Приложение 8
к приказу директора ГБПОУ
КК УТМиПТ
от 25.03.2024 г. № 64/1

ОЦЕНКА
вреда, который может быть причинен субъектам персональных данных государственного бюджетного профессионального образовательного учреждения Краснодарского края «Успенский техникум механизации и профессиональных технологий»

1. Общие положения

1.1. Настоящий документ содержит оценку вреда, который может быть причинен субъектам персональных данных, (далее – Оценка возможного вреда), обрабатываемых в государственном бюджетном профессиональном образовательном учреждении Краснодарского края «Успенский техникум механизации и профессиональных технологий» (далее – образовательная организация). Методику проведения оценки возможного вреда, а также соотношение указанного вреда и принимаемых оператором мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (далее – Федеральный закон «О персональных данных»).

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

1.3. В связи с отсутствием нормативных документов Правительства Российской Федерации, Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю Российской Федерации по оценке возможного вреда субъектам персональных данных, производится качественная оценка возможного вреда по методике, описанной в разделе 3 настоящего документа.

2. Термины и определения

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

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

2.3. Биометрические персональные данные – персональные данные, 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).

2.4. Персональные данные, разрешенные субъектом персональных данных для распространения – персональные данные, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных путем дачи согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения в порядке, предусмотренном Федеральным законом «О персональных данных».

2.5. Иные персональные данные – любая информация, относящаяся к прямо или косвенно определенному, или определяемому физическому лицу (субъекту персональных данных), за исключением персональных данных, относящихся к специальным, биометрическим или общедоступным персональным данным.

2.6. 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.

2.7. Распространение персональных данных – действия, направленные на раскрытие персональных данных неопределенному кругу лиц.

2.8. Предоставление персональных данных – действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.

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

2.10. 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.

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

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

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

3. Методики оценки возможного вреда

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 характеристик безопасности информации (персональных данных):

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

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

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

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

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

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

3.2.7. 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.

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

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

3.3.1. Морального вреда – физические или нравственные страдания, причиненные 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.

3.3.2. Убытков – расходы, которые лицо (субъект персональных данных), чье 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).

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

3.4.1. Высокий – приводит к значительным негативным последствиям для

субъекта персональных данных, а именно:

3.4.1.1 нанесение крупного ущерба субъекту персональных данных;

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

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

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

3.4.2.1 причинение ущерба субъекту персональных данных;

3.4.2.2 значительные финансовые потери в результате неправомерных действий с персональными данными;

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

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

3.4.3.1 нанесение незначительного ущерба субъекту персональных данных или отсутствие подобного вреда;

3.4.3.2 отсутствие финансовых потерь или незначительные потери для субъекта персональных данных;

3.4.3.3 отсутствие вреда здоровью или жизни субъекту персональных данных, или незначительный вред.

4. Оценка возможного вреда

4.1. Степень возможного вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона «О персональных данных», определяется по наибольшему значению возможного нарушения каждой из характеристик безопасности информации и отношении категорий субъектов персональных данных, чьи персональные данные обрабатываются в образовательной организации.

4.2. Оценка возможного вреда приведена в приложении 1 к настоящему документу.

4.3. Для всех категорий субъектов персональных данных, чьи персональные данные обрабатываются в образовательной организации, определена средняя степень возможного ущерба, так как:

в составе персональных данных, обрабатываемых в образовательной организации, 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.

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

5.1. В образовательной организации 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.

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

5.2.1 Федеральным законом Российской Федерации «О персональных данных»;

5.2.2 Федеральным законом Российской Федерации от 2 мая 2006 г. № 59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации»;

5.2.3 Федеральным законом Российской Федерации от 27 июля 2010 г. № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг»;

5.2.4 Федеральным законом Российской Федерации от 25 декабря 2008 г. № 273-ФЗ «О противодействии коррупции»;

5.2.5 постановлением Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке информационных системах персональных данных»;

5.2.6 постановлением Правительства Российской Федерации от 15 августа 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;

5.2.7 приказом Федеральной службы по техническому и экспертному контролю Российской Федерации от 18 февраля 2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

5.2.8 приказом Федеральной службы по техническому и экспертному контролю Российской Федерации России от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

5.3. Соотношение возможного вреда и принимаемых оператором мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных», приведено в приложении 2 к настоящему документу.

Приложение 1
к оценке вреда, который может
быть причинен субъектам
персональных данных
образовательной организации

ОЦЕНКА возможного вреда

№ п/п	Категория субъектов персональных данных	Категория персональных данных	Характеристика безопасности информации	Степень возможного вреда	Примечание
1	2	3	4	5	6
1	Работники образовательной организации	Персональные данные, разрешенные субъектом персональных данных для распространения	Конфиденциальность		Нарушение конфиденциальности данной категории персональных данных не несет за собой вред субъектам
			Целостность	Низкая	
			Доступность	Низкая	
		Биометрические	Конфиденциальность		Данная категория персональных данных не обрабатывается
			Целостность		
			Доступность		
		Специальные	Конфиденциальность		
			Целостность		
			Доступность		
		Иные	Конфиденциальность	Средняя	
			Целостность	Средняя	
			Доступность	Низкая	
2	Граждане, претендующие на замещение вакантных должностей образовательной организации	Персональные данные, разрешенные субъектом персональ-	Конфиденциальность		Данная категория персональных данных не обрабатывается
			Целостность		
			Доступность		

1	2	3	4	5	6
		ных данных для распространения			
		Биометрические	Конфиденциальность		
			Целостность		
			Доступность		
		Специальные	Конфиденциальность		
			Целостность		
			Доступность		
		Иные	Конфиденциальность	Средняя	
			Целостность	Средняя	
			Доступность	Низкая	
3	Граждане, обратившиеся в образовательную организацию в порядке, предусмотренном Федеральным законом от 02.05.2006 № 59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации»	Персональные данные, разрешенные субъектом персональных данных для распространения	Конфиденциальность		Данные категории персональных данных не обрабатывается
			Целостность		
			Доступность		
		Биометрические	Конфиденциальность		
			Целостность		
			Доступность		
		Специальные	Конфиденциальность		
			Целостность		
			Доступность		
		Иные	Конфиденциальность	Средняя	
			Целостность	Средняя	
			Доступность	Низкая	

Приложение 2
к оценке вреда, который может
быть причинен субъектам
персональных данных
образовательной организации

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

№ п/п	Перечень мер, принимаемых для обеспечения защиты персональных данных	Степень возможного вреда субъекту персональных данных, при невыполнении меры
1	2	3
1	Сбор согласий на обработку персональных данных, в случаях, установленных Федеральным законом «О персональных данных»	Средняя
2	Оценка вреда субъектам персональных данных	Средняя
3	Обезличивание, уточнение и уничтожение персональных данных, в случаях, когда это необходимо	Средняя
4	Определение правил рассмотрения запросов субъектов персональных данных или их представителей	Средняя
5	Определение правил работы с обезличенными данными в случае обезличивания персональных данных	Средняя
6	Определение порядка доступа в помещения образовательной организации, в которых ведется обработка персональных данных	Средняя
7	Осуществление внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных, установленным Федеральным законом «О персональных данных», принятыми в соответствии с ним нормативными правовыми актами и локальными актами образовательной организации	Средняя
8	Определение угроз безопасности персональных данных, при их обработке в информационных системах образовательной организации	Средняя
9	Определение уровня защищенности персональных данных, обрабатываемых в информационных системах образовательной организации	Средняя
10	Применение организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах образовательной организации, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные уровни защищенности персональных данных	Средняя

1	2	3
11	Исключение несанкционированного, в том числе случайного, доступа к персональным данным, а также иных неправомерных действий в отношении персональных данных	Средняя
12	Применение прошедших в установленном порядке процедуру оценки соответствия средств защиты информации	Средняя
13	Оценка эффективности принимаемых мер по обеспечению безопасности персональных данных	Средняя
14	Учет машинных носителей персональных данных	Средняя
15	Обнаружение фактов несанкционированного доступа к персональным данным и принятие мер	Средняя
16	Восстановление персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним	Средняя
17	Установление правил доступа к персональным данным, а также обеспечением регистрации и учета всех действий, совершаемых с персональными данными в информационных системах образовательной организации	Средняя
18	Контроль за принимаемыми мерами по обеспечению безопасности персональных данных	Средняя