**Муниципальное автономное общеобразовательное учреждение**
**Городского округа «город Ирбит» Свердловской области**
**«Средняя общеобразовательная школа № 10»**

Принято
Педагогическим советом,
от 27.08. 2021 г.,
протокол № 6

Утверждено
приказом директора
МАОУ «Школа № 10»
от 31.08.2021г. № 46-ОД/17

# Правила
# оценки вреда, который может быть причинен субъектам персональных данных в случае нарушения требований по обработке и обеспечению безопасности персональных данных в МАОУ «Школа № 10»

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 МАОУ «Школа №10», (далее – Правила) определяют порядок оценки вреда, который может быть причинён субъектам персональных в случае нарушения Федерального закона № 152-ФЗ «О персональных данных» (далее – Закон № 152-ФЗ), и отражают соотношение указанного возможного вреда и принимаемых МАОУ «Школа №10» (далее – Оператор) мер, направленных на обеспечение выполнения обязанностей, предусмотренныхЗаконом № 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 вФедеральном 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:

1. нарушение конфиденциальности персональных данных:

- неправомерное предоставление, распространение и копирование персональных данных;
- обработка персональных данных, выходящая за рамки установленных целей обработки, в объёме 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;

2. нарушение доступности персональных данных:

- нарушение права субъекта на получение информации, касающейся обработки его персональных данных;
- неправомерное уничтожение и блокирование персональных данных;

3. 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 причинён 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 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 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.

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 определение 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, предусмотренныхЗаконом № 152-ФЗ, осуществляется должностными лицами управления информационных технологий, связи и документооборота администрации области 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 администрации области

**Оценка вреда, который может быть причинен субъектам персональных данных, а также соотнесение возможного вреда и реализуемых мер в Муниципальном автономном общеобразовательном учреждении Городского округа «город Ирбит» Свердловской области «Средняя общеобразовательная школа №10»**

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 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 персональных данных** |
|---|---|---|---|---|
| **1** | **2** | | **3** | **4** |
| 1. Порядок и условия применения организационных и технических мер по обеспечению безопасности персональных данных при их | Убытки и моральный вред | + | высокий | В соответствии с законодательством в области защиты информации и Политика обработки персональных данных. Положение об обработке персональных данных |
| | Целостность | | | |
| | Доступность | | | |
| | Конфиденциальность | + | | |

| | | | | |
|---|---|---|---|---|
| обработке, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные уровни защищенности персональных данных | | | | работников.<br>Положение об обработке персональных данных учащихся и третьих лиц |
| 2. Порядок и условия применения средств защиты информации | Убытки и моральный вред | + | средний | 1)ПД на бумажных и материальных носителях хранятся в закрытых сейфах (согласно приказа)<br>2)технические средства, используемые для работы с ИСПДн, обеспечены: лицензионным программным обеспечение «Антивирус Касперского» и защищенным каналом связи (ПО ViPNet Client), используемые для работы с ИСПДн, защищены от несанкционированного проникновения в систему, в том числе случайного, путем ограничения лиц, имеющих доступ в помещение где расположено техническое средство, установка пароля защиты на все технические средства на которых ведется работа в ИСПДн |
| | Целостность | + | | |
| | Доступность | | | |
| | Конфиденциальность | | | |
| 3. Эффективность принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных | Убытки и моральный вред | + | высокий | Программа и методика испытаний систем защиты |
| | Целостность | + | | |
| | Доступность | + | | |
| | Конфиденциальность | + | | |

| | | | | |
|---|---|---|---|---|
| данных | | | | |
| 4. Учет машинных носителей персональных данных | Убытки и моральный вред | | | Учет машинных носителей определен «перечнем мест утвержденный приказом» |
| | Целостность | | | |
| | Доступность | | | |
| | Конфиденциальность | | | |
| 5. Соблюдение правил доступа к персональным данным | Убытки и моральный вред | + | высокий | Утверждение приказом списка работников, помещений, в которых содержатся и хранятся ПДн списка лиц, имеющих право доступа в данные помещения |
| | 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 осуществляется комиссией по проведению внутреннего контроля работы с персональными данными в соответствии с требованиями законодательства в сфере обработки персональных данных |
| | 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: утверждение приказом списка работников допущенных к обработке ПДн помещений, в которых содержатся и хранятся ПДн списка лиц, имеющих право доступа в |
| | Целостность | + | | |
| | Доступность | | | |
| | Конфиденциальность | | | |

| | | | | |
|---|---|---|---|---|
| | | | | помещения, в которых хранятся персональные данные |