

«УТВЕРЖДЕНО»
приказом директора
МАУ ДПО ЦРО
от 11.04.2025 № 85 о/д

Регламент

оценки вреда, который может быть причинён субъектам персональных данных в случае нарушения требований по обработке и обеспечению безопасности персональных данных

1. Термины и определения

Информация – сведения (сообщения, данные) независимо от формы их представления.

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

Безопасность информации – состояние защищенности информации, при котором обеспечены ее конфиденциальность, доступность и целостность.

Конфиденциальность информации – обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя.

Конфиденциальность персональных данных — обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространение без согласия субъекта персональных данных или наличия иного законного основания.

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), обезличивание, блокирование, удаление, уничтожение персональных данных.

Оператор (персональных данных) - государственный орган, муниципальный орган, юридическое или физическое лицо, организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели и содержание обработки персональных данных.

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

Система защиты персональных данных (СЗПДн) – совокупность организационных мер и технических средств защиты информации, а также используемых в информационной системе информационных технологий, в рамках которых реализуются организационные и технические мероприятия, обеспечивающие безопасность персональных данных.

Уничтожение персональных данных - действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных.

Целостность информации – состояние информации, при котором любое ее изменение либо изменение осуществляется преднамеренно субъектами, имеющими право на такое изменение.

Доступность информации информационной – состояние информации (ресурсов информационной системы), при котором субъекты, имеющие права доступа, могут реализовать их беспрепятственно.

Оценка возможного вреда – определение уровня вреда на основании учёта причинённых убытков и морального вреда, нарушения конфиденциальности, целостности и доступности персональных данных.

2. Общие положения

Регламент оценки вреда, который может быть причинен субъектам персональных данных в случае нарушения требований по обработке и обеспечению безопасности персональных данных (далее - Регламент) определяет единый и обязательный порядок и методику оценки вреда, который может быть причинен субъектам персональных данных в случае нарушения требований Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (далее - закон № 152-ФЗ) в МАУ ДПО ЦРО (далее – Оператор), и отражают соотношение указанного возможного вреда и принимаемых Оператором мер, направленных на обеспечение выполнения обязанностей, предусмотренных ФЗ № 152-ФЗ.

Настоящий регламент принят в целях обеспечения соответствия деятельности Оператора требованиям Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

Настоящий регламент обязаны знать и использовать в работе члены комиссии по оценке вреда, который может быть причинен субъектам персональных данных в случае нарушения требований Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

3. Порядок проведения оценки возможного вреда субъекту персональных данных, а также соотнесения возможного вреда и реализуемых Оператором мер

3.1. Оценка возможного вреда субъектам персональных данных осуществляется лицом, ответственным за организацию обработки персональных данных, соответствии с методикой, описанной в разделе 3 настоящих Правил, и на основании экспертных значений, приведённых в Приложении.

3.2. Состав реализуемых Оператором мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных», определяется лицом, ответственным за организацию обработки персональных данных, исходя из правомерности и разумной достаточности указанных мер.

4. Методика оценки возможного вреда субъектам персональных данных

Субъекту персональных данных может быть причинен вред в форме:

а) 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;

б) 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;

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 оператора уточнения его персональных данных, их блокирования или уничтожения 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 законных целей обработки, в объёме 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.

4.4. Оператор для целей оценки вреда определяет одну из степеней вреда, который может быть причинен субъекту персональных данных в случае нарушения Закона о персональных данных.

4.4.1. Высокая степень вреда устанавливается в случаях:

- обработки оператором сведений, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность (биометрические персональные данные) и которые используются Оператором для установления личности субъекта персональных данных, за исключением случаев, установленных федеральными законами, предусматривающими цели, порядок и условия обработки биометрических персональных данных;

- обработки Оператором специальных категорий персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни, сведений о судимости, за исключением случаев, установленных федеральными законами, предусматривающими цели, порядок и условия обработки специальных категорий персональных данных;

- обработки Оператором персональных данных несовершеннолетних для исполнения договора, стороной которого либо выгодоприобретателем или поручителем по которому является несовершеннолетний, а также для заключения договора по инициативе несовершеннолетнего или договора, по которому несовершеннолетний будет являться выгодоприобретателем или поручителем в случаях, не предусмотренных законодательством Российской Федерации;

- обезличивания персональных данных, в том числе с целью проведения оценочных (скоринговых) исследований, оказания услуг по прогнозированию поведения потребителей товаров и услуг, а также иных исследований, не предусмотренных пунктом 9 части 1 статьи 6 Закона о персональных данных;

- поручения иностранному лицу (иностранным лицам) осуществлять обработку персональных данных граждан Российской Федерации;
- сбора персональных данных с использованием баз данных, находящихся за пределами Российской Федерации.

4.4.2. Средний уровень потенциального вреда - последствия нарушения принципов обработки персональных данных включают только нарушение целостности иных данных, повлекшее убытки и моральный вред, либо только нарушение доступности персональных данных, повлекшее убытки и моральный вред, либо только нарушение конфиденциальности персональных данных.

Средняя степень вреда устанавливается в случаях:

- распространения персональных данных на официальном сайте Оператора в сети Интернет, а равно предоставление персональных данных неограниченному кругу лиц, за исключением случаев, установленных федеральными законами, предусматривающими цели, порядок и условия такой обработки персональных данных;
- обработки персональных данных в дополнительных целях, отличных от первоначальной цели сбора;
- продвижения товаров, работ, услуг на рынке путем осуществления прямых контактов с потенциальным потребителем с использованием баз персональных данных, владельцем которых является иной оператор;
- получения согласия на обработку персональных данных посредством реализации на официальном сайте в сети Интернет функционала, не предполагающего дальнейшую идентификацию и (или) аутентификацию субъекта персональных данных;
- осуществления деятельности по обработке персональных данных, предполагающей получение согласия на обработку персональных данных, содержащего положения о предоставлении права осуществлять обработку персональных данных определенному и (или) неопределенному кругу лиц в целях, несовместимых между собой.

4.4.3. Низкий уровень потенциального вреда - последствия нарушения принципов обработки персональных данных включают только нарушение целостности персональных данных, либо только нарушение доступности персональных данных;

Низкая степень вреда устанавливается в случаях: - ведения общедоступных источников персональных данных.

5. Оформление результатов оценки вреда

Результаты оценки вреда оформляются актом оценки вреда.

Акт оценки вреда должен содержать:

- а) наименование или фамилию, имя, отчество (при наличии) и адрес оператора;
- б) дату издания акта оценки вреда;
- в) дату проведения оценки вреда;
- г) фамилию, имя, отчество (при наличии), должность лиц (лица) (при наличии), проводивших оценку вреда, а также их (его) подпись;
- д) степень вреда, которая может быть причинена субъекту персональных данных, определенная в соответствии с методикой оценки вреда, указанной в разделе 4 настоящего регламента.

Акт оценки вреда в электронной форме, подписанный в соответствии с федеральным законом электронной подписью, признается электронным документом, равнозначным акту оценки вреда на бумажном носителе, подписанному собственноручной подписью.

В случае если по итогам проведенной оценки вреда установлено, что в рамках деятельности по обработке персональных данных субъекту персональных данных в соответствии с методикой оценки вреда могут быть причинены различные степени вреда, подлежит применению более высокая степень вреда.

6. Пересмотр регламента

6.1. Пересмотр настоящего регламента осуществляется в следующих случаях, но не реже одного раза в три года:

- при изменении действующих нормативных правовых актов в области обеспечения безопасности персональных данных;
- при существенном изменении процессов обработки персональных данных МАУ ДПО ЦРО;
- по итогам проведения контрольных мероприятий и реагированию на инциденты информационной безопасности.

**Акт по оценке вреда,
который может быть причинен субъектам персональных данных,
а также соотнесение возможного вреда и реализуемых оператором мер**

Комиссия в составе:

Председатель

Члены комиссии

составила настоящий акт о том, что согласно описи, утвержденной актом № ____ от _____ 20__ года, во исполнение Федерального закона от 27.07.2006 № 152 ФЗ «О персональных данных» и приказа Роскомнадзора от 27.10.2022 № 178 «Об утверждении Требований к оценке вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона «О персональных данных» составила акт по результатам оценки вреда:

№ п/п	Действия, которые осуществляет организация при обработке персональных данных	Степень вреда, который может быть причинен субъекту персональных данных при нарушении

Проводили оценку вреда:

Председатель комиссии: _____/_____

Члены комиссии:

_____/_____
 _____/_____
 _____/_____

ОБРАЗЕЦ

**Оценка вреда,
который может быть причинен субъектам персональных данных,
а также соотнесение возможного вреда и реализуемых оператором мер**

№ п/п	Требования Федерального закона «О персональных данных», которые могут быть нарушены	Возможные нарушение безопасности информации и причинённый субъекту вред	Уровень возможного вреда	Принимаемые меры по обеспечению выполнения обязанностей оператора персональных данных	
1	Применение организационных и технических мер по обеспечению безопасности персональных данных при их обработке, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные уровни защищенности персональных данных	Убытки и моральный вред	+	средний	В соответствии с законодательством в области защиты информации и Положением о работе с персональными данными работников, слушателей курсов повышения квалификации, несовершеннолетних и их родителей (законных представителей) ПМПК в МАУ ДПО ЦРО
		Целостность	-		
		Доступность	-		
2	Применение средств защиты информации	Убытки и моральный вред	+	средний	В соответствии с технической документацией на средства защиты ИСПД
		Целостность	+		
		Доступность	-		

		Конфиденциально сть	-		
3	Соблюдение правил доступа к персональным данным	Убытки и моральный вред	+	высокий	В соответствии с принятыми организационными мерами и в соответствии с разграничения доступа
		Целостность	+		
		Доступность	-		
		Конфиденциально сть	+		
4	Отсутствие фактов несанкционированного доступа к персональным данным и принятие необходимых мер	Убытки и моральный вред	+	средний	Контроль сохранности средств защиты информации от несанкционированного доступа
		Целостность	-		
		Доступность	-		
		Конфиденциально сть	+		
5	Осуществление мероприятий по обеспечению целостности персональных данных.	Убытки и моральный вред	-	низкий	Организация режима доступа к техническим и программным средствам
		Целостность	+		
		Доступность	-		
		Конфиденциально сть	-		