

МУНИЦИПАЛЬНОЕ БЮДЖЕТНОЕ ДОШКОЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ «ИНЖАВИНСКИЙ ДЕТСКИЙ САД «БЕРЕЗКА»

ПРИКАЗ

«01» _____ 12 _____ 2023 г.

№68/16

р.п. Инжавино

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

Во исполнение требований пункта 5 части 1 статьи 18.1 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» (в редакции от 30.06.2018):

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 МБДОУ «Инжавинский детский сад «Березка».
2. Назначить заведующего ответственным за оценку вреда, который может быть причинен субъектам персональных данных в случае нарушения требований по обработке и обеспечению безопасности персональных данных в МБДОУ «Инжавинский детский сад «Березка».
3. Руководителям структурных подразделений МБДОУ «Инжавинский детский сад «Березка» ознакомить под подпись сотрудников с настоящим приказом.
4. Контроль за исполнением настоящего приказа возложить на заведующего.

Заведующий

Л.А. Ивкина

ПРАВИЛА

оценки вреда, который может быть причинен субъектам персональных данных в случае нарушения требований по обработке и обеспечению безопасности персональных данных в МБДОУ «Инжавинский детский сад «Березка»

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 в МБДОУ «Инжавинский детский сад «Березка», (далее - Правила) определяют порядок оценки вреда, который может быть причинён субъектам персональных данных в случае нарушения от 27.07.2006 № 152-ФЗ «О персональных данных» (далее - Закон № 152-ФЗ), и отражают соотношение указанного возможного вреда и принимаемых МБДОУ «Инжавинский детский сад «Березка» (далее - Оператор) мер, направленных на обеспечение выполнения обязанностей, предусмотренных Законом № 152-ФЗ.

1.2. Настоящие Правила разработаны в соответствии с требованиями действующего законодательства Российской Федерации в области обработки и защиты персональных данных.

2. ОСНОВНЫЕ ПОНЯТИЯ

2.1. В настоящих Правилах используются основные понятия, приведенные в Гражданском кодексе Российской Федерации, в Федеральном законе от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», в Федеральном законе от 27.07.2006 № 152-ФЗ «О персональных данных».

2.2. В настоящих Правилах используются основные понятия:

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

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

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

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

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

2.6.6. 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.

2.2.7. 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.

2.2.8. 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:

3.2.1. Нарушение конфиденциальности персональных данных:

а) неправомерное предоставление, распространение и копирование персональных данных;

б) обработка персональных данных, выходящая за рамки установленных целей обработки, в объеме больше необходимого;

в) неправомерное получение персональных данных от лица, не являющегося субъектом персональных данных;

г) принятие решения, порождающего юридические последствия в отношении субъекта персональных данных или иным образом затрагивающего права и законные интересы, на основании исключительно автоматизированной обработки его персональных данных без согласия на то в письменной форме субъекта персональных данных или не предусмотренного федеральными законами;

3.2.2. Нарушение доступности персональных данных:

а) нарушение права субъекта на получение информации, касающейся обработки его персональных данных;

б) неправомерное уничтожение и блокирование персональных данных;

3.2.3. Нарушение целостности персональных данных:

а) неправомерное изменение персональных данных;

б) нарушение права субъекта требовать от Оператора уточнения его персональных данных, их блокирования или уничтожения.

3.3. Вред, который может быть причинён субъекту персональных данных, определяется в виде:

а) убытков – расходов;

б) недополученного дохода, который этот субъект персональных данных получил бы при обычных условиях гражданского оборота, если бы его право не было нарушено;

в) морального вреда.

3.4. В оценке возможного вреда необходимо исходить из следующего способа учёта последствий допущенного нарушения принципов обработки персональных данных:

а) низкий уровень возможного вреда - последствия нарушения принципов обработки персональных данных включают только нарушение целостности персональных данных, либо

только нарушение доступности персональных данных;

б) 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;

в) 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 проводится для исполнения требований к защите персональных данных при их обработке в информационной системе персональных данных (далее - ИСПДн), в частности, при определении типа актуальных угроз безопасности персональных данных при их обработке в ИСПДн во исполнение п. 5 ч. 1 ст. 18.1 Закона № 152-ФЗ.

4.2. Оценка возможного вреда субъектам персональных данных и состав реализуемых Оператором мер, направленных на обеспечение выполнения обязанностей, предусмотренных Законом № 152-ФЗ, осуществляется должностными лицами МБДОУ «Инжавинский детский сад «Березка» в соответствии с методикой оценки возможного вреда субъектам персональных данных, определенной в разделе 3 настоящих Правил, и на основании оценки вреда, который может быть причинен субъектам персональных данных, а также соотнесения возможного вреда и реализуемых Оператором мер, приведенных в приложении к Правилам, исходя из правомерности и разумной достаточности указанных мер. При необходимости допускается привлечение сторонних экспертов в области защиты информации.

к правилам оценки вреда, который может быть причинен субъектам персональных данных в случае нарушения требований по обработке и обеспечению безопасности персональных данных в МБДОУ «Инжавинский детский сад «Березка»

ОЦЕНКА ВРЕДА, КОТОРЫЙ МОЖЕТ БЫТЬ ПРИЧИНЕН СУБЪЕКТАМ ПЕРСОНАЛЬНЫХ ДАННЫХ, А ТАКЖЕ СООТНЕСЕНИЕ ВОЗМОЖНОГО ВРЕДА И РЕАЛИЗУЕМЫХ ОПЕРАТОРОМ МЕР

При определении уровня возможного вреда необходимо учитывать, что сами по себе нарушения целостности и доступности могут принести наименьший вред субъекту персональных данных, так как субъект персональных данных может и имеет право требовать восстановления целостности и доступности.

Если такое правомочие субъекта персональных данных затруднено, считается, что имеется основание для судебного иска, поэтому нарушение целостности или доступности, повлекшие моральный вред или ущерб, отнесены к среднему уровню вреда.

Если нарушение конфиденциальности потенциально необратимо (ставшие публичными данные невозможно снова сделать конфиденциальными), то даже в случае, если оно не повлекло причинение морального вреда субъекту персональных данных, такое нарушение относится к среднему уровню возможного вреда.

Если нарушения конфиденциальности повлекли за собой моральный ущерб и убытки, то такие нарушения относятся к наивысшему уровню возможного вреда.

Таблица 1. Оценка уровня возможного вреда

Требования Закона № 152-ФЗ, 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	+	высокий	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	В соответствии с технической документацией на систему защиты информационной системы персональных данных
	Целостность	+		
	Доступность			
	Конфиденциальность			

Требования Закона № 152-ФЗ, которые могут быть нарушены	Возможные нарушения безопасности информации и причиненный субъекту вред		Уровень возможного вреда	Принимаемые меры по обеспечению выполнения обязанностей Оператора персональных данных
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			
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	+	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		средний	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			

