



**МИНИСТЕРСТВО ЗДРАВООХРАНЕНИЯ
САРАТОВСКОЙ ОБЛАСТИ**

ПРИКАЗ

«09» 03. 2016г.

г. Саратов

№ 328

**Об утверждении правил оценки вреда,
который может быть причинен субъектам
персональных данных в случае нарушения
требований по обработке и обеспечению
безопасности персональных данных**

В соответствии с требованиями Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных»

ПРИКАЗЫВАЮ:

1. Утвердить Правила оценки вреда, который может быть причинен субъектам персональных данных в случае нарушения требований по обработке и обеспечению безопасности персональных данных в министерстве здравоохранения области согласно Приложению к настоящему приказу.

2. Назначить заместителя начальника управления организации работы министерства здравоохранения области Курганова Сергея Владимировича ответственными за оценку вреда, который может быть причинен субъектам персональных данных в случае нарушения требований по обработке и обеспечению безопасности персональных данных в министерстве здравоохранения области.

3. Настоящий приказ подлежит официальному опубликованию в средствах массовой информации.

4. Контроль за исполнением настоящего приказа возложить на первого заместителя министра здравоохранения области В.Б. Николаева.

Министр

Ж.А. Никулина

**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 (далее – Правила) определяют порядок оценки вреда, который может быть причинён субъектам персональных данных в случае нарушения Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных» (далее – ФЗ № 152-ФЗ), и отражают соотношение указанного возможного вреда и принимаемых оператором мер, направленных на обеспечение выполнения обязанностей, предусмотренных ФЗ № 152-ФЗ.

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

2. Основные понятия

2.1. В настоящих Правилах используются основные понятия:

2.1.1. Информация – сведения (сообщения, данные) независимо от формы их представления.

2.1.2. Безопасность информации – состояние защищенности информации, при котором обеспечены ее конфиденциальность, доступность и целостность.

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

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

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

2.1.6. Убытки – расходы, 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.

2.1.7. Моральный вред – физические или нравственные страдания, причиняемые действиями, нарушающими личные неимущественные права гражданина либо посягающими на принадлежащие гражданину другие нематериальные блага, а также в других случаях, предусмотренных законом.

2.1.8. Оценка возможного вреда – определение уровня вреда на основании учёта причинённых убытков и морального вреда, нарушения конфиденциальности, целостности и доступности 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:

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

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

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

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

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

3.2.6. Обработка персональных данных, выходящая за рамки установленных и законных целей обработки, в объёме больше необходимого для достижения установленных и законных целей и дольше установленных сроков является нарушением конфиденциальности персональных данных.

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

3.2.8. 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.

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

3.3.1. 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.

3.3.2. 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.

3.4. В оценке возможного вреда министерство здравоохранения области исходит из следующего способа учёта последствий допущенного нарушения принципов обработки персональных данных:

3.4.1. Низкий уровень возможного вреда – последствия нарушения принципов обработки персональных данных включают только нарушение целостности персональных данных, либо только нарушение доступности персональных данных;

3.4.2. 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;

3.4.3. Высокий уровень возможного вреда – во всех остальных случаях.

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

4.1. Оценка возможного вреда субъектам персональных данных осуществляется лицом, ответственным в министерстве здравоохранения области за защиту информации, в соответствии с методикой, описанной в разделе 3 настоящих Правил, и на основании экспертных значений, приведённых в Приложении 1.

4.2. Состав реализуемых Оператором мер, направленных на обеспечение выполнения обязанностей, предусмотренных ФЗ № 152-ФЗ «О персональных данных», определяется лицом, ответственным в министерстве здравоохранения области за организацию обработки персональных данных, исходя из правомерности и разумной достаточности указанных мер.

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

№п/п	Требования Федерального закона «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	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					

		ьность			
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 доступа к персональным данным и принятие необходимых мер;	Убытки и моральный вред	+	средний	Мониторинг 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			