«Утверждаю»
Директор МАУ
«МФЦ г. Заречного Пензенской области»

_____ Г.А. Маликова

«02» 06 2025 г. приказ - 10/ОД

Правила оценки вреда, который может быть причинен субъектам персональных данных в случае нарушения требований по обработке и обеспечению безопасности персональных данных

2025

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 причинен субъектам персональных данных в случае нарушения Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных» (далее - Закон), и отражают соотношение указанного возможного вреда и принимаемых МАУ «МФЦ г. Заречного Пензенской области» (далее – Оператор) мер, направленных на обеспечение выполнения обязанностей, предусмотренных Законом.

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:

- **Информация** - сведения (сообщения, данные) независимо от формы их представления;

- **Безопасность информации** - состояние защищенности информации, при котором обеспечены ее конфиденциальность, доступность и целостность;

- **Конфиденциальность информации** - обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя;

- **Целостность информации** - состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими право на такое изменение;

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

- **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;

- **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;

- **Оценка возможного вреда** - определение уровня вреда на основании учета причиненных 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:

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

- неправомерное уничтожение и блокирование персональных данных является нарушением доступности персональных данных;

- неправомерное изменение персональных данных является нарушением целостности персональных данных;

- нарушение права субъекта требовать от оператора уточнения его персональных данных, их блокирования или уничтожение является нарушением целостности информации;

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

- 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;

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

- 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 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.

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

- нулевой уровень вреда – вред субъекту персональных данных не причиняется;

- 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.

3.5. С целью обеспечения объективности вводится коэффициент вероятности инцидента:

- коэффициент равен 3, если инцидент безопасности информации возникал как минимум один раз за предыдущий год.

- коэффициент равен 2, если инцидент безопасности информации возникал более чем за год до даты оценки ущерба, но менее, чем два года до даты оценки ущерба.

- коэффициент равен 1, если инцидент безопасности информации произошел ранее, чем за два года до даты оценки ущерба или не возникал.

При определении возможного вреда субъектам персональных данных учитывается как коэффициент вероятности инцидента безопасности

Таблица. Возможный вред субъектам персональных данных

		Коэффициент вероятности		
		1	2	3
Уровень возможного ущерба	низкий	незначительный	незначительный	незначительный
	средний	незначительный	незначительный	средний
	высокий	незначительный	средний	большой

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

4.1. Оценка возможного вреда субъектам персональных данных осуществляется назначенной приказом директора комиссией.

4.2. Каждым членом комиссии на основании собственного субъективного мнения выставляется один из возможных уровней возможного вреда субъекту персональных данных при нарушении конкретного требования Закона. При этом учитывается и значение коэффициента вероятности инцидента безопасности. При несовпадении мнений членов комиссии об уровне возможного вреда, решение принимается большинством голосов.

4.3. Результаты работы комиссии оформляются в виде Акта, который утверждается директором.

4.4. После формирования оценки вреда, который может быть причинен субъектам персональных данных в случае нарушения требований по обработке и обеспечению безопасности персональных данных оператора проводится анализ применяемых оператором мер, направленных на обеспечение выполнения обязанностей, предусмотренных действующим законодательством в области персональных данных. Пример анализа приведен в Приложении к настоящим Правилам.

По итогам анализа принимается решение о достаточности применяемых мер, направленных на обеспечение выполнения обязанностей, предусмотренных действующим законодательством в области персональных данных и возможности или необходимости принятия дополнительных мер или изменения установленного оператором порядка обработки и обеспечения безопасности персональных данных.

4.5. Оценка соотношения вреда, который может быть причинен субъектам персональных данных в случае нарушения требований по обработке и обеспечению безопасности персональных данных и принимаемых мер по обработке и обеспечению безопасности персональных данных подписывается лицом, ответственным за организацию обработки персональных данных. По результатам принятых решений, лицом, ответственным за организацию обработки персональных данных организуется работа по их реализации.

Приложение

к Правилам оценки вреда, который может быть причинен субъектам персональных данных в случае нарушения требований по обработке и обеспечению безопасности персональных данных

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

N п\п	Требования Федерального закона "О персональных данных", которые могут быть нарушены	Возможные нарушение безопасности информации и причиненный субъекту вред	Есть ли 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 обрабатываемых в ИСПДн
		Целостность	-		
		Доступность	-		
		Конфиденциальность	+		
2	Порядок и условия применения средств защиты информации;	Убытки и моральный вред	+	Средний	В соответствии с техническими паспортами ИСПДн
		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	Проведение проверки эффективности мер защиты ИСПДн
		Целостность	+		
		Доступность	+		
		Конфиденциальность	+		
4	Состояние учета машинных носителей персональных данных	Убытки и моральный вред		Низкий	Журнал учета машинных носителей
		Целостность	+		
		Доступность			
		Конфиденциальность			

N п\п	Требования Федерального закона "О персональных данных", которые могут быть нарушены	Возможные нарушение безопасности информации и причиненный субъекту вред	Есть ли вред	Уровень возможного вреда	Принимаемые меры по обеспечению выполнения обязанностей оператора персональных данных
					информации
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 персональным данным
		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			

№ п/п	**Требования Федерального закона «О персональных данных», которые могут быть нарушены**	**Возможные нарушение безопасности информации**		**Уровень возможного вреда субъекту персональных данных**	**Принимаемые администрацией меры по исключению нанесения возможного вреда**
1.	Обработка персональных данных должна	Целостность		Высокий	Цели обработки персональных

№ п/п	Требования Федерального закона «О персональных данных», которые могут быть нарушены	Возможные нарушение безопасности информации		Уровень возможного вреда субъекту персональных данных	Принимаемые администрацией меры по исключению нанесения возможного вреда
	ограничиваться достижением конкретных, заранее определенных и законных целей	Доступность			данных закреплены в Правилах обработки персональных данных в администрации и в договорах, регламентирующих правоотношения администрации с третьими лицами.
		Конфиденциальность	+		
2.	Не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой	Целостность		Высокий	Соответствующие нормы закреплены в Политике администрации в отношении обработки персональных данных и Правилах обработки персональных данных в администрации
		Доступность			
		Конфиденциальность	+		
3.	Обработке подлежат только персональные данные, которые отвечают целям их обработки	Целостность		Средний	Соответствующие нормы закреплены в Правилах обработки персональных данных в администрации.
		Доступность			
		Конфиденциальность			
4.	Содержание и объем обрабатываемых персональных данных должны соответствовать заявленным целям	Целостность		Средний	Содержание и объем обрабатываемых персональных определены в
		Доступность	+		
		Конфиденци			

№ п/п	Требования Федерального закона «О персональных данных», которые могут быть нарушены	Возможные нарушение безопасности информации		Уровень возможного вреда субъекту персональных данных	Принимаемые администрацией меры по исключению нанесения возможного вреда
	обработки	альность			Правилах обработки персональных данных в администрации.
5.	При обработке персональных данных должны быть обеспечены точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных	Целостность	+	Низкий	Соответствующие нормы закреплены в Правилах обработки персональных данных в администрации.
		Доступность			
		Конфиденциальность			
6.	Хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных	Целостность		Средний	Соответствующие нормы закреплены в Правилах обработки персональных данных в администрации
		Доступность			
		Конфиденциальность			
7.	Лицо, осуществляющее обработку персональных данных по поручению оператора, обязано соблюдать принципы и правила обработки персональных данных, предусмотренные	Целостность	+	Высокий	Необходимые требования закреплены в договорах, регламентирующих правоотношения администрации с
		Доступность	+		
		Конфиденциальность	+		

№ п/п	Требования Федерального закона «О персональных данных», которые могут быть нарушены	Возможные нарушение безопасности информации		Уровень возможного вреда субъекту персональных данных	Принимаемые администрацией меры по исключению нанесения возможного вреда
	настоящим Федеральным законом. В поручении оператора должны быть определены перечень действий (операций) с персональными данными, которые будут совершаться лицом, осуществляющим обработку персональных данных, и цели обработки, должна быть установлена обязанность такого лица соблюдать конфиденциальность персональных данных и обеспечивать безопасность персональных данных при их обработке, а также должны быть указаны требования к защите обрабатываемых персональных данных в соответствии со статьей 19 настоящего Федерального закона				третьими лицами.
8.	Операторы и иные лица, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом	Целостность		Средний	Соответствующие нормы закреплены в организационно-распорядительных документах администрации, регламентирующих обработку и защиту персональных данных и в договорах, регламентирующих правоотношения администрации с
		Доступность			
		Конфиденциальность	+		

№ п/п	Требования Федерального закона «О персональных данных», которые могут быть нарушены	Возможные нарушение безопасности информации		Уровень возможного вреда субъекту персональных данных	Принимаемые администрацией меры по исключению нанесения возможного вреда
					третьими лицами.
9.	В целях информационного обеспечения могут создаваться общедоступные источники персональных данных (в том числе справочники, адресные книги). В общедоступные источники персональных данных с письменного согласия субъекта персональных данных могут включаться его фамилия, имя, отчество, абонентский номер, сведения о профессии и иные персональные данные, сообщаемые субъектом персональных данных	Целостность	+	Средний	Соответствующие нормы закреплены в Правилах обработки персональных данных в администрации. Размещение информации в общедоступных источниках осуществляется на основании письменного согласия субъекта персональных данных.
		Доступность	+		
		Конфиденциальность			
10.	Персональные данные могут быть получены оператором от лица, не являющегося субъектом персональных данных, при условии предоставления оператору подтверждения наличия оснований, указанных в пунктах 2 - 11 части 1 статьи 6, части 2 статьи 10 и части 2 статьи 11 настоящего Федерального закона	Целостность	+	Средний	Соответствующие нормы закреплены в договорах, регламентирующих правоотношения администрации с третьими лицами.
		Доступность	+		
		Конфиденциальность			

№ п/п	Требования Федерального закона «О персональных данных», которые могут быть нарушены	Возможные нарушение безопасности информации		Уровень возможного вреда субъекту персональных данных	Принимаемые администрацией меры по исключению нанесения возможного вреда
11.	Обработка специальных категорий персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни, не допускается, за исключением случаев, предусмотренных частью 2 настоящей статьи	Целостность	+	Средний	Соответствующие нормы закреплены в договорах, регламентирующих правоотношения администрации с третьими лицами.
		Доступность	+		
		Конфиденциальность			
12.	Сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность (биометрические персональные данные) и которые используются оператором для установления личности субъекта персональных данных, могут обрабатываться только при наличии согласия в письменной форме субъекта персональных данных, за исключением случаев, предусмотренных частью 2 настоящей статьи	Целостность	+	Средний	Обработка биометрических персональных данных в администрации не осуществляется
		Доступность			
		Конфиденциальность			
13.	Оператор обязан убедиться в том, что иностранным государством, на территорию которого осуществляется передача персональных данных, обеспечивается адекватная защита прав субъектов персональных данных, до начала осуществления	Целостность	+	Высокий	Соответствующие нормы закреплены в организационно-распорядительных документах администрации, регламентирующих обработку и защиту персональных данных и в
		Доступность	+		
		Конфиденциальность	+		

№ п/п	Требования Федерального закона «О персональных данных», которые могут быть нарушены	Возможные нарушение безопасности информации		Уровень возможного вреда субъекту персональных данных	Принимаемые администрацией меры по исключению нанесения возможного вреда
	трансграничной передачи персональных данных				договорах, регламентирующих правоотношения администрации с третьими лицами.
14.	Субъект персональных данных вправе требовать от оператора уточнения его персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав	Целостность	+	Средний	Соответствующие нормы закреплены в Правилах рассмотрения запросов субъектов персональных данных или их представителей в администрации и других организационно-распорядительных документах администрации, регламентирующих обработку и защиту персональных данных.
		Доступность	+		
		Конфиденциальность			
15.	Субъект персональных данных имеет право на получение информации, касающейся обработки его персональных данных	Целостность		Низкий	Соответствующие нормы закреплены в Правилах рассмотрения запросов субъектов персональных данных или их представителей в администрации и других организационно-распорядительных документах администрации, регламентирующих обработку и защиту персональных данных.
		Доступность	+		
		Конфиденциальность			
		Целостность			
		Доступность			
		Конфиденциальность	+		