Приложение № 5
к Положению об обработке и защите персональных данных в ОГБУ «ЦСА г. Томска»,
утвержденному приказом ОГБУ «ЦСА г. Томска» от 13.09.2021 № 102

ПРАВИЛА
оценки вреда, который может быть причинен субъектам персональных данных в случае нарушения требований по обработке и обеспечению безопасности персональных данных в ОГБУ «ЦСА г. Томска»

1. Общие положения

1.1. Настоящие Правила оценки возможного вреда субъектам персональных данных и принятия мер по его предотвращению (далее – Правила) определяют порядок оценки вреда, который может быть причинён субъектам персональных в случае нарушения федерального законодательства по защите персональных данных, в частности Федерального закона № 152-ФЗ «О персональных данных» (Федеральный закон «О персональных данных»), и отражают соотношение указанного возможного вреда и принимаемых ОГБУ «ЦСА г. Томска» мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных».

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

2. Термины и определения

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. Описание 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 ОГБУ «ЦСА г. Томска» 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.

4. Методика оценки возможного вреда субъектам персональных данных в случае нарушения Федерального закона «О персональных данных»

4.1. Оценка возможного вреда должна производиться коллегиально. В комиссии должно быть не менее трех человек.

4.2. В оценке возможного вреда исходить из учёта последствий допущенного нарушения принципов обработки персональных данных. Вводится четыре уровня возможного вреда:

нулевой – вред субъекту персональных данных не причиняется;

низкий – последствия нарушения принципов обработки персональных данных включают только нарушение целостности персональных данных, либо только нарушение доступности персональных данных;

средний – 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 – во всех остальных случаях.

4.3. Каждому уровню возможного вреда сопоставляется числовая оценка, а именно:

0 – при нулевом уровне вреда;

0,05 – при низком уровне вреда;

0,1 – при среднем уровне вреда;

0,2 – при высоком уровне вреда.

4.4. Каждым членом комиссии на основании собственного субъективного мнения выставляется одна из возможных оценок возможного вреда субъекту для каждой актуальной угрозы безопасности его персональных данных из-за несанкционированного, в том числе случайного, доступа к его персональным данным.

4.5. Все коэффициенты оценок суммируются по каждой актуальной угрозе.

4.6. По значению суммарной оценки Вр определяется возможный вред следующим образом:

если Вр >0,9, то вред субъектам ПДн признается высоким;

если 0,5<Вр ≤0,9, то вред субъектам ПДн признается средним;

если 0,2<Вр ≤0,5, то вред субъектам ПДн признается низким;

если 0 <Вр ≤0,5, то вред субъектам ПДн признается нулевым.

4. Порядок проведения оценки возможного вреда, а также соотнесения возможного вреда и реализуемых ОГБУ «ЦСА г. Томска» мер

Оценка вреда, который может быть причинен субъектам персональных данных в случае нарушения требований Федерального закона «О персональных данных», соотношению указанного вреда и принимаемых ОГБУ «ЦСА г. Томска» мер, направленных на обеспечение выполнения обязанностей, предусмотренных указанным Федеральным законом, осуществляется комиссией по защите персональных данных ОГБУ «ЦСА г. Томска» (далее - Комиссия) в соответствии с Методикой, описанной в разделе 4 настоящих Правил, с составлением акта оценки вреда, который может быть причинен субъекту персональных данных, в случае нарушения требований Федерального закона «О персональных данных» согласно Приложению к настоящим Правилам.

Состав реализуемых ОГБУ «ЦСА г. Томска» мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» определяется Комиссией исходя из правомерности и разумной достаточности указанных мер. При необходимости допускается привлечение сторонних экспертов в области защиты информации.

5. Требования к мерам защиты

5.1. С использованием данных обрабатываемых категориях персональных данных, на основе требований, предъявляемых к обработке персональных данных, предусмотренных действующим законодательством, формулируются и применяются конкретные организационные и технические меры защиты, которые могут быть использованы при обработке персональных данных.

Приложение 1 к правилам оценки вреда, который может быть причинен субъектам персональных данных в случае нарушения требований по обработке и обеспечению безопасности персональных данных в ОГБУ «ЦСА г. Томска»

Соотношение вреда и принимаемых ОГБУ «ЦСА г. Томска» мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных»

№ п\п	Требования Федерального закона «О персональных данных», которые могут быть нарушены	Возможные нарушение безопасности информации и причинённый 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 обеспечению безопасности персональных данных
		Целостность	-		
		Доступность	-		
		Конфиденциальность	+		
2.	Порядок и условия применения средств защиты информации	Убытки и моральный вред	+	средний	Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных
		Целостность	-		
		Доступность	-		
		Конфиденциальность	+		
3.	Эффективность принимаемых мер по обеспечению безопасности	Убытки и моральный вред	+	высокий	В соответствии с Правилами обработки персональных
		Целостность	+		
		Доступность	+		

	персональных данных до ввода в эксплуатацию информационной системы персональных данных	Конфиденциальность	+		данных
4.	Состояние учета машинных носителей персональных данных	Убытки и моральный вред	-	низкий	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
		Целостность	+		
		Доступность	-		
		Конфиденциальность	+		
6.	Наличие (отсутствие) фактов несанкционированного доступа к персональным данным и принятие необходимых мер	Убытки и моральный вред	+	высокий	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	-		

УТВЕРЖДАЮ
Директор ОГБУ «ЦСА г. Томска»

_____ _____

«___» _____ 20__ г.

АКТ
оценки вреда, который может быть причинен субъектам персональных данных в случае нарушения требований по обработке и обеспечению безопасности персональных данных в ОГБУ «ЦСА г. Томска»

Комиссия ОГБУ «ЦСА г. Томска» во исполнение требований пункта 5 части 1 статьи 18.1 Федерального закона «О персональных данных», в составе:

Председатель комиссии:

Директор (Эксперт № 1)	Титова Татьяна Николаевна (ФИО)

Секретарь:

Юрисконсульт (Эксперт № 2)	Фролова Екатерина Николаевна (ФИО)

Члены комиссии:

Заместитель директора (Эксперт № 3)	Ефанов Алексей Викторович (ФИО)
Главный бухгалтер (Эксперт № 4)	Шадрина Юлия Владимировна (ФИО)

руководствуясь Правилами оценки вреда, который может быть причинен субъектам персональных данных в случае нарушения требований по обработке и обеспечению безопасности персональных данных в ОГБУ «ЦСА г. Томска», определила:

Типы актуальных угроз безопасности ПДн	Оценки возможного вреда субъекту ПДн, определенные членами комиссии				Определение возможного вреда (Вр)
	Эксперт 1	Эксперт 2	Эксперт 3	Эксперт 4	
Уничтожение, изменение, блокирование ПДн	Высокий 0,2	Высокий 0,2	Высокий 0,2	Высокий 0,2	Высокий Вр = 1,6
Копирование, предоставление, распространение	Средний 0,1	Средний 0,1	Средний 0,1	Средний 0,1	Средний Вр = 0,8
Использование ПДн в криминальных целях	Средний 0,1	Средний 0,1	Средний 0,1	Средний 0,1	Средний Вр = 0,8
Публикация ПДн в открытом доступе	Средний 0,1	Средний 0,1	Средний 0,1	Средний 0,1	Средний Вр = 0,8
Рекламный СПАМ по телефонной и электронной связи	Средний 0,1	Средний 0,1	Средний 0,1	Средний 0,1	Средний Вр = 0,8

Председатель комиссии:

Директор (Эксперт № 1) _____ (подпись) Титова Татьяна Николаевна (ФИО)

Секретарь:

Юрисконсульт (Эксперт № 2) _____ (подпись) Фролова Екатерина Николаевна (ФИО)

Члены комиссии:

Заместитель директора (Эксперт № 3) _____ (подпись) Ефанов Алексей Викторович (ФИО)

Главный бухгалтер (Эксперт № 4) _____ (подпись) Шадрина Юлия Владимировна (ФИО)

«___» _____ 2020 года