

Министерство образования Саратовской области  
государственное автономное профессиональное образовательное учреждение  
Саратовской области  
«Энгельсский промышленно-экономический колледж»  
(ГАПОУ СО «ЭПЭК»)

СОГЛАСОВАНО:

Совет учреждения

Протокол

от «01» 03 2023г № 3

Секретарь Т.А. Чернышева

УТВЕРЖДАЮ:

Директор ГАПОУ СО

«ЭПЭК»

М.А. Кукушкин

Приказ от «02» 03 2023г.

№ 37



**Регламент**

**оценки возможного вреда субъектам персональных данных и принятию мер по его предотвращению государственным автономным профессиональным образовательным учреждением Саратовской области «Энгельсский промышленно-экономический колледж»**

Энгельс 2023 г.

## 1. Назначение и область применения

1.1. Настоящий Регламент определяет порядок оценки вреда, который может быть причинен субъектам персональных данных в государственном автономном профессиональном образовательном учреждении Саратовской области «Энгельсский промышленно-экономический колледж» (далее – ГАПОУ СО «ЭПЭК») в случае нарушения Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных», и отражает соотношение указанного возможного вреда и принимаемых ГАПОУ СО «ЭПЭК» мер, направленных на обеспечение выполнения обязанностей предусмотренных Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных».

1.2. Настоящий Регламент вводится в действие с момента его утверждения.

1.3. Настоящий Регламент является локальным актом ГАПОУ СО «ЭПЭК», обязательным для исполнения всеми работниками ГАПОУ СО «ЭПЭК», допущенными к работе с персональными данными.

1.4. Настоящий Регламент разработан в соответствии со следующими нормативными правовыми актами:

- Конституцией Российской Федерации;
- Трудовым кодексом Российской Федерации;
- Гражданским кодексом Российской Федерации;
- Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных»
- Федеральным законом от 27.07.200 №149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральным законом от 29.12.2012 №273-ФЗ «Об образовании в Российской Федерации»;
- внутренними нормативными документами ГАПОУ СО «ЭПЭК», регламентирующими вопросы обработки и защиты персональных данных.

## 2. Термины и определения

2.1. Для целей настоящего Регламента используются следующие основные понятия:

- **персональные данные** – любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных);

- **субъекты персональных данных** – физические лица (в том числе работники ГАПОУ СО «ЭПЭК», кандидаты на вакантные должности, работники с которыми прекращены трудовые отношения, обучающиеся в ГАПОУ СО «ЭПЭК», законные

представители обучающихся в ГАПОУ СО «ЭПЭК», родственники обучающихся в ГАПОУ СО «ЭПЭК», абитуриенты, лица, состоящие в договорных и иных гражданско-правовых отношениях с ГАПОУ СО «ЭПЭК»), персональные данные которых обрабатываются ГАПОУ СО «ЭПЭК».

- **безопасность персональных данных** – состояние защищенности персональных данных, при котором обеспечены их конфиденциальность, доступность и целостность;

- **конфиденциальность персональных данных** – обязательное для соблюдения лицом, получившим доступ к персональным данным, требование не допускать их распространения без согласия субъекта персональных данных или иного законного основания.

- **целостность информации** – состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими право на такое изменение;

- **доступность информации** – состояние информации (ресурсов информационной системы), при котором субъекты, имеющие права доступа, могут реализовать их беспрепятственно;

- **обработка персональных данных** – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), блокирование, удаление, уничтожение персональных данных;

- **предоставление персональных данных** – действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц;

- **распространение персональных данных** – действия, направленные на раскрытие персональных данных неопределенному кругу лиц;

- **использование персональных данных** – действия (операции) с персональными данными, совершаемые должностным лицом ГАПОУ СО «ЭПЭК» в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъектов персональных данных либо иным образом затрагивающих их права и свободы или права и свободы других лиц;

- **блокирование персональных данных** – временное прекращение обработки 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;

- **обезличивание персональных данных** – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных;

- **общедоступные персональные данные** – персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта персональных данных или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности;

- **информационная система персональных данных** – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;

- **трансграничная передача персональных данных** – передача персональных данных на территорию иностранного государства органу власти иностранному государству, иностранному физическому или юридическому лицу;

- **моральный вред** – физические или нравственные страдания, причиняемые действиями, нарушающими личные неимущественные права гражданина либо посягающими на принадлежащие гражданину другие нематериальные блага, а также в других случаях, предусмотренных законом;

- **оценка возможного вреда** – определение уровня вреда на основании учета причиненных убытков и морального вреда, нарушения конфиденциальности, целостности и доступности персональных данных.

### **3. Общие положения**

3.1. ГАПОУ СО «ЭПЭК» осуществляет как неавтоматизированную обработку персональных данных, так и обработку персональных данных в информационной системе персональных данных лиц, состоящих в трудовых отношениях с ГАПОУ СО «ЭПЭК», лиц с которыми прекращены трудовые отношения, обучающихся в ГАПОУ СО «ЭПЭК», физических лиц, состоящих в договорных и иных гражданско – правовых отношениях с ГАПОУ СО «ЭПЭК».

3.2. Мероприятия по оценке вреда, который может быть причинен субъектам персональных данных, а также соотнесению возможного вреда и реализуемых ГАПОУ СО «ЭПЭК» мер проводятся в следующих целях:

3.2.1. выполнения требований действующего законодательства Российской Федерации в области обработки и защиты персональных данных;

3.2.2. оценки ущерба, нанесенного субъектам персональных данных, вследствие нарушения защищенности их персональных данных (в случае наступления таких событий);

3.2.3. оценки обоснованности и эффективности мер и средств защиты, применяемых для защиты персональных данных;

3.2.4. оценка ущерба, нанесенного субъектам персональных данных, вследствие нарушения состояния защищенности их персональных данных (в случае наступления таких событий) проводится комиссией, состав которой утверждается приказом директора ГАПОУ СО «ЭПЭК».

#### **4. Методика оценки возможного вреда субъектам персональных данных**

4.1. Вред субъекту персональных данных возникает в результате неправомерного или случайного доступа к персональным данным, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

4.2. Перечисленные неправомерные действия определяются как следующие нарушения безопасности информации:

4.2.1. неправомерное предоставление, распространение и копирование персональных данных являются нарушением конфиденциальности персональных данных;

4.2.2. неправомерное уничтожение и блокирование персональных данных является нарушением доступности персональных данных;

4.2.3. неправомерное изменение персональных данных является нарушением целостности персональных данных;

4.2.4. нарушение права субъекта требовать от ГАПОУ СО «ЭПЭК» уточнения его персональных данных, их блокирования или уничтожение является нарушением целостности информации;

4.2.5. нарушение права субъекта на получение информации, касающейся обработки его персональных данных, является нарушением доступности персональных данных;

4.2.6. обработка персональных данных, выходящая за рамки установленных и законных целей обработки, в объеме больше необходимого для достижения установленных и законных целей и дольше установленных сроков является нарушением конфиденциальности персональных данных;

4.2.7. неправомерное получение персональных данных от лица, не являющегося субъектом персональных данных, является нарушением конфиденциальности персональных данных;

4.2.8. принятие решения, порождающего юридические последствия в отношении субъекта персональных данных или иным образом затрагивающие его права и законные интересы, на основании исключительно автоматизированной обработки его персональных данных без согласия на то в письменной форме субъекта персональных данных или непредусмотренное федеральными законами, является нарушением конфиденциальности персональных данных.

4.3. Субъекту персональных данных может быть причинен вред в форме:

4.3.1. убытков – расходов, которые лицо, чье право нарушено, понесло или должно будет понести для восстановления нарушенного права, утраты или повреждения его имущества (реальный ущерб), а также неполученных доходов, которые это лицо получило бы при обычных условиях гражданского оборота, если бы его право не было нарушено;

4.3.2. морального вреда – физических или нравственных страданий, причиняемых действиями, нарушающими личные неимущественные права гражданина либо посягающими на принадлежащие гражданину другие нематериальные блага, а также в других случаях, предусмотренных законом.

4.4. При оценке вреда, который может быть причинен субъектам персональных данных, используется понятие высокого, среднего и низкого уровней вреда. Уровень вреда определяется в зависимости от наличия нарушения целостности, доступности и конфиденциальности персональных данных, а также в зависимости от того, причинили или не причинили эти нарушения убытки и моральный вред субъекту персональных данных.

4.5. В оценке возможного вреда ГАПОУ СО «ЭПЭК» исходит из следующего способа учета последствий допущенного нарушения принципов обработки персональных данных:

4.5.1. низкий уровень возможного вреда – последствия нарушения принципов обработки персональных данных включает только нарушение целостности персональных данных либо только нарушение доступности персональных данных;

4.5.2. средний уровень возможного вреда – последствия нарушения принципов обработки персональных данных включает только нарушение целостности персональных данных, повлекшее убытки и моральный вред, либо только нарушение доступности персональных данных, повлекшее убытки и моральный вред, либо только нарушение конфиденциальности персональных данных;

4.5.3. высокий уровень возможного вреда – во всех остальных случаях;

4.5.4. нарушение целостности или доступности могут принести наименьший вред субъекту персональных данных, так как субъект может и имеет право требовать восстановления целостности и доступности своих персональных данных;

4.5.5. нарушение конфиденциальности всегда представляет собой как минимум средний уровень вреда, так как является потенциально необратимым нарушением даже в том случае, если не влечет за собой морального вреда;

4.5.6. комбинации нескольких нарушений или нарушение конфиденциальности, которое повлекло моральный ущерб и убытки, являются наивысшим уровнем возможного вреда.

4.6. Правила оценки возможного вреда представляются в форме численных значений:

4.6.1. убытки и моральный вред, нарушение целостности и нарушение доступности имеют вес вреда «+1»;

4.6.2. нарушение конфиденциальности имеет вес вреда «+2»;

4.6.3. уровни возможного вреда с низкого по высокий соответствуют значениям вреда «1», «2», «3». Уровень вреда не может иметь значение выше «3», например, «целостность» + «доступность» + «конфиденциальность» («1» + «1» + «2» = «4») даст значение «3» (высокий уровень ущерба).

Приложение к Регламенту  
оценки возможного вреда субъектам  
персональных данных и принятию  
мер по его предотвращению в ГАПОУ СО «ЭПЭК»

**Оценка вреда, который может быть причинен субъектам персональных данных, а также  
соотнесение возможного вреда и реализуемых ГАПОУ СО «ЭПЭК» мер**

№ п/п	Требования 152-ФЗ «О персональных данных» (далее – 152ФЗ), которые могут быть нарушены	Возможные нарушения безопасности информации и причиненный субъекту вред		Уровень возможного вреда	Принимаемые меры по обеспечению выполнения обязанностей ГАПОУ СО «ЭПЭК» как оператора ПДн
1	Обработка ПДн должна ограничиваться достижением конкретных, заранее определенных и законных целей (часть 2 статьи 5 152-ФЗ)	Убытки и моральный вред	+	Высокий	Цели обработки персональных данных закреплены в следующих документах: Положение о защите, хранении, обработке и передаче ПДн работников и обучающихся; Политика в отношении обработки ПДн; Правила осуществления в ГАПОУ СО «ЭПЭК» внутреннего контроля соответствия обработки ПДн.
		Целостность			
		Доступность			
		Конфиденциальность	+		
2	Не допускается объединение баз данных, содержащих ПДн, обработка которых осуществляется в целях, несовместимых между собой (часть 3 статьи 5 152-ФЗ)	Убытки и моральный вред	+	Высокий	Соответствующие нормы закреплены в следующих документах: Положение о защите, хранении, обработке и передаче ПДн работников и обучающихся; Правила работы с обезличенными данными, Политика в отношении обработки ПДн; Правила осуществления в ГАПОУ СО «ЭПЭК» внутреннего контроля соответствия обработки ПДн.
		Целостность			
		Доступность			
		Конфиденциальность	+		
3	Обработке подлежат только ПДн, которые отвечают целям их обработки (часть 4 статьи 5 152-ФЗ)	Убытки и моральный вред	+	Высокий	Перечень ПДн, закреплен в следующих документах: Положение о защите, хранении, обработке и передаче ПДн работников и обучающихся; Политика в отношении обработки ПДн.
		Целостность			
		Доступность			
		Конфиденциальность	+		
4	Содержание и объем обрабатываемых ПДн должны соответствовать заявленным целям обработки (часть 5 статьи 5 152-ФЗ)	Убытки и моральный вред	+	Высокий	Содержание и объем обрабатываемых ПДн определены в следующих документах: Положение о защите, хранении, обработке и передаче ПДн работников и обучающихся; Политика в отношении обработки ПДн.
		Целостность			
		Доступность			
		Конфиденциальность	+		
5	При обработке ПДн должны быть обеспечены точность ПДн, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки ПДн (часть 6 статьи 5 152-ФЗ)	Убытки и моральный вред		Низкий	Соответствующие нормы закреплены в следующих документах: Положение о защите, хранении, обработке и передаче ПДн работников и обучающихся; Политика в отношении обработки ПДн; Правила осуществления в ГАПОУ СО «ЭПЭК» внутреннего контроля соответствия обработки
		Целостность	+		
		Доступность			
		Конфиденциальность			



					ПДн, Положение о порядке уничтожения ПДн.
6	Хранение ПДн должно осуществляться в форме, позволяющей определить субъекта ПДн, не дольше, чем этого требуют цели обработки ПДн, если срок хранения ПДн не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем, по которому является субъект ПДн (часть 7 статьи 5 152-ФЗ)	Убытки и моральный вред	+	Высокий	Соответствующие нормы закреплены в следующих документах: Положение о защите, хранении, обработке и передаче ПДн работников и обучающихся в ГАПОУ СО «ЭПЭК»; Политика в отношении обработки ПДн в ГАПОУ СО «ЭПЭК». ; Правила осуществления в ГАПОУ СО «ЭПЭК» внутреннего контроля соответствия обработки ПДн, Положение о порядке уничтожения ПДн в ГАПОУ СО «ЭПЭК» .
	Целостность				
	Доступность				
	Конфиденциальность	+			
7	Лицо, осуществляющее обработку ПДн по поручению оператора, обязано соблюдать принципы и правила обработки ПДн, предусмотренные 152-ФЗ. В поручении оператора должны быть, определены перечень действий (операций) с ПДн, которые будут совершаться лицом, осуществляющим обработку ПДн, и цели обработки, должна быть установлена обязанность такого лица соблюдать конфиденциальность ПДн и обеспечивать безопасность ПДн при их обработке, а также должны быть указаны требования к защите обрабатываемых ПДн в соответствии со статьей 19 152-ФЗ, часть 3 статьи 6 152-ФЗ.	Убытки и моральный вред	+	Высокий	Соответствующие нормы закреплены в Положении о защите, хранении, обработке и передаче ПДн работников и обучающихся в ГАПОУ СО «ЭПЭК». . Регламент допуска работников к обработке ПДн в ГАПОУ СО «ЭПЭК»..
	Целостность				
	Доступность				
	Конфиденциальность	+			
8	Операторы и иные лица, получившие доступ к ПДн, обязаны не раскрывать третьим лицам и не распространять ПДн без согласия субъекта ПДн, если иное не предусмотрено федеральным законом (статья 7 152-ФЗ)	Убытки и моральный вред	+	Высокий	Соответствующие нормы закреплены в следующих документах: Положение о защите, хранении, обработке и передаче ПДн работников и обучающихся в ГАПОУ СО «ЭПЭК». . Правила осуществления в ГАПОУ СО «ЭПЭК» внутреннего контроля соответствия обработки ПДн. Положение о конфиденциальной информации в ГАПОУ СО «ЭПЭК».
	Целостность				
	Доступность				
	Конфиденциальность	+			

9	<p>Субъект ПДн принимает решение о предоставлении его ПДн и дает согласие на их обработку свободно, своей волей и в своем интересе. Согласие на обработку ПДн может быть дано субъектом ПДн или его представителем в любой позволяющей подтвердить факт его получения форме, если иное не установлено федеральным законом (часть 1 статьи 9 152-ФЗ)</p>	Убытки и моральный вред	+	Высокий	<p>Согласия субъектов на обработку ПДн в ГАПОУ СО «ЭПЭК» фиксируются надлежащим образом, позволяющим подтвердить факт их получения. Соответствующие нормы закреплены в следующих документах: Положение о защите, хранении, обработке и передаче ПДн работников и обучающихся в ГАПОУ СО «ЭПЭК».. Регламент допуска работников к обработке ПДн в ГАПОУ СО «ЭПЭК».</p>
		Целостность			
		Доступность			
		Конфиденциальность	+		
10	<p>Обработка специальных категорий ПДн, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни, не допускается, за исключением случаев, предусмотренных частью 2 статьи 10 152-ФЗ</p>	Убытки и моральный вред	+	Высокий	<p>Правила получения ПДн, отражены в следующих документах: Положение о защите, хранении, обработке и передаче ПДн работников и обучающихся в ГАПОУ СО «ЭПЭК». Регламент допуска работников к обработке ПДн в ГАПОУ СО «ЭПЭК».</p>
		Целостность			
		Доступность			
		Конфиденциальность	+		
11	<p>Субъект ПДн вправе требовать от оператора уточнения его ПДн, их блокирования или уничтожения в случае, если ПДн являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав (часть 1 статьи 14 152-ФЗ)</p>	Убытки и моральный вред	+	Средний	<p>Соответствующие нормы закреплены в следующих документах: Положение о защите, хранении, обработке и передаче ПДн работников и обучающихся, Правила рассмотрения запросов субъектов ПДн и их представителей в ГАПОУ СО «ЭПЭК»</p>
		Целостность	+		
		Доступность			
		Конфиденциальность			
12	<p>Субъект ПДн имеет право на получение информации, касающейся обработки его ПДн (часть 7 статьи 14 152-ФЗ)</p>	Убытки и моральный вред	+	Высокий	<p>Соответствующие нормы закреплены в следующих документах: Положение о защите, хранении, обработке и передаче ПДн работников и обучающихся, Правила рассмотрения запросов субъектов ПДн и их представителей в ГАПОУ СО «ЭПЭК»</p>
		Целостность			
		Доступность			
		Конфиденциальность	+		