**МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РД**
**ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ РЕСПУБЛИКИ ДАГЕСТАН**
**«КОЛЛЕДЖ ЭКОНОМИКИ И ПРАВА»**

368600,РД.г.Дербент,пер.С.Стальского 26,тел.8(8722)98-99-46,e-mail:keipderbent@mail.ru,сайт:kolle.dagestanschool.ru

«3» 08 2022 г. №101

# ПРИКАЗ

## Об утверждении правил проведения внутренних контрольных мероприятий и реагированию на инциденты информационной безопасности в информационных системах персональных данных

В целях выполнения требований Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», Постановления Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», Постановления Правительства Российской Федерации от 01.11.2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»

ПРИКАЗЫВАЮ:

1. Утвердить Регламент по проведению внутренних контрольных мероприятий и реагированию на инциденты информационной безопасности в информационных системах персональных данных ГБПОУ РД «КЭИП» (Приложение № 1 к настоящему Приказу) (далее – Регламент) с Листом ознакомления работников ГБПОУ РД «КЭИП» с указанным Регламентом (Приложение № 2 к настоящему Приказу).

2. Контроль за исполнением настоящего Приказа, ознакомлением работников ГБПОУ РД «КЭИП» с настоящим Приказом (включая приложения к нему) под роспись оставляю за собой.

**Директор** **Н. А. Гайдаров**

Приложение № 1
к Приказу ГБПОУ РД «КЭИП»
№ 201 от «3» сентября 2022г.

УТВЕРЖДАЮ
Директор ГБПОУ РД «КЭИП»
_____ Н.А. Гайдаров
«3» сентября 2022 г.

**РЕГЛАМЕНТ**

**по проведению внутренних контрольных мероприятий и реагированию на инциденты информационной безопасности в информационных системах персональных данных ГБПОУ РД «КЭИП»**

Дербент

2022

## 1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящий Регламент по проведению контрольных мероприятий и реагированию на инциденты информационной безопасности при обработке персональных данных (далее – Регламент) в ГБПОУ РД «КЭИП» (далее также – Оператор) разработан в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», Постановлением Правительства Российской Федерации от 15.09.2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», Постановлением Правительства Российской Федерации от 01.11.2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

1.2. Настоящий Регламент определяет особенности и порядок проведения внутренних мероприятий по контролю обеспечения защиты персональных данных, порядок реагирования на инциденты информационной безопасности в информационных системах персональных данных ГБПОУ РД «КЭИП», а также порядок предотвращения таких инцидентов.

## 2. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

2.1. В настоящем Регламенте используются следующие термины и их определения:

**Информационная система персональных данных, ИСПДн** – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

**Обработка персональных данных** – действия (операции) с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

**Персональные данные, ПДн –** любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

**Блокирование персональных данных** - временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных).

**Уничтожение персональных данных** - действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных.

## 3. ЦЕЛИ И ТЕМАТИКА ВНУТРЕННЕГО КОНТРОЛЯ

3.1. Целями осуществления внутренних мероприятий по контролю обеспечения защиты персональных данных (далее – внутренний контроль) являются:

- оценка выполнения требований по обработке и защите персональных данных установленных законодательством Российской Федерации, а также локальными нормативными актами Оператора;

- выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных.

3.2.Тематиками внутреннего контроля обработки и защиты ПДн являются:

- соблюдение пользователями ИСПДн парольной политики;

- соблюдение пользователями ИСПДн антивирусной политики;

- соблюдение пользователями ИСПДн правил работы с отчуждаемыми материальными носителями ПДн;

- соблюдение правил работы с криптографическими средствами защиты информации;

- соблюдение порядка доступа в помещения, в которых расположены ИСПДн;

- соблюдение порядка резервирования и восстановления ПДн;

- соблюдение порядка работы со средствами защиты информации;

- знания пользователей ИСПДн порядка поведения во внештатных ситуациях;

- хранение материальных носителей ПДн;

- доступ к материальным носителям ПДн;

- доступ в помещения, где обрабатываются и хранятся материальные носители ПДн;

- иные тематики, вытекающие из локальных нормативных актов Оператора.

## 4. ПОРЯДОК ОСУЩЕСТВЛЕНИЯ ВНУТРЕННЕГО КОНТРОЛЯ

4.1. В целях осуществления внутреннего контроля соответствия обработки ПДн требованиям к защите ПДн в ГБПОУ РД «КЭИП» проводятся периодические проверки условий обработки ПДн в соответствии с ежегодным Планом проведения мероприятий по внутреннему контролю обеспечения защиты ПДн в ГБПОУ РД «КЭИП» (далее – План внутреннего контроля) (Форма - Приложение 1 к Регламенту), а также при необходимости – внеплановые проверки условий обработки ПДн.

4.2. План внутреннего контроля на очередной год (начиная с 2022 года) утверждается Директором ГБПОУ РД «КЭИП» не позднее 31 декабря каждого года.

4.3. Проверки осуществляются Комиссией по приведению деятельности ГБПОУ РД «КЭИП» в соответствие с требованиями законодательства в области персональных данных (далее – Комиссия), или в случае, если она не сформирована - лицом, ответственным за организацию обработки ПДн в ГБПОУ РД «КЭИП».

4.4. Члены Комиссии, получившие доступ к ПДн в ходе проведения мероприятий по внутреннему контролю, обязаны обеспечивать конфиденциальность таких ПДн.

4.5. Плановые проверки проводятся 1 (один) раз в год в соответствии с Планом внутреннего контроля.

4.6. Внеплановые проверки могут проводится по инициативе лица, ответственного за организацию обработки ПДн в ГБПОУ РД «КЭИП», в следующих случаях:

- при существенных изменениях организационной структуры, процессов и процедур обработки и защиты ПДн;

- по результатам расследования выявленных нарушения требований законодательства Российской Федерации в области обработки и защиты ПДн;

- при выявлении большого количества нарушений требований законодательства Российской Федерации в области обработки и защиты ПДн или систематическом повторении одних и тех же нарушений, выявленных в результате плановых проверок;

- по результатам внешних контрольных мероприятий, проводимых уполномоченным органом по защите прав субъектов ПДн;

- в случае поступления сведений об имеющихся нарушениях при осуществлении обработки и защиты ПДн.

4.7. Проведение внеплановой проверки организуется в течение 3 (трех) рабочих дней с момента поступления соответствующего заявления лица, ответственного за организацию обработки ПДн.

4.8. Основными способами проведения внутреннего контроля являются:

- проверка соблюдения работниками Оператора правил обработки и защиты ПДн;

- устный опрос работников Оператора;

- проверка документов, относящихся к деятельности Оператора в части обработки и защиты ПДн, или возникающих в проверяемых процессах обработки ПДн;

- инструментальные проверки защищенности ИСПДн.

4.9. Перечень возможных проверок в ходе проведения внутреннего контроля устанавливается в Приложении 2 к Регламенту.

4.10. Результат проведения внутреннего контроля фиксируется к Акте о проведении внутренней проверки условий обработки и защиты ПДн, который подписывается председателем и членами Комиссии или в случае, если она не сформирована - лицом, ответственным за организацию обработки ПДн в ГБПОУ РД «КЭИП» и утверждается Директором ГБПОУ РД «КЭИП» (Форма – Приложение 3 к Регламенту).

4.11. Результаты проведения внутренних проверок и меры, необходимые для устранения нарушений, выявленных в ходе проверки, доводятся до сведения Директора ГБПОУ РД «КЭИП» для принятия решений о необходимости проведения работ по устранению выявленных нарушений, которые подлежат реализации в установленном порядке.

4.12. В целях контроля устранения выявленных нарушений Комиссия может проводить повторные проверки.

4.13. Акты о проведении внутренних проверок условий обработки и защиты ПДн хранятся в течение 5 (пяти) лет и уничтожаются по истечению срока хранения.

## 5.ПРАВА КОМИССИИ В РАМКАХ ПРОВЕДЕНИЯ ВНУТРЕННИХ ПРОВЕРОК

5.1. Комиссия или в случае, если она не сформирована - лицо, ответственное за организацию обработки ПДн в ГБПОУ РД «КЭИП» в рамках проведения внутренних проверок имеет право:

- привлекать к проведению проверок иных работников Оператора;

- запрашивать у работников Оператора информацию, необходимую для проведения проверки;

- инициировать уточнение, блокирование или уничтожение недостоверных или полученных незаконным путем ПДн;

- инициировать принятие мер по приостановлению или прекращению обработки ПДн, осуществляемой с нарушением требований законодательства РФ в области ПДн;

- вносить на рассмотрение Директору ГБПОУ РД «КЭИП» предложения о необходимых мерах по устранению выявленных нарушений выполнения требований к защите ПДн;

- вносить на рассмотрение Директору ГБПОУ РД «КЭИП» предложения о необходимых мерах по устранению выявленных нарушений выполнения требований к защите ПДн;

- инициировать проведение служебных расследований выявленных нарушений выполнения требований к защите ПДн;

- вносить предложения о привлечении к дисциплинарной ответственности лиц, виновных в нарушении законодательства РФ в отношении обработки ПДн, в том числе по итогам служебных расследований.

5.2. К проведению проверок могут привлекаться лица на договорной основе в соответствии с действующим законодательством РФ.

## 6. ПОРЯДОК РЕАГИРОВАНИЯ НА ИНЦИДЕНТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ

6.1.К инцидентам информационной безопасности в ИСПДн относятся:

6.1.1. Нарушение конфиденциальности, целостности или доступности ПДн;

6.1.2. Отказ оборудования, сервисов, средств обработки и (или) защиты ПДн;

6.1.3. Несоблюдение требований внутренней локальных нормативных актов Оператора и действующего законодательства Российской Федерации в области защиты и обработки ПДн;

6.1.4. Заражение ИСПДн вредоносными программами;

6.1.5. Попытки и факты получения несанкционированного доступа к ИСПДн, включая:

- сеансы работы в ИСПДн незарегистрированных пользователей;

- сеансы работы пользователей ИСПДн с нарушением установленного времени доступа;

- сеансы работы пользователей ИСПДн, срок действия полномочий которых истек либо в состав полномочий которых не входят выявленные действия с ПДн;

- действия третьего лица, пытающегося получить доступ (или получившего доступ) с использованием учетной записи другого пользователя в целях получения коммерческой или другой личной выгоды методом подбора пароля или другого метода (случайного разглашения пароля и т.п.) без ведома владельца учетной записи;

- совершение попыток несанкционированного доступа к персональной рабочей станции, сейфу, шкафу и др. (нарушение целостности пломб, наклеек с защитной и идентификационной информацией, нарушение или несоответствие номеров печатей и др.);

- несанкционированное внесение изменений в конфигурации программных или аппаратных средств обработки или защиты ПДн.

6.2. В случае выявления инцидента информационной безопасности в ИСПДн работник Оператора обязан:

6.2.1. Прекратить работу с ресурсом, в котором выявлен инцидент информационной безопасности;

6.2.2. Оповестить своего непосредственного руководителя и лицо, ответственное за организацию обработки ПДн в ГБПОУ РД «КЭИП» о факте выявления инцидента;

6.2.3. По требованию лица, ответственного за организацию обработки ПДн в ГБПОУ РД «КЭИП» или иных ответственных лиц представить всю необходимую информацию о выявленном инциденте.

6.3.После выявления инцидента информационной безопасности лицо, ответственное за организацию обработки ПДн в ГБПОУ РД «КЭИП» и (или) лицо, ответственное за организацию безопасности в ИСПДн ГБПОУ РД «КЭИП» (если таковое будет назначено) проводит краткий анализ произошедшего инцидента информационной безопасности и причин, способствующих его наступлению, и составляет служебную записку, в которой описываются произошедший инцидент информационной безопасности, его последствия и оценка необходимости проведения расследования инцидента информационной безопасности.

6.4.В случае если инцидент информационной безопасности может стать (или уже стал) причиной негативных последствий для субъектов ПДн, персональные данные этих субъектов необходимо немедленно блокировать до устранения причин, повлекших наступление инцидента информационной безопасности и его последствий. В этом случае лицо, ответственное за организацию обработки ПДн в ГБПОУ РД «КЭИП», уведомляет субъекта о блокировании его ПДн.

6.5.Обязанности по устранению последствий и причин инцидента информационной безопасности возлагаются на лицо, ответственное за организацию обработки ПДн в ГБПОУ РД «КЭИП». Не позднее 3 (трех) дней с момента наступления инцидента лицо, ответственное за организацию обработки ПДн в ГБПОУ РД «КЭИП» составляет и представляет для утверждения Директору ГБПОУ РД «КЭИП» план устранения последствий и причин наступления инцидента информационной безопасности, в котором должно быть указано:

- общая информация о произошедшем инциденте;

- анализ ситуации, оперативные контрмеры, которые можно применить для локализации инцидента;

- определение лиц, ответственных за расследование и установление причин, по которым стало возможным наступление инцидента;

- определение лиц, ответственных за проведение профилактических мероприятий, разработку и внедрение мер по недопущению повторного наступления инцидента.

6.6.Если причины возникновения инцидента информационной безопасности невозможно устранить, то ПДн должны быть уничтожены. Лицо, ответственное за организацию обработки ПДн в ГБПОУ РД «КЭИП», и (или) лицо, ответственное за организацию безопасности в ИСПДн ГБПОУ РД «КЭИП» (если таковое будет назначено) обеспечивают немедленное уничтожение ПДн. Лицо, ответственное за организацию обработки ПДн, оповещает субъекта ПДн о прекращении обработки и уничтожении его ПДн.

6.7.Лицо, ответственное за организацию обработки ПДн в ГБПОУ РД «КЭИП» вправе инициировать проведение служебного расследования инцидента информационной безопасности в случае выявления халатности или иного грубого нарушения требований по обеспечению безопасности ПДн со стороны работника Оператора. Служебное расследование в данном случае проводится Комиссией, или, если она не сформирована - иными работниками ГБПОУ РД «КЭИП» на основании приказа Директора ГБПОУ РД «КЭИП».

## 7. ПРЕДОТВРАЩЕНИЕ ПОВТОРНЫХ ИНЦИДЕНТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ

7.1. Мероприятия по предотвращению повторное возникновение инцидентов информационной безопасности в зависимости от произошедшего инцидента включают в себя:

7.1.1. Мониторинг событий в информационной системе персональных данных;

7.1.2. Восстановление операционной системы рабочей станции, на которой произошел инцидент информационной безопасности, на заводские настройки;

7.1.3. Своевременное удаление неиспользуемых учетных записей;

7.1.4. Контроль и мониторинг действий пользователей ИСПДн;

7.1.5. Контроль над действиями системных администраторов;

7.1.6. Проверка знаний пользователей ИСПДн правилам в области обработки и защиты персональных данных;

7.1.7. Ознакомление пользователей ИСПДн с мерами ответственности, установленными законодательством Российской Федерации за нарушение норм

и правил обработки персональных данных, а также за разглашение полученных данных;

7.1.8. Пересмотр локальных нормативных актов Оператора, устанавливающих правила обработки и обеспечения безопасности при работе с персональными данными.

**Приложение 1**
к Регламенту по проведению внутренних контрольных мероприятий и
реагированию на инциденты информационной безопасности
в информационных системах персональных данных ГБПОУ РД «КЭИП»

Форма

УТВЕРЖДАЮ
Директор ГБПОУ РД «КЭИП»
_____
«____»_____ 20___г.

**ПЛАН**
**проведения мероприятий по внутреннему контролю обеспечения защиты персональных данных в ГБПОУ РД «КЭИП» на 20___ год**

| № п/п | Наименование мероприятия | Проверяемый период | Сроки проведения |
|---|---|---|---|
| | | | |
| | | | |
| | | | |

**Приложение 2**
к Регламенту по проведению внутренних контрольных мероприятий и реагированию на инциденты информационной безопасности в информационных системах персональных данных ГБПОУ РД «КЭИП»

**ПЕРЕЧЕНЬ**
**возможных проверок в ходе проведения мероприятий по внутреннему контролю обеспечения защиты персональных данных в ГБПОУ РД «КЭИП»**

| № п/п | Предмет проверки |
|---|---|
| 1 | Соответствие указанных в Перечне персональных данных, обрабатываемых в ГБПОУ РД «КЭИП», фактически обрабатываемым |
| 2 | Соответствие установленных прав доступа к персональным данным полномочиям в рамках трудовых обязанностей работников |
| 3 | Актуальность перечней работников, осуществляющих обработку персональных данных и имеющих доступ к обрабатываемым персональным данным |
| 4 | Подтверждение факта ознакомления работников с локальными нормативными актами ГБПОУ РД «КЭИП» в области обработки и защиты персональных данных |
| 5 | Наличие в поручениях оператора сведений, установленных п.3 ст. 6 Федерального закона «О персональных данных» (если применимо) |
| 6 | Наличие законных целей и оснований обработки всех персональных данных по категориям субъектов персональных данных |
| 7 | Соответствие целей обработки персональных данных содержанию и объему обрабатываемых персональных данных |
| 8 | Выборочные проверки уровня знаний работниками локальных нормативных актов ГБПОУ РД «КЭИП» в области обработки и защиты персональных данных |
| 9 | Соблюдение сроков и порядка хранения и порядка уничтожения носителей персональных данных |
| 10 | Соблюдение процедур и сроков подготовки ответов на запросы субъектов персональных данных |
| 11 | Необходимость актуализации сведений, содержащихся в реестре операторов персональных данных |
| 12 | Соблюдение условий использования средств защиты информации, используемых для обеспечения защиты персональных данных, предусмотренных эксплуатационной и технической документацией на них |
| 13 | Функционирование технических средств защиты информации, используемых при обеспечении защиты персональных данных |
| 14 | Выполнение мер по обеспечению безопасности персональных данных при их обработке, определенных в соответствии с установленным уровнем защищенности персональных данных, обрабатываемых в информационных системах персональных данных, включая, но не |

| | |
|---|---|
| | ограничиваясь:<br>- проверка регулярности обновления средств антивирусной защиты<br>- проверка проведения резервного копирования персональных данных<br>- проверка соблюдения порядка реагирования на инциденты информационной безопасности в информационных системах персональных данных<br>- проверка процесса управления конфигурациями информационных систем персональных данных и системы защиты персональных данных<br>- проверка реализации процесса управления доступа к ресурсам информационных систем персональных данных |
| 15 | Правильность эксплуатации средств криптографической защиты информации |

**Приложение 3**
к Регламенту по проведению внутренних контрольных мероприятий и
реагированию на инциденты информационной безопасности
в информационных системах персональных данных ГБПОУ РД «КЭИП»

Форма

УТВЕРЖДАЮ
Директор ГБПОУ РД «КЭИП»
_____
«____»_____ 20___г.

**АКТ №___**
**о проведении внутренней проверки обеспечения защиты персональных данных в ГБПОУ РД «КЭИП»**

г. Дербент «_____»_____ 20__ г.

Комиссия по приведению деятельности ГБПОУ РД «КЭИП» в соответствие с требованиями законодательства в области персональных данных (далее – Комиссия) в составе:

Председатель Комиссии:
_____

Члены Комиссии:
_____
_____
_____
…
произвела внутреннюю проверку обеспечения защиты персональных данных в ГБПОУ РД «КЭИП» на основании Регламента по проведению внутренних контрольных мероприятий и реагированию на инциденты информационной безопасности в информационных системах персональных данных ГБПОУ РД «КЭИП», утвержденного Приказом Директора ГБПОУ РД «КЭИП» №____ от «____»_____ 20___г.

Проверка проводилась «___»_____20__г. по адресу: _____.

В ходе проверки были проведены следующие мероприятия:
1) _____
2) _____

3) _____
4) _____
5) _____

Результаты проведения проверки:
1) _____
2) _____
3) _____
4) _____
5) _____

На основании проведения внутренней проверки режима обработки и защиты персональных данных рекомендуется принять следующие меры по устранению нарушений:
1) _____
2) _____
3) _____
4) _____
5) _____

| | | |
|---|---|---|
| Председатель Комиссии | _____ | _____ |
| | *(подпись)* | *(Фамилия И.О.)* |
| Члены Комиссии | _____ | _____ |
| | *(подпись)* | *(Фамилия И.О.)* |
| | _____ | _____ |
| | *(подпись)* | *(Фамилия И.О.)* |
| | .... | ... |

Приложение № 2
к Приказу ГБПОУ РД «КЭИП»
№ 201 от «3» 09 2022 г.

УТВЕРЖДАЮ
Директор ГБПОУ РД «КЭИП»
_____ Н.А. Гайдаров
«3» 09 2022 г.

**ЛИСТ ОЗНАКОМЛЕНИЯ**
**работников ГБПОУ РД «КЭИП» с Регламентом по проведению внутренних контрольных мероприятий и реагированию на инциденты информационной безопасности в информационных системах персональных данных ГБПОУ РД «КЭИП»**

С Регламентом по проведению внутренних контрольных мероприятий и реагированию на инциденты информационной безопасности в информационных системах персональных данных ГБПОУ РД «КЭИП», утвержденной Приказом Директора ГБПОУ РД «КЭИП» №201 от «3» 09 2022 года **ознакомлены следующие заинтересованные работники:**

| № | ФИО | Должность | Дата | Подпись | Примечания |
|---|---|---|---|---|---|
| 1. | Гайдаров Насир Алиевич | Директор | 03.09.22 | | |
| 2. | Аразов Селим Самбурханович | Главный бухгалтер | 03.09.22 | | |
| 3. | Ашурова Гюлляраханум Якубовна | Заместители директора ОЗО и кадровой работе | 03.09.22 | | |
| 4. | Джалилова Анна Леонидовна | Заместитель директора по учебной работе | 03.09.2022 | | |
| 5. | Дадашев Эльхан Камильевич | Заместитель директора по административно-хозяйственной части | 03.09.2022г. | | |

| | | | | | |
|---|---|---|---|---|---|
| 6. | Акимов Замидин Мислимович | Заместитель директора по безопасности | 03.09.22. | | |
| 7. | Матиева Зухра Сефербековна | Заместитель директора по научно-методической работе | 03.09.22 | | |
| 8. | Ибрагимова Зарифа Алисухбатовна | Заместитель директора по воспитательной работе | 03.09.22. | | |
| 9. | Магомедова Гюльнара Али-Экперовна | Заведующая отделением «Юриспруденция» | 03.09.2022 | | |
| 10. | Казибекова Наиля Руслановна | Заведующая отделением «Экономика и бухгалтерский учёт (по отраслям)» | 03.09.2022 | | |
| 11. | Эфендиева Римма Рахметуллаевна | Заведующая отделением «Техносферная безопасность и природообустройство» | 03.09.22 | | |
| 12. | Алиева Фатима Узденовна | Инспектор отдела кадров | 03.09.22 | | |
| 13. | Сурхаева Эльвира Вагидовна | Архивариус | 03.09.22г. | | |
| 14. | Керимханова Наргиз Наримановна | Бухгалтер расчётного стола | 03.09.2022г. | | |
| 15. | Ибрагимова Минаят Сейфетдиновна | Бухгалтер кассир | 03.09.22г. | | |
| 16. | Бутаева Фаризат Кафлановна | Библиотекарь | 03.09.22 | | |
| 17. | Бачханов Джамал Букарович | Оператор ЭВМ | 03.09.22 | | |
| 18. | Тагирова Сакина Надыровна | Оператор ЭВМ | 03.09.22 | | |

| | | | | | |
|---|---|---|---|---|---|
| 19. | Саруханова Заира Ибайдуллаховна | Педагог-психолог | 03.09.22 | | |
| 20. | Эльдарова Фериде Юсифовна | Секретарь учебной части | 03.09.2022 | | |
| 21. | Бабатова Изумруд Сиражутдиновна | Секретарь учебной части | 03.09.2022 | | |