Минобрнауки России
Федеральное государственное бюджетное научное учреждение
«Федеральный исследовательский центр
Институт прикладной физики им. А.В. Гапонова-Грехова
Российской академии наук»
(ИПФ РАН)

ПРИКАЗ

23.05.2024 № 201

Нижний Новгород

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

Во исполнение требований Федерального закона №152-ФЗ от 27.07.2006 г. «О персональных данных» и прочих нормативных документов по защите информации п р и к а з ы в а ю:

1. Утвердить:

1.1 Правила оценки вреда, который может быть причинен субъекту (субъектам) персональных данных в случае нарушения требований по обработке и обеспечению безопасности персональных данных (Приложение 1) в Федеральном государственном бюджетном научном учреждении «Федеральный исследовательский центр Институт прикладной физики им. А.В. Гапонова-Грехова Российской академии наук» (далее – Правила).

1.2 Оценку вреда, который может быть причинен субъектам персональных данных, а также соотнесение возможного вреда и реализуемых оператором мер (Приложение 2).

1.3 Состав комиссии по оценке вреда, который может быть причинен субъекту (субъектам) персональных данных в случае нарушения требований по обработке и обеспечению безопасности персональных данных. (Приложению 3).

1.4 Акт оценки вреда, который может быть причинен субъекту (субъектам) персональных данных в случае нарушения требований по обработке и обеспечению безопасности персональных данных. (Приложению 4).

2. Контроль за исполнением приказа оставляю за собой.

Директор
академик РАН  Г.Г. Денисов

Приложение № 1 к приказу
от "23".05. 2024 г. № 201

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

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 закона № 152-ФЗ «О персональных данных» (далее - № 152-ФЗ), и отражают соотношение указанного возможного вреда и принимаемых оператором мер, направленных на обеспечение выполнения обязанностей, предусмотренных № 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. Оператор для целей оценки вреда определяет одну из степеней вреда, который может быть причинен субъекту персональных данных в случае нарушения Закона о персональных данных.

3.4.1. Высокая степень вреда устанавливается в случаях:

-обработки оператором сведений, 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, за исключением случаев, установленных федеральными законами, предусматривающими цели, порядок и условия обработки биометрических персональных данных;

- обработки Оператором специальных категорий персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни, сведений о судимости, за исключением случаев, установленных федеральными законами, предусматривающими цели, порядок и условия обработки специальных категорий персональных данных;

- обработки Оператором персональных данных несовершеннолетних для исполнения договора, стороной которого либо выгодоприобретателем или поручителем по которому является несовершеннолетний, а также для заключения договора по инициативе несовершеннолетнего или договора, по которому несовершеннолетний будет являться выгодоприобретателем или поручителем в случаях, не предусмотренных законодательством Российской Федерации;

- обезличивания персональных данных, в том числе с целью проведения оценочных исследований, оказания услуг по прогнозированию поведения потребителей товаров и услуг, а также иных исследований, не предусмотренных пунктом 9 части 1 статьи 6 Закона о персональных данных;

- поручения иностранному лицу (иностранным лицам) осуществлять обработку персональных данных граждан Российской Федерации;
- сбора персональных данных с использованием баз данных, находящихся за пределами Российской Федерации.

3.4.2. Средняя степень вреда устанавливается в случаях:
- распространения персональных данных на официальном сайте Оператора в сети Интернет, а равно предоставление персональных данных неограниченному кругу лиц, за исключением случаев, установленных федеральными законами, предусматривающими цели, порядок и условия такой обработки персональных данных;
- обработки персональных данных в дополнительных целях, отличных от первоначальной цели сбора;
- продвижения товаров, работ, услуг на рынке путем осуществления прямых контактов с потенциальным потребителем с использованием баз персональных данных, владельцем которых является иной оператор;
- получения согласия на обработку персональных данных посредством реализации на официальном сайте в сети Интернет функционала, не предполагающего дальнейшую идентификацию и (или) аутентификацию субъекта персональных данных;
- осуществления деятельности по обработке персональных данных, предполагающей получение согласия на обработку персональных данных, содержащего положения о предоставлении права осуществлять обработку персональных данных определенному и (или) неопределенному кругу лиц в целях, несовместимых между собой.

3.4.3. Низкая степень вреда устанавливается в случаях:
- ведения общедоступных источников персональных данных.

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 за организацию обработки персональных данных, в соответствии с методикой, описанной в разделе 3 настоящих Правил, и на основании экспертных значений, приведённых в Приложении.

4.2. Состав реализуемых Оператором мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных», определяется лицом, ответственным за организацию обработки персональных данных, исходя из правомерности и разумной достаточности указанных мер.

5 Оформление результатов оценки вреда

Результаты оценки вреда оформляются актом оценки вреда.

Акт оценки вреда должен содержать:

а) наименование или фамилию, имя, отчество (при наличии) и адрес оператора;

б) дату издания акта оценки вреда;

в) дату проведения оценки вреда;

г) фамилию, имя, отчество (при наличии), должность лиц (лица) (при наличии),
проводивших оценку вреда, а также их (его) подпись;

д) степень вреда, которая может быть причинена субъекту персональных данных,
определенная в соответствии с методикой оценки вреда, указанной в разделе 4 настоящего регламента.

Акт оценки вреда в электронной форме, подписанный в соответствии с федеральным законом электронной подписью, признается электронным документом, равнозначным акту оценки вреда на бумажном носителе, подписанному собственноручной подписью. В случае если по итогам проведенной оценки вреда установлено, что в рамках деятельности по обработке персональных данных субъекту персональных данных в соответствии с методикой оценки вреда могут быть причинены различные степени вреда, подлежит применению более высокая степень вреда.

Приложение № 2 к приказу
от "23".05. 2024 г. № 201

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

№	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	Применение 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 Положение об организации обработки и защите персональных данных, обрабатываемых в ИПФ РАН
		Целостность	-		
		Доступность	-		
		Конфиденциальность	+		
2	Применение средств защиты информации.	Убытки и моральный вред	+	средний	В соответствии с технической документацией на средства защиты ИСПД
		Целостность	+		
		Доступность	-		
		Конфиденциальность	-		
3	Соблюдение правил доступа к персональным данным	Убытки и моральный вред	+	высокий	В соответствии с принятыми организационными мерами и в соответствии с разграничения доступа
		Целостность	+		
		Доступность	-		
		Конфиденциальность	+		
4	Отсутствие фактов несанкционированного доступа к персональным данным и принятие необходимых мер.	Убытки и моральный вред	+	средний	Контроль сохранности средств защиты информации от несанкционированного доступа
		Целостность	-		
		Доступность	-		
		Конфиденциальность	+		
5	Осуществление мероприятий по обеспечению целостности персональных данных.	Убытки и моральный вред	-	низкий	Организация режима доступа к техническим и программным средствам
		Целостность	+		
		Доступность	-		
		Конфиденциальность	-		

Приложение № 3 к приказу
от "23".05. 2024 г. № 201

Состав комиссии по оценке вреда, который может быть причинен субъектам персональных данных, а также соотнесение возможного вреда и реализуемых оператором мер

Заместитель директора по общим вопросам и экономике	Председатель комиссии
Помощник директора по обеспечению информационной безопасности	Член комиссии
Заведующий отделом кадров	Член комиссии
Ведущий юрисконсульт	Член комиссии

Приложение № 4к приказу
от "23".05. 2024 г. № 201

Минобрнауки России
Федеральное государственное бюджетное научное учреждение
«Федеральный исследовательский центр
Институт прикладной физики им. А.В. Гапонова-Грехова
Российской академии наук»
(ИПФ РАН)

УТВЕРЖДАЮ
Директор
академик РАН
_____ /Г.Г. Денисов/
«___» _____ 2024 г.

Акт по оценке вреда,
который может быть причинен субъектам персональных данных,
а также соотнесение возможного вреда и реализуемых оператором мер

Комиссия в составе:

	ФИО	Должность
Председатель комиссии		
Члены комиссии:		

составила настоящий акт о том, что согласно описи, утвержденной актом №____ от _____ 20__ года, во исполнение Федерального закона от 27.07.2006 № 152 ФЗ «О персональных данных» и приказа Роскомнадзора от 27.10.2022 № 178 «Об утверждении Требований к оценке вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона “О персональных данных”» составила акт по результатам оценки вреда:

№	Действия, которые осуществляет организация при обработке персональных данных	Степень вреда, который может быть причинен субъекту персональных данных при нарушении
1		
2		

Проводили оценку вреда:
Председатель комиссии: _____/_____/
Члены комиссии: _____/_____/
_____/_____/

Дата проведения оценки вреда: _____ 202_ года

Лист ознакомления с Правилами оценки вреда, который может быть причинен субъекту (субъектам) персональных данных в случае нарушения требований по обработке и обеспечению безопасности персональных данных от "23".05. 2024 г. № 201		
Занимаемая должность, дата ознакомления	Подпись	И. О. Фамилия
"___" _____ 20___ г.		
"___" _____ 20___ г.		
"___" _____ 20___ г.		
"___" _____ 20___ г.		
"___" _____ 20___ г.		
"___" _____ 20___ г.		
"___" _____ 20___ г.		
"___" _____ 20___ г.		
"___" _____ 20___ г.		
"___" _____ 20___ г.		
"___" _____ 20___ г.		
"___" _____ 20___ г.		
"___" _____ 20___ г.		
"___" _____ 20___ г.		
"___" _____ 20___ г.		
"___" _____ 20___ г.		
"___" _____ 20___ г.		
"___" _____ 20___ г.		