Утверждено
Приказом генерального директора от 31.01.2023 года
Общества с ограниченной ответственностью
Микрокредитная компания «М-КРЕДИТ»

ПРАВИЛА

оценки вреда, который может быть причинен 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 законодательства по защите персональных данных, в частности 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. Термины и определения

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 определённой 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. Описание 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.

4. Перечисленные неправомерные действия определяются как следующие нарушения безопасности информации:

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

4.2. Неправомерное уничтожение и блокирование персональных данных является нарушением доступности персональных данных.

4.3. Неправомерное изменение персональных данных является нарушением целостности персональных данных.

4.4. Нарушение права субъекта требовать от оператора уточнения его персональных данных, их блокирования или уничтожение является нарушением целостности информации.

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

4.6. 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.

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

4.8. 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.

5. Субъекту персональных данных может быть причинён вред в форме:

5.1. 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.

5.2. 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.

6. Методика оценки возможного вреда субъектам персональных данных

6.1. Оценка возможного вреда должна производиться коллегиально. В комиссии должно быть не менее трех человек.

6.2. В оценке возможного вреда исходить из учёта последствий допущенного нарушения принципов обработки персональных данных. Вводится четыре уровня возможного вреда:

6.2.1. нулевой - вред субъекту ПДн не причиняется;

6.2.2. низкий - последствия нарушения принципов обработки персональных данных включают только нарушение целостности персональных данных, либо только нарушение доступности персональных данных;

6.2.3. средний - 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;

6.2.4. высокий - во всех остальных случаях.

7. Каждому уровню возможного вреда сопоставляется числовая оценка Y1, а именно:

0 - при нулевом уровне вреда;

0,05 - при низком уровне вреда;

0,1 - при среднем уровне вреда;

0,2 - при высоком уровне вреда.

8. Каждым членом комиссии на основании собственного субъективного мнения выставляется одна из возможных оценок возможного вреда субъекту для каждой актуальной угрозы безопасности его ПДн из-за несанкционированного, в том числе случайного, доступа к его ПДн при их обработке в информационных системах.

9. Все коэффициенты оценок суммируются по каждой актуальной угрозе.

10. По значению суммарной оценки Y2 определяется возможный вред следующим образом:

если $Y2 > 0,9$, то вред субъектам ПДн признается высоким; если $0,5 < Y2 \leq 0,9$, то вред субъектам ПДн признается средним;

если $0,2 < Y2 \leq 0,5$, то вред субъектам ПДн признается низким; если $0 < Y2 \leq 0,5$, то вред субъектам ПДн признается нулевым.

11. Требования к мерам защиты

11.1. С использованием данных об уровне защищенности ИСПДн и категориях персональных данных, обрабатываемых в них, на основе «Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» формулируются и применяются конкретные организационные и технические меры защиты, которые могут быть использованы при эксплуатации ИСПДн.