

УТВЕРЖДАЮ

Директор МАОУ СОШ № 101

\_\_\_\_\_  
И.В.Землякова

« \_\_\_\_ » \_\_\_\_\_ 2022

## **ПОРЯДОК**

оценки вреда, который может быть причинён  
субъектам персональных данных  
муниципального автономного общеобразовательного учреждения  
муниципального образования город Краснодар  
средней общеобразовательной школы № 101  
имени Героя Советского Союза Степана Андреевича Неустроева

### **Раздел I**

#### **Общие положения**

1. Настоящий Порядок оценки вреда, который может быть причинён субъектам персональных данных муниципального автономного общеобразовательного учреждения муниципального образования город Краснодар средней общеобразовательной школы № 101 имени Героя Советского Союза Степана Андреевича Неустроева МАОУ СОШ № 101 (далее – Порядок) в случае нарушения Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» (далее – Оценка возможного вреда), содержит методику проведения оценки вреда, а также соотношение указанного вреда и принимаемых оператором мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» (далее – Федеральный закон «О персональных данных»).

2. Оценка возможного вреда осуществляется в соответствии с требованиями статьи 18.1 Федерального закона «О персональных данных».

3. Оценка возможного вреда производится по методике, описанной в разделе III настоящего Порядка.

## Раздел II

### Термины и определения

**4. Персональные данные** – любая информация, относящаяся к прямо или косвенно определённому или определяемому физическому лицу (субъекту персональных данных).

**5. Специальные категории персональных данных** – персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни субъектов персональных данных.

**6. Биометрические персональные данные** – сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность и которые используются оператором для установления личности субъекта персональных данных (за исключением сведений, относящихся к специальным категориям персональных данных).

**7. Общедоступные персональные данные** – персональные данные, полученные только из общедоступных источников персональных данных, созданных в соответствии со статьёй 8 Федерального закона «О персональных данных».

**8. Иные категории персональных данных** – любая информация, относящаяся к прямо или косвенно определённому, или определяемому физическому лицу (субъекту персональных данных), за исключением персональных данных, относящихся к специальным, биометрическим или общедоступным персональным данным.

**9. Оператор** – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

**10. Распространение персональных данных** – действия, направленные на раскрытие персональных данных неопределённому кругу лиц.

**11. Предоставление персональных данных** – действия, направленные на раскрытие персональных данных определённому лицу или определённому кругу лиц.

**12. Блокирование персональных данных** – временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных).

**13. 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.

**14. Конфиденциальность информации** – обязательное для выполнения лицом, получившим доступ к определённой информации, требование не передавать такую информацию третьим лицам без согласия её обладателя.

**15. Целостность информации** – состояние информации, при котором отсутствует любое её изменение либо изменение осуществляется только преднамеренно субъектами, имеющими право на такое изменение.

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

### **Раздел III**

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

17. 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.

18. Перечисленные неправомерные действия определяются как следующие нарушения характеристик безопасности информации (персональных данных):

18.1. Неправомерное предоставление, распространение и копирование персональных данных являются нарушением конфиденциальности персональных данных.

18.2. Неправомерное блокирование персональных данных является нарушением доступности персональных данных.

18.3. Неправомерное уничтожение персональных данных является нарушением доступности и целостности персональных данных.

18.4. Неправомерное изменение персональных данных является нарушением целостности персональных данных.

18.5. Нарушение права субъекта персональных данных требовать от оператора персональных данных уточнения его персональных данных, их блокирования или уничтожения является нарушением целостности информации.

18.6. Нарушение права субъекта на получение информации, касающейся обработки его персональных данных, является нарушением доступности персональных данных.

18.7. Обработка персональных данных, выходящая за рамки установлен-

ных и законных целей обработки, в объёме больше необходимого для достижения установленных и законных целей и дольше установленных сроков является нарушением конфиденциальности персональных данных.

18.8. Неправомерное получение персональных данных от лица, не являющегося субъектом персональных данных, является нарушением конфиденциальности персональных данных.

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

19.1. Морального вреда – физические или нравственные страдания, причинённые субъекту персональных данных действиями или бездействием оператора персональных данных, нарушающими личные неимущественные права субъекта персональных данных либо посягающими на принадлежащие субъекту персональных данных нематериальные блага, а также в других случаях, предусмотренных законом.

19.2. Убытков – расходы, которые лицо (субъект персональных данных), чьё право нарушено, произвело или должно будет произвести для восстановления нарушенного права, утрата или повреждение его имущества (реальный ущерб), а также неполученные доходы, которые это лицо получило бы при обычных условиях гражданского оборота, если бы его право не было нарушено (упущенная выгода).

20. Оценка возможного вреда субъектам персональных данных определяется в соответствии со следующими качественными критериями оценки нарушения заданных характеристик безопасности персональных данных:

20.1. Высокий – приводит к значительным негативным последствиям для субъекта персональных данных, а именно:

нанесение крупного ущерба субъекту персональных данных;

крупные финансовые потери для субъекта персональных данных в результате неправомерных действий с персональными данными;

возможно нанесение тяжёлого вреда здоровью субъекта или возможность реализации прямой угрозы жизни.

20.2. Средний – приводит к негативным последствиям для субъекта персональных данных, а именно:

причинение ущерба субъекту персональных данных;

значительные финансовые потери в результате неправомерных действий с персональными данными;

возможно нанесение вреда, не создающего угрозы жизни или здоровью, субъекту персональных данных.

20.3. Низкий – приводит к незначительным последствиям для субъекта персональных данных, а именно:

нанесение незначительного ущерба субъекту персональных данных или отсутствие подобного вреда;

отсутствие финансовых потерь или незначительные потери для субъекта персональных данных;

отсутствие вреда здоровью или жизни субъекта персональных данных, или причинён незначительный вред.

**Раздел IV**  
**Оценка вреда, который может быть причинён**  
**субъектам персональных данных в случае нарушения**  
**Федерального закона «О персональных данных»**

21. Степень возможного вреда, который может быть причинён субъектам персональных данных в случае нарушения Федерального закона «О персональных данных», определяется по наибольшему значению возможного нарушения каждой из характеристик безопасности информации в отношении категорий субъектов персональных данных, чьи персональные данные обрабатываются в МАОУ СОШ № 101.

22. Оценка возможного вреда приведена в приложении № 1 к настоящему Порядку.

23. Для всех категорий субъектов персональных данных, чьи персональные данные обрабатываются МАОУ СОШ № 101, определена средняя степень возможного ущерба, так как:

в составе персональных данных, обрабатываемых в МАОУ СОШ № 101, отсутствуют сведения, неправомерные действия с которыми, могут привести к причинению крупного вреда субъекту персональных данных;

угроза нанесения тяжкого вреда здоровью или угроза жизни и здоровью субъектам персональных данных отсутствует.

**Раздел V**  
**Соотношение возможного вреда и принимаемых**  
**оператором мер, направленных на обеспечение**  
**выполнения обязанностей, предусмотренных**  
**Федеральным законом «О персональных данных»**

24. МАОУ СОШ № 101 принимаются правовые, организационные и технические меры, необходимые и достаточные для обеспечения исполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении них.

25. Состав мер, направленных на защиту персональных данных, определяется исходя из требований, установленных:

Федеральным законом «О персональных данных»;

Федеральным законом от 25.12.2008 № 273-ФЗ «О противодействии коррупции»;

постановлением Правительства Российской Федерации от 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных»;

постановлением Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

постановлением Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;

приказом Федеральной службы по техническому и экспортному контролю Российской Федерации от 18.02.2013 № 21 «Об утверждении Состав и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

Положением об обработке и защите персональных данных работников, обучающихся и их родителей (законных представителей) МАОУ СОШ № 101.

26. Соотношение возможного вреда и принимаемых оператором мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных», приведено в приложении № 2 к настоящему Порядку.