УТВЕРЖДЕНЫ
приказом №
от «03» 10 2022 г.

ПРАВИЛА
оценки возможного вреда субъектам персональных данных и соотнесения указанного вреда с принимаемыми мерами

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

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

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

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

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

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 учёта причинённых убытков и морального вреда, нарушения конфиденциальности, целостности и доступности персональных данных.

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.

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

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1 Настоящие правила оценки возможного вреда субъектам персональных данных и соотнесения указанного вреда с принимаемыми мерами (далее – Правила) определяют порядок оценки вреда, который может быть причинён субъектам персональных данных в случае нарушения Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (далее – Федеральный закон), и отражают соотношение указанного возможного вреда и принимаемых МБОУ «СОШ № 1 с УИОП имени Княжны Ольги Николаевны Романовой» г. Новый Оскол Белгородской области (далее – Учреждение) мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом.

1.2 Настоящие Правила разработаны в соответствии с Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

2. МЕТОДИКА ОЦЕНКИ ВОЗМОЖНОГО ВРЕДА

2.1 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.

2.2 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 Учреждения 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 объёме 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.

2.3 Субъекту персональных данных может быть причинён 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.

2.4 В оценке возможного вреда Учреждение исходит из следующего способа учёта 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.

3. ПОРЯДОК ПРОВЕДЕНИЯ ОЦЕНКИ ВОЗМОЖНОГО ВРЕДА, А ТАКЖЕ СООТНЕСЕНИЯ ВОЗМОЖНОГО ВРЕДА И РЕАЛИЗУЕМЫХ МЕР

3.1 Оценка возможного вреда субъектам персональных данных осуществляется лицом, ответственным за организацию обработки персональных данных, или комиссией в соответствии с методикой, описанной в разделе 2 настоящих Правил, и на основании экспертных значений, приведённых в Приложении 1.

3.2 Состав реализуемых мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом, определяется лицом, ответственным за организацию обработки персональных данных, исходя из правомерности и разумной достаточности указанных в Приложении 1 мер.

3.3 По результатам оценки оформляется акт. Форма акта приведена в Приложении 2.

ПРИЛОЖЕНИЕ 1

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

№ п/п	Требования, которые могут быть нарушены	Возможные нарушение безопасности информации и причинённый субъекту вред		Уровень возможного вреда	Принимаемые меры
1.	Обработка персональных данных должна ограничиваться достижением конкретных, заранее определенных и законных целей (часть 2 статьи 5)	Убытки и моральный вред	+	Высокий	Определены цели обработки.
		Целостность			
		Доступность			
		Конфиденциальность	+		
2.	Не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой (часть 3 статьи 5)	Убытки и моральный вред	+	Высокий	Соответствующие нормы закреплены в Положении об обработке персональных данных.
		Целостность			
		Доступность			
		Конфиденциальность	+		
3.	Обработке подлежат только персональные данные, которые отвечают целям их обработки (часть 4 статьи 5)	Убытки и моральный вред	+	Высокий	Утвержден перечень обрабатываемых персональных данных.
		Целостность			
		Доступность			
		Конфиденциальность	+		
4.	Содержание и объем обрабатываемых персональных данных должны соответствовать заявленным целям обработки (часть 5 статьи 5)	Убытки и моральный вред	+		Определены цели обработки и перечень обрабатываемых персональных данных.
		Целостность			
		Доступность			
		Конфиденциальность	+		
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 (часть 6 статьи 5)	Убытки и моральный вред		Низкий	Соответствующие нормы закреплены в Положении об обработке персональных данных.
		Целостность	+		
		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 (часть 7 статьи 5)	Убытки и моральный вред	+	Высокий	Соответствующие нормы закреплены в Положении об обработке персональных данных.
		Целостность			
		Доступность			
		Конфиденциальность	+		

№ п/п	Требования, которые могут быть нарушены	Возможные нарушение безопасности информации и причинённый субъекту вред		Уровень возможного вреда	Принимаемые меры
7.	Лицо, осуществляющее обработку персональных данных по поручению оператора, обязано соблюдать принципы и правила обработки персональных данных, предусмотренные 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 Федерального закона (часть 3 статьи 6)	Убытки и моральный вред	+	Высокий	Соответствующие нормы закреплены в Положении об обработке персональных данных.
		Целостность			
		Доступность			
		Конфиденциальность	+		
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 (статья 7)	Убытки и моральный вред	+	Высокий	Соответствующие нормы закреплены в Политике в отношении обработки персональных данных. Соответствующие нормы закреплены в договорах, регламентирующих правоотношения с третьими лицами.
		Целостность			
		Доступность			
		Конфиденциальность	+		
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, год и место рождения, адрес, абонентский номер, сведения о профессии и иные персональные данные, сообщаемые субъектом персональных данных (часть 1 статьи 8)	Убытки и моральный вред	+	Высокий	Соответствующие нормы закреплены в Политике в отношении обработки персональных данных.
		Целостность			
		Доступность			
		Конфиденциальность	+		

№ п/п	Требования, которые могут быть нарушены	Возможные нарушение безопасности информации и причинённый субъекту вред		Уровень возможного вреда	Принимаемые меры
10.	Субъект персональных данных принимает решение о предоставлении его персональных данных и дает согласие на их обработку свободно, своей волей и в своем интересе. Согласие на обработку персональных данных может быть дано субъектом персональных данных или его представителем в любой позволяющей подтвердить факт его получения форме, если иное не установлено федеральным законом (часть 1 статьи 9)	Убытки и моральный вред	+	Высокий	Согласия субъектов на обработку их персональных данных фиксируются надлежащим образом, позволяющим подтвердить факт их получения
		Целостность			
		Доступность			
		Конфиденциальность	+		
11.	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 Федерального закона (часть 8 статьи 9)	Убытки и моральный вред	+	Высокий	Соответствующие нормы закреплены в Положении об обработке персональных данных.
		Целостность			
		Доступность			
		Конфиденциальность	+		
12.	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 (часть 1 статьи 10)	Убытки и моральный вред	+	Высокий	Соответствующие нормы закреплены в Политике в отношении обработки персональных данных, а также в Положении об обработке персональных данных.
		Целостность			
		Доступность			
		Конфиденциальность	+		
13.	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 (часть 1 статьи 11)	Убытки и моральный вред	+	Высокий	Соответствующие нормы закреплены в Политике в отношении обработки персональных данных, а также в Положении об обработке персональных данных.
		Целостность			
		Доступность			
		Конфиденциальность	+		

№ п/п	Требования, которые могут быть нарушены	Возможные нарушение безопасности информации и причинённый субъекту вред		Уровень возможного вреда	Принимаемые меры
14.	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 трансграничной передачи персональных данных (часть 3 статьи 12)	Убытки и моральный вред	+	Высокий	Трансграничная передача персональных данных не осуществляется
		Целостность			
		Доступность	+		
		Конфиденциальность	+		
15.	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 (часть 1 статьи 14)	Убытки и моральный вред	+	Средний	Соответствующие нормы закреплены в Политике в отношении обработки персональных данных, а также в Положении об обработке персональных данных.
		Целостность	+		
		Доступность			
		Конфиденциальность			
16.	Субъект персональных данных имеет право на получение информации, касающейся обработки его персональных данных (часть 7 статьи 14)	Убытки и моральный вред	+	Средний	Соответствующие нормы закреплены в Положении об обработке персональных данных.
		Целостность			
		Доступность	+		
		Конфиденциальность			
17.	Решение, порождающее юридические последствия в отношении субъекта персональных данных или иным образом затрагивающее его права и законные интересы, может быть принято на основании исключительно автоматизированной обработки его персональных данных только при наличии согласия в письменной форме субъекта персональных данных или в случаях, предусмотренных федеральными законами, устанавливающими также меры по обеспечению соблюдения прав и законных интересов субъекта персональных данных (часть 2 статьи 16)	Убытки и моральный вред	+	Высокий	Соответствующие нормы закреплены в Политике в отношении обработки персональных данных, а также в Положении об обработке персональных данных.
		Целостность			
		Доступность			
		Конфиденциальность	+		

ПРИЛОЖЕНИЕ 2

Типовая форма акта оценки возможно вреда субъектам персональных данных

«___» _____ 20__ г. г. Новый Оскол № _____

Комиссия в составе:
председатель комиссии

_____
(Ф.И.О., должность)

члены комиссии

_____
(Ф.И.О., должность)

_____
(Ф.И.О., должность)

провела оценку вреда, который может быть причинен субъектам персональных данных в случае нарушения МБОУ «СОШ № 1 с УИОП имени Княжны Ольги Николаевны Романовой» г. Новый Оскол Белгородской области обязанностей, предусмотренных Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, определила, что на основе возможных нарушений безопасности информации, уровня возможно вреда, в случае нарушения, а также соотнесении указанного вреда с принимаемыми мерами, субъектам персональных данных может быть причинен вред, который оценивает как _____ .
(уровень вреда)

Председатель комиссии:

_____	_____	_____
(должность)	*(подпись)*	*(Ф.И.О.)*

Члены комиссии:

_____	_____	_____
(должность)	*(подпись)*	*(Ф.И.О.)*
_____	_____	_____
(должность)	*(подпись)*	*(Ф.И.О.)*