудования.
- Графа 5 – дата передачи пользователю;
- Графа 6 – Ф.И.О. работника, занимаемая должность в организации;
- Графа 7 – подпись работника за получение устройства (средства);
- Графа 8 – дата возврата работником оборудования администратору безопасности;
- Графа 9 – Ф.И.О. работника, подпись за возврат устройства;
- Графа 10 – любая информация, относящаяся к записанному устройству или программному средству.

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