Утверждаю
Директор МБУК «ЦДБ города Мурманска»
_____ Балева В.В.
«__» _____ 2023 г.

ПРАВИЛА
оценки вреда, который может быть причинен субъектам персональных данных в случае нарушения требований по обработке и обеспечению безопасности персональных данных в МБУК «ЦДБ города Мурманска»

Оглавление

I. Назначение

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 МБУК «ЦДБ города Мурманска» (далее - Правила) определяют порядок оценки вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона от 27.07.2006 №152-ФЗ "О персональных данных" , и отражают соотношение указанного возможного вреда и принимаемых оператором мер, направленных на обеспечение выполнения обязанностей, предусмотренных указанным федеральным законом.

II. Область применения

2.1. Настоящие Правила применяются структурными подразделениями МБУК «ЦДБ города Мурманска», обрабатывающими персональные данные в электронном виде и на бумажных носителях. В первую очередь настоящие Правила предназначены для лиц, ответственных за оценку вреда, который может быть причинен субъектам персональных данных в случае нарушения требований по обработке и обеспечению безопасности персональных данных в МБУК «ЦДБ города Мурманска»

2.2. Настоящие Правила подлежат опубликованию или размещению на официальном сайте оператора. Невыполнение оператором предусмотренной законодательством Российской Федерации в области персональных данных обязанности по опубликованию или обеспечению иным образом неограниченного доступа к документу, определяющему политику оператора в отношении обработки персональных данных, или сведениям о реализуемых требованиях к защите персональных данных - влечет предупреждение или наложение административного штрафа на граждан в размере от семисот до одной тысячи пятисот рублей; на должностных лиц - от трех тысяч до шести тысяч рублей; на индивидуальных предпринимателей - от пяти тысяч до десяти тысяч рублей; на юридических лиц - от пятнадцати тысяч до тридцати тысяч рублей[1].

III. Нормативные ссылки

3.1. Настоящие Правила разработаны в соответствии с требованиями п.5) ч.1 ст.18.1 Федерального закона от 27.07.2006 №52-ФЗ "О персональных данных".

---

1 См.: ч.3 ст.13.11 Кодекса Российской Федерации об административных правонарушениях от 30.12.2001 №195-ФЗ.

IV. Термины и обозначения

4.1. В настоящих Правилах используются следующие термины и определения:

4.1.1. **Безопасность информации [данных]** - 1) состояние защищенности информации [данных], при котором обеспечены ее [их] конфиденциальность, доступность и целостность[2]; 2) состояние защищенности информации, характеризуемое способностью персонала, технических средств и информационных технологий обеспечивать конфиденциальность (т.е. сохранение в тайне от субъектов, не имеющих полномочий на ознакомление с ней), целостность и доступность информации при ее обработке техническими средствами[3].

4.1.2. **Доступность (санкционированная доступность) информации** - состояние информации, характеризуемое способностью технических средств и информационных технологий обеспечивать беспрепятственный доступ к информации субъектов, имеющих на это полномочия[4].

4.1.3. **Информация** - сведения (сообщения, данные) независимо от формы их представления.[5]

4.1.4. **Конфиденциальность информации** – обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя[6].

4.1.5. **Моральный вред**- физические или нравственные страдания, причиненные субъекту действиями, нарушающими его личные неимущественные права либо посягающими на принадлежащие гражданину нематериальные блага, а также в других случаях, предусмотренных законом. Суд может возложить на нарушителя обязанность денежной компенсации указанного вреда.[7]

---

[2] См.:
- п. 2.4.5 ГОСТ Р 50922-2006. ЗАЩИТА ИНФОРМАЦИИ. ОСНОВНЫЕ ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ;
- п.3.1.4 «Рекомендации по стандартизации Р.50.1.053 – 2005. Информационная технология. Основные термины и определения в области защиты информации».

[3] См. п. 1.6. Специальных требований и рекомендаций по технической защите конфиденциальной информации (СТР-К), утвержденных приказом Гостехкомиссии России от 30.08.2002 № 282.

[4] См.:
- п.1.9. Специальных требований и рекомендаций по технической защите конфиденциальной информации (СТР-К), утвержденных приказом Гостехкомиссии России от 30.08.2002 № 282;
- Приложение 1 к методическому документу «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014);
- п.3.1.9 «Рекомендации по стандартизации Р.50.1.053 – 2005. Информационная технология. Основные термины и определения в области защиты информации».

[5] См.: п.1 ч.1 ст.2 Федерального закона от 27.07.2006 №149-ФЗ "Об информации, информационных технологиях и о защите информации"

[6] См.: п.7) ст.2 Федерального закона от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации».

[7] См.: ч.1 ст.151 Гражданского кодекса Российской Федерации (часть первая)" от 30.11.1994 №51-ФЗ.

4.1.6. **Оценка возможного вреда** - определение уровня вреда на основании учета причиненных убытков и морального вреда, нарушения конфиденциальности, целостности и доступности персональных данных.

4.1.7. **Убытки**- расходы, которые лицо, 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). Если лицо, нарушившее право, получило вследствие этого доходы, лицо, право которого нарушено, вправе требовать возмещения наряду с другими убытками упущенной выгоды в размере не меньшем, чем такие доходы[8].

4.1.8. **Целостность информации** – 1) Устойчивость информации к несанкционированному или случайному воздействию на нее в процессе обработки техническими средствами, результатом которого может быть уничтожение и искажение информации[9]. 2) Состояние информации (ресурсов автоматизированной информационной системы), при котором ее (их) изменение осуществляется только преднамеренно субъектами, имеющими на него право[10]. 3) Свойство безопасности информации, при котором отсутствует любое ее изменение либо изменение субъектами доступа, имеющими на него право[11].

V. Методика оценки возможного вреда субъектам персональных данных

5.1. 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.

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

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

---

[8] См.: ч.2 ст.15 Гражданского кодекса Российской Федерации (часть первая)" от 30.11.1994 №51-ФЗ.

[9] См.: п.1.27. Специальных требований и рекомендаций по технической защите конфиденциальной информации (СТР-К), утвержденных приказом Гостехкомиссии России от 30.08.2002 № 282.

[10] См.: п.3.1.8 «Рекомендации по стандартизации Р.50.1.053 – 2005. Информационная технология. Основные термины и определения в области защиты информации».

[11] См.: Приложение 1 к методическому документу «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014).

5.4. Неправомерное уничтожение и блокирование персональных данных является нарушением доступности персональных данных.

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

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

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

5.8. 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.

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

5.10. 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.

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

- 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;
- 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.

5.12. В оценке возможного вреда МБУК «ЦДБ города Мурманска» исходит 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.

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

6.1. Оценка возможного вреда субъектам персональных данных осуществляется должностным лицом, ответственным за проведение указанной оценки в соответствии с методикой, описанной в разделе V настоящих Правил, и на основании экспертных значений, приведенных в Приложении к настоящим Правилам.

6.2. Состав реализуемых Оператором мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом от 27.07.2006 №152-ФЗ "О персональных данных", определяется лицом, ответственным в МБУК «ЦДБ города Мурманска» за организацию обработки персональных данных, исходя из правомерности и разумной достаточности указанных мер.

VII. Ответственность должностных лиц

7.1. Должностные лица МБУК «ЦДБ города Мурманска» несут ответственность в соответствии с нормами действующего законодательства за виновные действия, повлекшие причинение вреда субъектам персональных данных при нарушении требований по обработке и обеспечению безопасности персональных данных в МБУК «ЦДБ города Мурманска».

Приложение № 1

ОЦЕНКА

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

N п\п	Требования Федерального закона от 27.07.2006 №152-ФЗ "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
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 обеспечивает установленные уровни защищенности персональных данных;	Убытки и моральный вред	+	средний	В соответствии с законодательством в области защиты информации и Положением по обеспечением безопасности 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 ИСПД
		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)	Убытки и	+	средний	Мониторинг

	фактов несанкционированного доступа к персональным данным и принятие необходимых мер;	моральный вред			средств защиты информации на наличие фактов доступа к ПД
		Целостность			
		Доступность			
		Конфиденциальность	+		
7	мероприятия по восстановлению персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;	Убытки и моральный вред		низкий	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			