ПРИЛОЖЕНИЕ № 12

к приказу ГБУК ИЛМ «А.П. Чехов и Сахалин»

 от 27.07.2022 г. №229

**МЕТОДИКА**

 **оценки вреда, который может быть причинен субъектам персональных данных**

1. Настоящая Методика определяет порядок оценки вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» (далее - Федеральный закон № 152-ФЗ), и отражает соотношение указанного возможного вреда и принимаемых ГБУК ИЛМ «А.П. Чехов и Сахалин» (далее - Оператор) мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом № 152-ФЗ.

2. 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. Перечисленные в пункте 2 настоящей Методики неправомерные действия определяются как следующие нарушения безопасности информации:

3.1. Неправомерное предоставление, распространение и копирование персональных данных являются нарушением конфиденциальности персональных данных;

3.2. Неправомерное уничтожение и блокирование персональных данных являются нарушением доступности персональных данных;

3.3. Неправомерное изменение персональных данных является нарушением целостности персональных данных;

3.4. Нарушение права субъекта персональных данных требовать от Оператора уточнения его персональных данных, их блокирования или уничтожения является нарушением целостности информации;

3.5. Нарушение права субъекта персональных данных на получение информации, касающейся обработки его персональных данных, является нарушением доступности персональных данных;

3.6. Обработка персональных данных, выходящая за рамки установленных и законных целей обработки, в объеме больше необходимого для достижения установленных и законных целей и дольше установленных сроков является нарушением конфиденциальности персональных данных;

3.7. Неправомерное получение персональных данных от лица, не являющегося субъектом персональных данных, является нарушением конфиденциальности персональных данных;

3.8. Принятие решения, порождающего юридические последствия в отношении субъекта персональных данных или иным образом затрагивающего его права и законные интересы, на основании исключительно автоматизированной обработки его персональных данных без согласия на то в письменной форме субъекта персональных данных или не предусмотренное федеральными законами, является нарушением конфиденциальности персональных данных.

4. Субъекту персональных данных может быть причинен вред в форме:

4.1. 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;

4.2. 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.

5. В оценке возможного вреда Оператор исходит из следующего способа учета последствий допущенного нарушения принципов обработки персональных данных:

5.1. Низкий уровень возможного вреда - последствия нарушения принципов обработки персональных данных включают только нарушение целостности персональных данных либо только нарушение доступности персональных данных;

5.2. 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;

5.3. Высокий уровень возможного вреда - во всех остальных случаях.

6. Оценка вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона № 152-ФЗ, и соотношение указанного возможного вреда и принимаемых Оператором мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом № 152-ФЗ, приведены в таблице №1.

Таблица № 1

| **№ п/п** | **Требования Закона, которые могут быть нарушены** | **Возможные нарушения безопасности информации и причиненный субъекту персональных данных вред** | **Уровень возможного вреда** | **Меры, принимаемые Оператором, направленные на обеспечение выполнения обязанностей** |
| --- | --- | --- | --- | --- |
| **1** | **2** | **3** | **4** | **5** |
| 1. | Определение угроз безопасности персональных данных при их обработке в информационных системах персональных данных | Убытки и моральный вред | + | Высокий | Актуализация моделей угроз безопасности персональных данных |
| Целостность | + |
| Доступность | + |
| Конфиденциальность | + |
| 2. | 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 Российской Федерации в области защиты информации и Положением об обработке персональных данных в ГБУК ИЛМ «А.П. Чехов и Сахалин» |
| Целостность | + |
| Доступность | + |
| Конфиденциальность | + |
| 3. | Порядок и условия применения прошедших в установленном порядке процедуру оценки соответствия средств защиты информации | Убытки и моральный вред | + | Средний | В соответствии с технической документацией на защиту информационных систем, содержащих персональные данные и применение сертифицированных средств защиты информации |
| Целостность | + |
| Доступность |  |
| Конфиденциальность |  |
| 4. | Эффективность принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных | Убытки и моральный вред | + | Высокий | Проведение проверки эффективности мер защиты информационных систем, содержащих персональные данные |
| Целостность | + |
| Доступность | + |
| Конфиденциальность | + |
| 5. | Состояние учета машинных носителей персональных данных | Убытки и моральный вред |  | Средний | Ведение учета машинных носителей информации |
| Целостность | + |
| Доступность | + |
| Конфиденциальность |  |
| 6. | 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 | + |
| 7. | Наличие (отсутствие) фактов несанкционированного доступа к персональным данным и принятие необходимых мер | Убытки и моральный вред | + | Средний | Мониторинг средств защиты информации на наличие фактов доступа к персональным данным |
| Целостность |  |
| Доступность |  |
| Конфиденциальность | + |
| 8. | Мероприятия по восстановлению персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним | Убытки и моральный вред |  | Средний | Применение резервного копирования |
| Целостность | + |
| Доступность | + |
| Конфиденциальность |  |
| 9. | Контроль за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем, содержащих персональные данные | Убытки и моральный вред |  | Высокий | Осуществление Оператором внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в ГБУК ИЛМ «А.П. Чехов и Сахалин» |
| Целостность | + |
| Доступность | + |
| Конфиденциальность | + |