

РОССИЙСКАЯ ФЕДЕРАЦИЯ
ДЕПАРТАМЕНТ КУЛЬТУРЫ БРЯНСКОЙ ОБЛАСТИ
ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ УЧРЕЖДЕНИЕ
ДОПОЛНИТЕЛЬНОГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ
«БРЯНСКИЙ ОБЛАСТНОЙ УЧЕБНО-МЕТОДИЧЕСКИЙ
ЦЕНТР КУЛЬТУРЫ И ИСКУССТВА»

ПРИКАЗ

06.02.2020г.

№ 201

г. Брянск

Об утверждении Правил оценки вреда, который может быть причинен субъектам персональных данных в случае нарушения требований по обработке и обеспечению безопасности персональных данных в ГБУ ДПО «Брянский областной учебно-методический центр культуры и искусства»

Во исполнение требований пункта 5 части 1 статьи 18.1 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»

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 информационных системах персональных данных ГБУ ДПО «Брянский областной учебно-методический центр культуры и искусства» (Приложение 1).

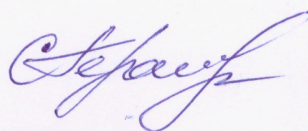
2. Назначить главного бухгалтера Яковлеву Н.В. ответственным за оценку вреда, который может быть причинен субъектам персональных данных в случае нарушения требований по обработке и обеспечению безопасности персональных данных в информационных системах персональных данных ГБУ ДПО «Брянский областной учебно-методический центр культуры и искусства».

3. Делопроизводителю Бардиной Л.Ю. ознакомить работников под подпись с настоящим приказом.

4. Заведующей отделом повышения квалификации и переподготовки кадров Ященко Е.А. разместить настоящий приказ в информационно-телекоммуникационной сети «Интернет» на официальном сайте ГБУ ДПО «Брянский областной учебно-методический центр культуры и искусства»

5. Контроль за исполнением приказа оставляю за собой.

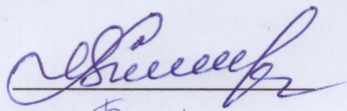
Директор



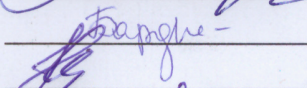
С.Н. Геращенко

С настоящим приказом ознакомлены:

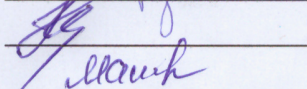
Яковлева Н.В.



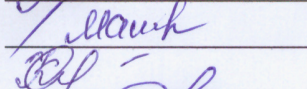
Бардина Л.Ю.



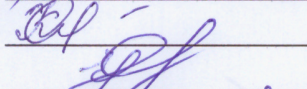
Ширко Ж.П.



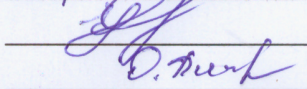
Маштакова О.А.



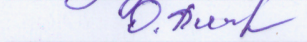
Клименко О.В.



Яценко Е.А.



Филькина О.М.



УТВЕРЖДЕНО

приказом директора ГБУ ДПО «Брянский
областной учебно-методический центр
культуры и искусства»

от «06» февраля 2020 г. № 20/1

Правила оценки вреда, который может быть причинен субъектам персональных данных в случае нарушения требований по обработке и обеспечению безопасности персональных данных в ГБУ ДПО «Брянский областной учебно-методический центр культуры и искусства»

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 информационных системах персональных данных ГБУ ДПО «Брянский областной учебно-методический центр культуры и искусства» (далее - Правила), определяют порядок оценки вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона № 152-ФЗ "О персональных данных" (далее - Закон № 152-ФЗ), и отражают соотношение указанного возможного вреда и принимаемых ГБУ ДПО «Брянский областной учебно-методический центр культуры и искусства» (далее - Оператор) мер, направленных на обеспечение выполнения обязанностей, предусмотренных Законом № 152-ФЗ.

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

2. Основные понятия

В настоящих Правилах используются основные понятия, приведенные в Гражданском кодексе Российской Федерации, в Федеральном законе от 27.07.2006 1149-ФЗ "Об информации, информационных технологиях и о защите информации" и в Федеральном законе от 27.07.2006 152-ФЗ "О 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:

нарушение конфиденциальности персональных данных:

неправомерное предоставление, распространение и копирование персональных данных;

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

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

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;

нарушение доступности персональных данных:

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

неправомерное уничтожение и блокирование персональных данных;

нарушение целостности персональных данных:

неправомерное изменение персональных данных;

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

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

убытков - расходов, которые субъект персональных данных, чье право нарушено, понесло или должно будет понести для восстановления нарушенного права, утраты или повреждения его имущества (реальный ущерб);

недополученного дохода, который этот субъект персональных данных получил 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 субъекта персональных данных либо посягающими на принадлежащие субъекту персональных данных другие нематериальные блага, а также в других случаях, предусмотренных законом.

3.4. В оценке возможного вреда необходимо исходить из следующего способа учета 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.

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

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.

Оценка возможного вреда субъектам персональных данных и состав реализуемых Оператором мер, направленных на обеспечение выполнения обязанностей, предусмотренных Законом № 152-ФЗ, осуществляется ответственным структурным подразделением Оператора 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.

Приложение
к Правилам оценки вреда,
который может быть причинен
субъектам персональных данных в
случае нарушения требований по
обработке и обеспечению
безопасности персональных данных в
информационных системах
персональных данных ГБУ ДПО
«Брянский областной учебно-
методический центр культуры и
искусства»

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

1.1. 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.

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

1.3. 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.

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

2. Оценка уровня возможного вреда

Требования Федерального закона от 27.07.2006 152-ФЗ "О персональных данных", которые могут быть нарушены	Возможные нарушения безопасности информации и причиненный субъекту вред	Уровень возможного вреда	Принимаемые меры по обеспечению выполнения обязанностей Оператора
1	2	3	4
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 + Целостность Доступность Конфиденциальность +	Высокий	В соответствии с законодательством в области защиты информации и Положением по обеспечению безопасности персональных данных
2. Порядок и условия применения средств защиты информации	Убытки и моральный вред + Целостность + Доступность Конфиденциальность	Средний	В соответствии с технической документацией на систему защиты информационной системы персональных данных
3. Эффективность принимаемых мер по обеспечению безопасности	Убытки и моральный вред + Целостность + Доступность +	Высокий	Программа и методика испытаний систем защиты

персональных данных до ввода в эксплуатацию информационной системы персональных данных	Конфиденциальность +		
4. Состояние учета машинных носителей персональных данных	Убытки и моральный вред Целостность Доступность Конфиденциальность		Инструкция по учету машинных носителей информации
5. Соблюдение правил доступа к персональным данным	Убытки и моральный вред + Целостность + Доступность Конфиденциальность +	Высокий	В соответствии с принятыми организационными мерами и в соответствии с системой разграничения доступа
6. Наличие (отсутствие) фактов несанкционированного доступа к персональным данным и принятие необходимых мер	Убытки и моральный вред + Целостность Доступность Конфиденциальность +	Высокий	Мониторинг средств защиты информации на наличие фактов доступа к персональным данным
7. Мероприятия по восстановлению персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним	Убытки и моральный вред Целостность + Доступность + Конфиденциальность	Средний	Применение резервного копирования
8. Осуществление мероприятий по обеспечению целостности персональных данных	Убытки и моральный вред Целостность + Доступность Конфиденциальность	Низкий	Организация режима доступа к техническим и программным средствам