Приложение № 7

к приказу от \_\_\_\_ 10.2018г. № \_\_\_\_\_

**Правила**

**оценки вреда, который может быть причинен субъектам персональных данных в случае нарушения требований по обработке и обеспечению безопасности персональных данных в ГБУЗ РК «Черноморская ЦРБ»**

### **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 (далее - Правила) в ГБУЗ РК «Черноморская ЦРБ» определяют порядок оценки вреда, который может быть причинен субъектам персональных данных в случае нарушения» (далее - ФЗ № 152-ФЗ), и отражают соотношение указанного возможного вреда и принимаемых оператором мер, направленных на обеспечение выполнения обязанностей, предусмотренных ФЗ № 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:

**Информация** - сведения (сообщения, данные) независимо от формы их представления; **Безопасность информации** - состояние защищенности информации, при котором обеспечены ее конфиденциальность, доступность и целостность;

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

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

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

**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;

**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;

**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:

* Неправомерное предоставление, распространение и копирование персональных данных являются нарушением конфиденциальности персональных данных;
* Неправомерное уничтожение и блокирование персональных данных является нарушением доступности персональных данных;
* Неправомерное изменение персональных данных является нарушением целостности персональных данных;
* Нарушение права субъекта требовать от оператора уточнения его персональных данных, их блокирования или уничтожение является нарушением целостности информации;
* Нарушение права субъекта на получение информации, касающейся обработки его персональных данных, является нарушением доступности персональных данных;
* 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;
* Неправомерное получение персональных данных от лица, не являющегося субъектом персональных данных, является нарушением конфиденциальности персональных данных;
* 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 причинен вред в форме:

* 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;
* 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. В оценке возможного вреда ГБУЗ РК «Черноморская ЦРБ» исходит 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 ГБУЗ РК «Черноморская ЦРБ» мер**

4.1. Оценка возможного вреда субъектам персональных данных осуществляется лицом, ответственным за защиту информации, в соответствии с методикой, описанной в разделе 3 настоящих Правил, и на основании экспертных значений, приведенных в Приложении 1.

4.2. Состав реализуемых ГБУЗ РК «Черноморская ЦРБ» мер, направленных на обеспечение выполнения обязанностей, предусмотренных ФЗ № 152-ФЗ "О персональных данных", определяется лицом, ответственным в ГБУЗ РК «Черноморская ЦРБ» за организацию обработки персональных данных, исходя из правомерности и разумной достаточности указанных мер.

Приложение № 1

к Правилам оценки вреда, который может быть причинен субъектам персональных данных в случае нарушения требований по обработке и обеспечению безопасности персональных данных в ГБУЗ РК «Черноморская ЦРБ»

**Оценка вреда,**

**который может быть причинен субъектам персональных данных, а также соотнесение возможного вреда и реализуемых ГБУЗ РК «Черноморская ЦРБ» мер**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| №  п/п | **Требования** [**Федерального закона "О персональных данных"**](http://docs.cntd.ru/document/901990046)**, которые могут быть нарушены** | **Возможные нарушение 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 |  |  |  |
| Целостность |  |
| Доступность |  |
| Конфиденциальность |  |
| 2 | Порядок и условия применения средств защиты информации; | Убытки и моральный вред |  |  | В соответствии с технической документацией на систему защиты ИСПД |
| Целостность |  |
| Доступность |  |
| Конфиденциальность |  |
| 3 | Эффективность принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных; | Убытки и моральный вред |  |  | 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 |  |  | 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 |  |  | Мониторинг средств защиты информации на наличие фактов доступа к ПД |
| Целостность |  |
| Доступность |  |
| Конфиденциальность |  |
| 7 | Мероприятия по восстановлению персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним; | Убытки и моральный вред |  |  | Применение резервного копирования |
| Целостность |  |
| Доступность |  |
| Конфиденциальность |  |
| 8 | Осуществление мероприятий по обеспечению целостности персональных данных | Убытки и моральный вред |  |  | Организация режима доступа к техническим и программным средствам |
| Целостность |  |
| Доступность |  |
| Конфиденциальность |  |