Министерство здравоохранения
Республика Карелия

ПРИКАЗ

г. Петрозаводск

от «22» ноября 2022 года № 2071

О внесении изменений в приказ Министерства здравоохранения Республики Карелия от 8 сентября 2020 года №1363

п р и к а з ы в а ю:

Внести в приказ Министерства здравоохранения Республики Карелия от 8 сентября 2020 года №1363 «Об утверждении документов, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом от 27 июля 2006 года №152-ФЗ «О персональных данных» следующие изменения:

1. Добавить пункт 1.6. следующего содержания:

«1.6. Методику оценки вреда, который может быть причинен субъектам персональных данных согласно Приложению №6 к настоящему приказу.».

2. Пункт 2 изложить в следующей редакции:

«2. Отделу ресурсного обеспечения, технического развития и информационной безопасности (М.Н. Игнатику) ознакомить государственных гражданских служащих и работников, обеспечивающих деятельность Министерства с настоящим приказом.».

3. Пункт 4 изложить в следующей редакции:

«4. Контроль за исполнением настоящего приказа возложить на заместителя Министра здравоохранения Республики Карелия И.А. Кижнермана.».

4. Дополнить Приложением №6 в редакции согласно Приложению №1 к настоящему приказу.

Министр М.Е. Охлопков

Приложение №1
к приказу Министерства здравоохранения и
Республики Карелия
от 11 ноября 2022 № 2072
«Приложение №6
к приказу Министерства здравоохранения и
Республики Карелия
От 08.09.2020 №1363

МЕТОДИКА
ОЦЕНКИ ВРЕДА, КОТОРЫЙ МОЖЕТ БЫТЬ ПРИЧИНЕН СУБЪЕКТАМ ПЕРСОНАЛЬНЫХ ДАННЫХ

1. Настоящая Методика определяет порядок оценки вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных» (далее - Закон), и отражает соотношение указанного возможного вреда и принимаемых Министерством здравоохранения Республики Карелия (далее - Оператор) мер, направленных на обеспечение выполнения обязанностей, предусмотренных Законом. Возможный вред субъектам персональных данных оценивается в соответствии с настоящей методикой, на основании экспертных значений и осуществляется в рамках проведения Оператором внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных.

2. 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. Перечисленные в пункте 2 настоящей Методики неправомерные действия определяются как следующие нарушения безопасности информации:

1) неправомерное предоставление, распространение и копирование персональных данных являются нарушением конфиденциальности персональных данных;

2) неправомерное уничтожение и блокирование персональных данных являются нарушением доступности персональных данных;

3) неправомерное изменение персональных данных является нарушением целостности персональных данных;

4) нарушение права субъекта персональных данных требовать от Оператора уточнения его персональных данных, их блокирования или уничтожения является нарушением целостности информации;

5) нарушение права субъекта персональных данных на получение информации, касающейся обработки его персональных данных, является нарушением доступности персональных данных;

6) 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;

7) неправомерное получение персональных данных от лица, не являющегося субъектом персональных данных, является нарушением конфиденциальности персональных данных;

8) принятие решения, порождающего юридические последствия в отношении субъекта персональных данных или иным образом затрагивающего его права и законные интересы, на основании исключительно автоматизированной обработки его персональных данных без согласия на то в письменной форме субъекта персональных данных или не предусмотренное федеральными законами, является нарушением конфиденциальности персональных данных.

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

1) 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;

2) 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. В оценке возможного вреда Оператор исходит из следующего способа учета последствий допущенного нарушения принципов обработки персональных данных:

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

2) 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;

3) высокий уровень возможного вреда - во всех остальных случаях.

6. Оценка вреда, который может быть причинен субъектам персональных данных в случае нарушения Закона, и соотношение указанного возможного вреда и принимаемых Оператором мер, направленных на обеспечение выполнения обязанностей, предусмотренных Законом, приведены в таблице.

Оценка вреда,
который может быть причинен субъектам персональных данных,
и соотношение возможного вреда и принимаемых Оператором мер

N п/п	Требования Закона, которые могут быть нарушены	Возможные нарушения безопасности информации и причиненный субъекту персональных данных вред		Уровень возможного вреда	Меры, принимаемые Оператором, направленные на обеспечение выполнения обязанностей
1	2	3		4	5
1.	Определение угроз безопасности персональных данных при их обработке в информационных системах, содержащих персональные данные	Убытки и моральный вред	+	Высокий	Актуализация моделей угроз безопасности персональных данных
		Целостность	+		
		Доступность	+		
		Конфиденциальность	+		
2.	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	+	Высокий	В соответствии с законодательством Российской Федерации в области защиты информации и Положением об обработке персональных данных в Министерстве здравоохранения Республики Карелия
		Целостность	+		
		Доступность	+		
		Конфиденциальность	+		
3.	Порядок и условия применения средств защиты информации	Убытки и моральный вред	+	Средний	В соответствии с технической документацией на защиту информационных систем, содержащих персональные данные
		Целостность	+		
		Доступность			
		Конфиденциальность			
4.	Эффективность принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных	Убытки и моральный вред	+	Высокий	Проведение проверки эффективности мер защиты информационных систем, содержащих персональные данные
		Целостность	+		
		Доступность	+		
		Конфиденциальность	+		
5.	Состояние учета машинных носителей персональных данных	Убытки и моральный вред		Средний	Ведение учета машинных носителей информации

		Целостность	+		
		Доступность	+		
		Конфиденциальность			
6.	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	+		
7.	Наличие (отсутствие) фактов несанкционированного доступа к персональным данным и принятие необходимых мер	Убытки и моральный вред	+	Средний	Мониторинг средств защиты информации на наличие фактов доступа к персональным данным
		Целостность			
		Доступность			
		Конфиденциальность	+		
8.	Мероприятия по восстановлению персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним	Убытки и моральный вред		Средний	Применение резервного копирования
		Целостность	+		
		Доступность	+		
		Конфиденциальность			
9.	Контроль за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем, содержащих персональные данные	Убытки и моральный вред		Высокий	Осуществление Оператором внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных
		Целостность	+		
		Доступность	+		
		Конфиденциальность	+		

».