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» 09 2022 г. №205

ПРИКАЗ

О проведении работ по определению уровня защищенности персональных данных, обрабатываемых 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 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»

ПРИКАЗЫВАЮ:

1. Комиссии по приведению деятельности ГБПОУ РД «КЭИП» в соответствие с требованиями законодательства в области персональных данных (далее – Комиссию) провести работы по определению уровня защищенности персональных данных, обрабатываемых в информационных системах персональных данных ГБПОУ РД «КЭИП», по итогам указанных работ составить и представить для утверждения соответствующий Акт.

2. Утвердить Регламент по определению уровня защищенности персональных данных, обрабатываемых 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).

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

Директор **Н. А. Гайдаров**

Приложение № 1
к Приказу ГБПОУ РД «КЭИП»
№ 205 от «1» 09 2022 г.

УТВЕРЖДАЮ
Директор ГБПОУ РД «КЭИП»
_____ Н.А. Гайдаров
«1» 09 2022 г.

РЕГЛАМЕНТ

определения уровня защищенности персональных данных, обрабатываемых в информационных системах персональных данных ГБПОУ РД «КЭИП»

Дербент

2022

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящий Регламент определения уровня защищенности персональных данных, обрабатываемых в информационных системах персональных данных ГБПОУ РД «КЭИП» (далее – Регламент) разработан в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», Постановлением Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», Постановлением Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

1.2. Цель разработки настоящего Регламента – установление порядка определения уровня защищенности персональных данных (далее – ПДн), обрабатываемых в информационных системах персональных данных (далее – ИСПДн) ГБПОУ РД «КЭИП» (далее также – Оператор).

1.3. Определение уровня защищенности ПДн, обрабатываемых в ИСПДн, возлагается на Комиссию по приведению деятельности ГБПОУ РД «КЭИП» в соответствие с требованиями законодательства в области персональных данных (далее – Комиссия).

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).

Угрозы безопасности персональных данных – совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может

стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий при их обработке в информационной системе персональных данных.

Уровень защищенности персональных данных – комплексный показатель, характеризующий требования, исполнение которых обеспечивает нейтрализацию определенных угроз безопасности персональных данных при их обработке в информационных системах персональных данных.

3. МЕТОДИКА ОПРЕДЕЛЕНИЯ УРОВНЯ ЗАЩИЩЕННОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ, ОБРАБАТЫВАЕМЫХ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ

3.1. Определение уровня защищенности ИСПДн включает в себя следующие этапы:

- анализ исходных данных об ИСПДн;

- оценка степени возможных последствий для субъекта ПДн в случае нарушения характеристик безопасности ПДн и определение типа угроз, актуальных для ИСПДн;

- присвоение уровня защищенности ПДн, обрабатываемых в ИСПДн;

- документальное оформление результатов.

3.2. Анализ исходных данных об ИСПДн

3.2.1. Анализ исходных данных об ИСПДн проводится на основании Перечня ИСПДн, в котором содержится информация об основных характеристиках ИСПДн:

- состав обрабатываемых ПДн;
- объем обрабатываемых ПДн;
- характеристики безопасности ПДн;
- структура ИСПДн;
- наличие подключения к сетям международного обмена;
- режим обработки ПДн;
- разграничение прав доступа;
- местонахождение ИСПДн;

- работники, имеющие доступ к ПДн.

3.2.2. На основании указанных сведений и в соответствии с Постановлением Правительства РФ от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» определяется уровень защищенности персональных данных, обрабатываемых в ИСПДн.

3.3. **Оценка степени возможных последствий для субъекта ПДн в случае нарушения характеристик безопасности ПДн и определение типа угроз, актуальных для ИСПДн**

3.3.1. Второй этап производится Оператором во исполнение пункта 5 части 1 статьи 18.1 Федерального закона «О персональных данных». На данном этапе производится оценка степени возможных последствий для субъекта ПДн при нарушении характеристик безопасности ПДн (реализации угроз) при обработке ПДн в ИСПДн.

3.3.2. Так же на данном этапе определяются вербальные показатели опасности угроз в ИСПДн. Угрозы имеют три значения:

- низкая опасность - реализация угрозы может привести к незначительным негативным последствиям для субъектов ПДн;

- средняя опасность - реализация угрозы может привести к негативным последствиям для субъектов ПДн;

- высокая опасность - реализация угрозы может привести к значительным негативным последствиям для субъектов ПДн.

3.3.3. В качестве данных для анализа Комиссией рассматриваются следующие документы:

- Перечень должностей и третьих лиц, имеющих доступ к ПДн;
- Перечень обрабатываемых ПДн;
- Перечень ИСПДн;
- Перечень применяемых средств защиты информации.

3.3.4. Анализ степени возможных последствий для субъекта ПДн проводится для каждой из характеристик безопасности информации в отдельности:

-нарушение конфиденциальности ПДн (копирование, неправомерное распространение)

-неконтролируемое распространение ПДн или получение доступа к ПДн без согласия субъекта ПДн или наличия иного законного основания лицами, не допущенными к обработке ПДн;

- нарушение целостности ПДн (уничтожение, изменение);

- преднамеренное или непреднамеренное изменение ПДн;

- нарушение доступности ПДн (блокирование);

-временная невозможность осуществлять сбор, систематизацию, накопление, использование, распространение или передачу персональных данных.

3.3.5. Поскольку показатель опасности угрозы является вербальным, то необходимо ввести четкие критерии для определения степени последствий для субъекта ПДн и соответственно показателя опасности угрозы. В Таблице 1 приведены базовые критерии, которые могут быть использованы для проведения определения уровней защищенности ПДн, при их обработке в ИСПДн. В отдельных случаях Комиссией может быть принято решение о выборе иных критериев.

Таблица 1

Критерии оценки последствий для субъекта ПДн и соответствующие им показатели опасности угроз

Критерий оценки последствий для субъекта ПДн	**Степень последствий для субъекта ПДн**	**Показатель опасности угрозы**
При нарушении характеристик безопасности ПДн: - последствия для субъекта ПДн незаметны либо малоощутимы; - отсутствует измеримый финансовый, репутационный, моральный ущерб для субъекта ПДн; - репутация субъекта ПДн, его материальное благополучие, жизнь и здоровье не затронуты; - основные интересы и права субъекта ПДн, закрепленные	Незначительные негативные последствия	Низкая опасность

Конституцией РФ, не затронуты.		
При нарушении характеристик безопасности ПДн: - последствия для субъекта ПДн приводят измеримым, но малым по объему или значению финансовым и/или моральным и/или репутационным потерям; - жизнь и здоровье субъекта ПДн не затронуты; - основные интересы и права субъекта ПДн, закрепленные Конституцией РФ, не затронуты.	Негативные последствия	Средняя опасность
При нарушении характеристик безопасности ПДн: - последствия для субъекта ПДн приводят к ощутимым финансовым, моральным, репутационным потерям, вплоть до потери средств к существованию; - возможно влияние на состояние здоровья или угрозы для жизни субъекта ПДн.	Значительные негативные последствия	Высокая опасность

3.3.6. После выбора критериев оценки последствий для субъекта ПДн Комиссия определяет показатели опасности нарушения конфиденциальности, целостности и доступности.

3.3.7. Исходя из определенных показателей опасности угроз Комиссией устанавливаются итоговые максимальные значения показателей опасности угроз для каждой характеристики безопасности.

3.3.8. На основании полученных итоговых максимальных значений показателей опасности угроз определяется тип угроз, актуальных для ИСПДн:

- Высокая опасность - Угрозы 1-го типа актуальны для информационной системы, если для нее, в том числе, актуальны угрозы, связанные с наличием недокументированных (недекларированных) возможностей в системном программном обеспечении, используемом в информационной системе.

- Средняя опасность - Угрозы 2-го типа актуальны для информационной системы, если для нее, в том числе, актуальны угрозы, связанные с наличием недокументированных (недекларированных) возможностей в прикладном программном обеспечении, используемом в информационной системе.

- Низкая опасность - Угрозы 3-го типа актуальны для информационной системы, если для нее актуальны угрозы, не связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении, используемом в информационной системе.

3.4. **Присвоение уровня защищенности ПДн, обрабатываемых в ИСПДн, и документальное оформление результатов**.

3.4.1. Уровень защищенности ПДн, обрабатываемых в ИСПДн, определяется исходя из типа угроз, актуального для ИСПДн, состава и объема обрабатываемых ПДн.

3.4.2. Необходимость обеспечения 1-го уровня защищенности ПДн при их обработке в информационной системе устанавливается при наличии хотя бы одного из следующих условий:

- для информационной системы актуальны угрозы 1-го типа и информационная система обрабатывает либо специальные категории ПДн, либо биометрические персональные данные, либо иные категории ПДн;

- для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает специальные категории ПДн более чем 100000 субъектов ПДн, не являющихся работниками оператора.

3.4.3. Необходимость обеспечения 2-го уровня защищенности ПДн при их обработке в информационной системе устанавливается при наличии хотя бы одного из следующих условий:

- для информационной системы актуальны угрозы 1-го типа и информационная система обрабатывает общедоступные ПДн;

- для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает специальные категории ПДн работников оператора или специальные категории персональных данных менее чем 100000 субъектов ПДн, не являющихся работниками оператора;

- для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает биометрические ПДн;

- для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает общедоступные ПДн более чем 100000 субъектов ПДн, не являющихся работниками оператора;

- для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает иные категории ПДн более чем 100000 субъектов ПДн, не являющихся работниками оператора;

- для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает специальные категории ПДн более чем 100000 субъектов ПДн, не являющихся работниками оператора.

3.4.4. Необходимость обеспечения 3-го уровня защищенности ПДн при их обработке в информационной системе устанавливается при наличии хотя бы одного из следующих условий:

- для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает общедоступные ПДн работников оператора или общедоступные ПДн менее чем 100000 субъектов ПДн, не являющихся работниками оператора;

- для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает иные категории ПДн работников оператора или иные категории ПДн менее чем 100000 субъектов ПДн, не являющихся работниками оператора;

- для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает специальные категории ПДн работников оператора или специальные категории ПДн менее чем 100000 субъектов ПДн, не являющихся работниками оператора;

- для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает биометрические ПДн;

- для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает иные категории ПДн более чем 100000 субъектов ПДн, не являющихся работниками оператора.

3.4.5. Необходимость обеспечения 4-го уровня защищенности ПДн при их обработке в информационной системе устанавливается при наличии хотя бы одного из следующих условий:

- для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает общедоступные ПДн;

- для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает иные категории ПДн работников оператора или иные категории ПДн менее чем 100000 субъектов ПДн, не являющихся работниками оператора.

3.4.6. Результаты определения уровня защищенности ПДн, обрабатываемых в ИСПДн, оформляются Актом определения уровня защищенности ПДн, обрабатываемых ИСПДн (составляется для каждой ИСПДн, если применимо), который подписывается председателем и членами Комиссии и утверждается Директором ГБПОУ РД «КЭИП».

4. ПЕРЕСМОТР УРОВНЯ ЗАЩИЩЕННОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ, ОБРАБАТЫВАЕМЫХ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ

4.1. Уровень защищенности ПДн, обрабатываемых в ИСПДн, может быть пересмотрен:

- по решению Комиссии на основании проведенного анализа и оценки угроз безопасности ПДн с учетом особенностей и/или изменений конкретной информационной системы;

-по результатам внутренних и внешних мероприятий по контролю за выполнением требований по обеспечению безопасности ПДн при их обработке в ИСПДн.

4.2. Изменения особенностей ИСПДн, следствием которых может стать пересмотр уровня защищенности обрабатываемых в ней ПДн, включают:

- изменение категории ПДн, обрабатываемых в ИСПДн;

- изменения целей обработки ПДн, следствием которых может стать изменение степени возможных последствий для субъекта ПДн при нарушении характеристик безопасности ПДн.

4.3. Результаты работы Комиссии по определению нового уровня защищенности оформляется в виде Акта определения уровня защищенности ПДн, обрабатываемых в ИСПДн.

4.4. Пересмотр уровня защищенности ПДн, обрабатываемых в ИСПДн, производится не реже 1 (одного) раза в год.

Приложение № 2
к Приказу ГБПОУ РД «КЭИП»
№ 205 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 определения уровня защищенности персональных данных, обрабатываемых в информационных системах персональных данных ГБПОУ РД «КЭИП»

С Регламентом определения уровня защищенности персональных данных, обрабатываемых в информационных системах персональных данных ГБПОУ РД «КЭИП», утвержденным Приказом Директора ГБПОУ РД «КЭИП» № 205 от «3» 09 2022 года Гайдарова Н.А. ознакомлены **следующие заинтересованные работники:**

№	ФИО	Должность	Дата	Подпись	Примечания
	Акимов Замидин Мислимович	Заместитель директора по безопасности	03.09.22		
	Аразов Селим Самбурханович	Главный бухгалтер	03.09.2022		
	Ашурова Гюлляраханум Якубовна	Заместитель директора по ОЗО и кадровой работе	03.09.2022		

	Эльдарова Фериде Юсифона	Секретарь учебной части	03.09.2022		
	Бачханов Джамал Букарович	Оператор ЭВМ	03.09.22		