

УТВЕРЖДАЮ:
Директор МОУ ДО «ДТДиЮ»
_____/
Приказ № 2 от 09.01.2025 г.

ПОРЯДОК ОЦЕНКИ ВРЕДА,

который может быть причинён субъектам персональных данных в случае нарушения закона «О персональных данных», в МОУ ДО «ДТДиЮ»

1. Общие положения

1.1. Настоящий Порядок оценки вреда субъектам персональных данных (далее – Порядок) определяет правила оценки вреда, который может быть причинён субъекту персональных данных в случае нарушения требований Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» в МОУ ДО «ДТДиЮ», а также форму акта оценки вреда.

1.2. Настоящий Порядок принят в целях обеспечения соответствия процессов обработки персональных данных требованиям Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

1.3. Порядок предназначен для следующих категорий сотрудников Учреждения:

- руководитель;
- сотрудник, ответственный за организацию обработки персональных данных;
- сотрудники, имеющий доступ к персональным данным.

Под сотрудниками в настоящем Порядке понимаются лица, состоящие в трудовых или договорных отношениях с Учреждением.

1.4. Положение разработано в целях реализации требований Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», в соответствии с требованиями Приказа Роскомнадзора от 27.10.2022 № 178 «Об утверждении Требований к оценке вреда, который может быть причинён субъектам персональных данных в случае нарушения Федерального закона «О персональных данных».

1.5. Порядок действует с момента утверждения и действует бессрочно до замены новой версией или документом, его заменяющим. Порядок подлежит пересмотру в случае изменения требований законодательства, изменения оценки рисков информационной безопасности. Изменения в документ вносятся путём издания новой версии и ознакомления с ним сотрудников, а также лиц, осуществляющих обработку персональных данных.

2. Оценка возможного вреда субъекту персональных данных

2.1. 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.

2.2. Оценка уровня вреда, который может быть причинен субъекту персональных данных в случае реализации угроз безопасности информации, проводится путём оценки тяжести

последствий от нарушения каждого из свойств безопасности персональных данных в отдельности.

2.3. Вводятся три вербальных градации показателя уровня вреда:

- вред отсутствует – если нарушение свойств безопасности персональных данных не может привести к каким-либо негативным последствиям для субъекта персональных данных;
- низкий уровень вреда – если нарушение свойств безопасности персональных данных может привести к незначительным негативным последствиям для субъекта персональных данных;
- средний уровень вреда – если нарушение свойств безопасности персональных данных может привести к негативным последствиям для субъекта персональных данных;
- высокий уровень вреда – если нарушение свойств безопасности персональных данных может привести к значительным негативным последствиям для субъекта персональных данных.

2.4. Субъекту персональных данных может быть причинён вред в форме:

Убытков – расходов, которые лицо, чьё 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.

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.

2.5. Оператор для целей оценки вреда определяет одну из степеней вреда, который может быть причинен субъекту персональных данных в случае нарушения Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»:

2.5.1. Высокую степень в случаях:

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

2.5.2. Среднюю степень в случаях:

- распространения персональных данных на официальном сайте в информационно-телекоммуникационной 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 путём 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 информационно-телекоммуникационной 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.

2.5.3. Низкую степень в случаях:

- ведения общедоступных источников персональных данных, сформированных в соответствии со статьей 8 Закона о персональных данных;
 - назначения в качестве ответственного за обработку персональных данных лица, не являющегося штатным сотрудником оператора.
- 2.6. В случае если по итогам проведённой оценки вреда установлено, что в рамках деятельности по обработке персональных данных субъекту персональных данных в соответствии подпунктами 2.5.1–2.5.3 пункта 2.5 настоящего Порядка могут быть причинены различные степени вреда, подлежит применению более высокая степень вреда.
- 2.7. Оценка вреда субъекту персональных данных осуществляется ответственным за организацию обработки персональных данных либо комиссией, образуемой Учреждением.

3. Порядок проведения оценки возможного вреда субъекту персональных данных

3.1. Оценка возможного вреда субъекту персональных данных осуществляется Комиссией по обеспечению безопасности персональных данных, в соответствии с методикой, описанной в разделе 2 настоящего Порядка.

3.2. По результатам оценки степени вреда субъекту персональных данных оформляется акт оценки вреда субъекту персональных данных (далее – Акт).

3.3. Допускается оформление одного Акта на несколько категорий субъектов персональных данных.

3.4. Акт может быть оформлен на бумажном носителе, подписанном собственноручно лицом (лицами), производившими оценку, либо в виде электронного документа, подписанного в соответствии с электронной подписью.

3.5. 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, определённая в соответствии с методикой оценки вреда, указанной в разделе 2.5 настоящего регламента.

3.6. Типовая форма Акта приведена в Приложении № 2.

3.7. Оценка вреда подлежит пересмотру не реже 1 раза в год.

Типовая форма акта оценки вреда субъектам персональных данных

УТВЕРЖДАЮ:
Директор МОУ ДО «ДТДиЮ»
_____ Н.Ю. Нетылько
Приказ № _____ от _____ 202__ г

АКТ

оценки вреда, который может быть причинён субъектам персональных данных в случае нарушения Федерального закона «О персональных данных»

«_____» _____ 20__ г.

№ _____

Настоящий Акт составлен ответственным за организацию обработки персональных данных/комиссией, действующей на основании приказа от «_____» _____ 20__ г. № _____,

в составе:

председатель комиссии: _____/ФИО, должность;

члены комиссии: _____/ФИО, должность;

_____/ФИО, должность

В ходе проведения оценки возможного вреда субъектам персональных данных комиссия руководствовалась следующими документами:

- Порядок оценки возможного вреда субъектам персональных данных
- Политика в отношении обработки персональных данных, утвержден

Комиссия «_____» _____ 20__ г. провела оценку вреда, который может быть причинён субъектам персональных данных в случае нарушения Федерального закона «О персональных данных», и установила следующее:

Таблица 1 — Исходные данные для определения необходимого уровня защищенности

Критерии оценки степени вреда субъектам персональных данных в случае нарушения закона «О персональных данных»

Высокая степень	
- обработка 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	
- обработка 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	
- обработка 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, <u>не предусмотренных</u> законодательством Российской Федерации	
- обезличивание персональных данных, в том числе с целью проведения оценочных (скоринговых) исследований, оказания услуг по прогнозированию поведения потребителей товаров и услуг, а также иных исследований	
- поручение иностранному лицу (иностранцам) осуществлять обработку персональных данных граждан Российской Федерации	
- сбор персональных данных с использованием баз данных, находящихся за пределами Российской Федерации	
Средняя степень	
- распространение персональных данных на официальном сайте в информационно-телекоммуникационной 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	
- обработка персональных данных в дополнительных целях, отличных от первоначальной цели сбора	
- продвижение товаров, работ, услуг на рынке путём осуществления прямых контактов с потенциальным потребителем с использованием баз персональных данных, владельцем которых является иной оператор	
- получение согласия на обработку персональных данных посредством реализации на официальном сайте в информационно-телекоммуникационной сети Интернет функционала, не предполагающего дальнейшую идентификацию и (или) аутентификацию субъекта персональных данных	
- осуществление 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	
Низкая степень	
- ведение общедоступных источников персональных данных, сформированных в соответствии со статьей 8 Закона о персональных данных	
- назначение в качестве ответственного за обработку персональных данных лица, не являющегося штатным сотрудником оператора	

№	Категория субъектов персональных данных	Нарушаемое свойство безопасности	Уровень возможного вреда для субъекта персон
	Работники	Конфиденциальность	Отсутствует / Низкий / Средний / Высокий
		Целостность	Отсутствует / Низкий / Средний / Высокий
		Доступность	Отсутствует / Низкий / Средний / Высокий
	Близкие родственники работников	Конфиденциальность	Отсутствует / Низкий / Средний / Высокий
		Целостность	Отсутствует / Низкий / Средний / Высокий
		Доступность	Отсутствует / Низкий / Средний / Высокий
	Уволенные работники	Конфиденциальность	Отсутствует / Низкий / Средний / Высокий
		Целостность	Отсутствует / Низкий / Средний / Высокий
		Доступность	Отсутствует / Низкий / Средний / Высокий
	Обучающиеся	Конфиденциальность	Отсутствует / Низкий / Средний / Высокий
		Целостность	Отсутствует / Низкий / Средний / Высокий
		Доступность	Отсутствует / Низкий / Средний / Высокий
	Лица, ранее обучавшиеся в образовательной организации	Конфиденциальность	Отсутствует / Низкий / Средний / Высокий
		Целостность	Отсутствует / Низкий / Средний / Высокий
		Доступность	Отсутствует / Низкий / Средний / Высокий
	Посетители оператора	Конфиденциальность	Отсутствует / Низкий / Средний / Высокий
		Целостность	Отсутствует / Низкий / Средний / Высокий
		Доступность	Отсутствует / Низкий / Средний / Высокий
	Представители контрагентов оператора (юридических лиц)	Конфиденциальность	Отсутствует / Низкий / Средний / Высокий
		Целостность	Отсутствует / Низкий / Средний / Высокий
		Доступность	Отсутствует / Низкий / Средний / Высокий
	Физические лица –фигуранты публикаций, лица, изображенные на публикуемых фотографиях	Конфиденциальность	Отсутствует / Низкий / Средний / Высокий
		Целостность	Отсутствует / Низкий / Средний / Высокий
		Доступность	Отсутствует / Низкий / Средний / Высокий
	Пользователь официального сайта Оператора в информационнотелекоммуникационной сети «Интернет»,	Конфиденциальность	Отсутствует / Низкий / Средний / Высокий
		Целостность	Отсутствует / Низкий / Средний / Высокий

	направивший обращение посредством форм обратной связи	Доступность	Отсутствует / Низкий / Средний / Высокий
--	--	-------------	---

Таблица 3 — Исходные данные для определения необходимого уровня защищенности

N п/п	Требования Федерального закона "О персональных данных", которые могут быть нарушены	Возможные нарушение безопасности информации и причиненный субъекту вред	Уровень возможного вреда	Принимаемые меры по обеспечению выполнения обязанностей оператора персональных данных
	порядок и условия применения 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		
		Конфиденциальность		
		Целостность		
		Доступность		
	порядок и условия применения средств защиты информации;	Убытки и моральный вред		
		Конфиденциальность		
		Целостность		
		Доступность		
	эффективность принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;	Убытки и моральный вред		
		Конфиденциальность		
		Целостность		
		Доступность		
	состояние учета машинных носителей персональных данных;	Убытки и моральный вред		
		Конфиденциальность		
		Целостность		
		Доступность		
	соблюдение правил доступа к персональным данным;	Убытки и моральный вред		
		Конфиденциальность		
		Целостность		
		Доступность		

	наличие (отсутствие) фактов несанкционированного доступа к персональным данным и принятие необходимых мер;	Убытки и моральный вред		
		Конфиденциальность		
		Целостность		
		Доступность		
	мероприятия по восстановлению персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;	Убытки и моральный вред		
		Конфиденциальность		
		Целостность		
		Доступность		
	осуществление мероприятий по обеспечению целостности персональных данных.	Убытки и моральный вред		
		Конфиденциальность		
		Целостность		
		Доступность		

Председатель комиссии _____

Члены комиссии

