

УТВЕРЖДЕНЫ  
Распоряжением Главы  
сельского поселения Красный Яр  
муниципального района Красноярский  
Самарской области  
от 18.08.2022 г № 53

## **ПРАВИЛА ОЦЕНКИ ВРЕДА, КОТОРЫЙ МОЖЕТ БЫТЬ ПРИЧИНЕН СУБЪЕКТАМ ПЕРСОНАЛЬНЫХ ДАННЫХ В СЛУЧАЕ НАРУШЕНИЯ ТРЕБОВАНИЙ ПО ОБРАБОТКЕ И ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ**

### 1. Общие положения

1.1. Настоящие правила оценки вреда, который может быть причинен субъектам персональных данных в случае нарушения требований по обработке и обеспечению безопасности персональных данных в администрации сельского поселения Красный Яр, (далее - Правила) определяют порядок оценки вреда, который может быть причинён субъектам персональных данных в случае нарушения [Федерального закона N 152-ФЗ "О персональных данных"](#) (далее - Закон N 152-ФЗ), и отражают соотношение указанного возможного вреда и принимаемых администрацией поселения (далее - Оператор) мер, направленных на обеспечение выполнения обязанностей, предусмотренных Законом N 152-ФЗ.

1.2. Настоящие Правила разработаны в соответствии с действующим законодательством Российской Федерации в области обработки и защиты персональных данных.

### 2. Основные понятия

В настоящих Правилах используются основные понятия приведенные в [Гражданском кодексе Российской Федерации](#), в Федеральном законе от 27.07.2006 1149-ФЗ "Об информации, информационных технологиях и о защите информации" и в Федеральном законе от 27.07.2006 152-ФЗ "О персональных данных".

### 3. Методика оценки возможного вреда субъектам персональных данных

3.1. 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.

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

нарушение конфиденциальности персональных данных:

неправомерное предоставление, распространение и копирование персональных данных;  
обработка персональных данных, выходящая за рамки установленных целей обработки,

в объеме больше необходимого;

неправомерное получение персональных данных от лица, не являющегося субъектом персональных данных;

принятие решения, порождающего юридические последствия в отношении субъекта персональных данных или иным образом затрагивающего права и законные интересы, на основании исключительно автоматизированной обработки его персональных данных без согласия на то в письменной форме субъекта персональных данных или не предусмотренного федеральными законами;

нарушение доступности персональных данных:

нарушение права субъекта на получение информации, касающейся обработки его персональных данных;

неправомерное уничтожение и блокирование персональных данных;

нарушение целостности персональных данных:

неправомерное изменение персональных данных;

нарушение права субъекта требовать от Оператора уточнения его персональных данных, их блокирования или уничтожения.

3.4. Вред, который может быть причинен субъекту персональных данных, определяется в виде:

убытков - расходов, которые субъект персональных данных, чье право нарушено, понесло или должно будет понести для восстановления нарушенного права, утраты или повреждения его имущества (реальный ущерб);

недополученного дохода, который этот субъект персональных данных получил 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 субъекта персональных либо посягающими на принадлежащие субъекту персональных данных другие нематериальные блага, а также в других случаях, предусмотренных законом.

3.4. В оценке возможного вреда необходимо исходить из следующего способа учета последствий допущенного нарушения принципов обработки персональных данных:

низкий уровень возможного вреда - последствия нарушения принципов обработки персональных данных включают только нарушение целостности персональных данных, либо только нарушение доступности персональных данных;

средний уровень возможного вреда - последствия нарушения принципов обработки персональных данных включают 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;

высокий уровень возможного вреда - во всех остальных случаях.

4. Порядок проведения оценки возможного вреда, а также соотнесения возможного вреда и реализуемых Оператором мер

Оценка возможного вреда проводится для исполнения требований к защите персональных данных при их обработке в информационной системе персональных данных (далее - ИСПДн), в частности, при определении типа актуальных угроз безопасности персональных данных при их обработке в ИСПДн во исполнение п. 5 ч. 1 ст. 18.1 Закона N 152-ФЗ.

Оценка возможного вреда субъектам персональных данных и состав реализуемых Оператором мер, направленных на обеспечение выполнения обязанностей, предусмотренных Законом N 152-ФЗ, осуществляется должностными лицами управления информационных технологий, связи и документооборота администрации области в соответствии с методикой оценки возможного вреда субъектам персональных данных, определенной в разделе 3 настоящих Правил, и на основании оценки вреда, который может быть причинен субъектам персональных данных, а также соотнесения возможного вреда и реализуемых Оператором мер, приведенных в приложении к Правилам, исходя из правомерности и разумной достаточности указанных мер. При необходимости допускается привлечение сторонних экспертов в области защиты информации.

Приложение  
к правилам оценки вреда, который может  
быть причинён субъектам персональных данных  
в случае нарушения требований по обработке и  
обеспечению безопасности персональных данных  
в администрации поселения.

## **ОЦЕНКА ВРЕДА, КОТОРЫЙ МОЖЕТ БЫТЬ ПРИЧИНЕН СУБЪЕКТАМ ПЕРСОНАЛЬНЫХ ДАННЫХ, А ТАКЖЕ СООТНЕСЕНИЕ ВОЗМОЖНОГО ВРЕДА И РЕАЛИЗУЕМЫХ ОПЕРАТОРОМ МЕР**

При определении уровня возможного вреда необходимо учитывать, что сами по себе нарушения целостности и доступности могут принести наименьший вред субъекту персональных данных, так как субъект персональных данных может и имеет право требовать восстановления целостности и доступности.

Если такое правомочие субъекта персональных данных затруднено, считается, что имеется основание для судебного иска, поэтому нарушение целостности или доступности, повлекшие моральный вред или ущерб, отнесены к среднему уровню вреда.

Если нарушение конфиденциальности потенциально необратимо (ставшие публичными данные невозможно снова сделать конфиденциальными), то даже в случае, если оно не повлекло причинение морального вреда субъекту персональных данных, такое нарушение относится к среднему уровню возможного вреда.

Если нарушения конфиденциальности повлекли за собой моральный ущерб и убытки, то такие нарушения относятся к наивысшему уровню возможного вреда.

Таблица

**Оценка уровня возможного вреда**

Требования Федерального закона от 27.07.2006 152-ФЗ "О персональных данных", которые могут быть нарушены	Возможные нарушения безопасности информации и причиненный субъекту вред		Уровень возможного вреда	Принимаемые меры по обеспечению выполнения обязанностей Оператора персональных данных
1	2		3	4
1. 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	Убытки и моральный вред	+	высокий	В соответствии с законодательством в области защиты информации и Положением по обеспечением безопасности персональных данных

обеспечивает установленные уровни защищенности персональных данных				
	Целостность			
	Доступность			
	Конфиденциальность	+		
2. Порядок и условия применения средств защиты информации	Убытки и моральный вред	+	средний	В соответствии с технической документацией на систему защиты информационной системы персональных данных
	Целостность	+		
	Доступность			
	Конфиденциальность			
3. Эффективность принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных	Убытки и моральный вред	+	высокий	Программа и методика испытаний систем защиты
	Целостность	+		
	Доступность	+		
	Конфиденциальность	+		
4. Состояние учета машинных носителей персональных данных	Убытки и моральный вред			Инструкция по учету машинных носителей информации
	Целостность			
	Доступность			
	Конфиденциальность			
5. Соблюдение правил доступа к персональным данным	Убытки и моральный вред	+	высокий	В соответствии с принятыми организационными мерами и в соответствии с системой разграничения доступа
	Целостность	+		
	Доступность			
	Конфиденциальность	+		
6. Наличие (отсутствие) фактов несанкционированного	Убытки и моральный вред	+	высокий	Мониторинг средств защиты информации на
	Целостность			
	Доступность			
	Конфиденциальность			

доступа к персональным данным и принятие необходимых мер				наличие фактов доступа к персональным данным
	Целостность			
	Доступность			
	Конфиденциальность	+		
7. Мероприятия по восстановлению персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним	Убытки и моральный вред		средний	Применение резервного копирования
	Целостность	+		
	Доступность	+		
	Конфиденциальность			
8. Осуществление мероприятий по обеспечению целостности персональных данных	Убытки и моральный вред		низкий	Организация режима доступа к техническим и программным средствам
	Целостность	+		
	Доступность			
	Конфиденциальность			