|  |  |
| --- | --- |
|  | УТВЕРЖДАЮ  Генеральный директор [***указать наименование***]  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/\_\_\_\_\_\_\_\_\_\_\_\_\_/  «\_\_» \_\_\_\_\_\_\_\_\_\_\_ 2023 г. |

ПОЛОЖЕНИЕ [*указать наименование*]

о порядке информирования о компьютерных инцидентах

1. Настоящее Положение определяет процедуру информирования [***указать наименование***] (далее также Общество, оператор) Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) о фактах неправомерной или случайной передачи (предоставления, распространения, доступа) персональных данных, повлекшей нарушение прав субъектов персональных данных (далее — компьютерный инцидент), а также порядок реагирования на указанные компьютерные инциденты и принятия мер по ликвидации их последствий.

2. Общество информирует уполномоченный государственный орган — Роскомнадзор обо всех компьютерных инцидентах, повлекших неправомерную передачу (предоставление, распространение, доступ) персональных данных.

3. Информирование осуществляется путем направления информации в Роскомнадзор в соответствии с форматами представления информации о факте неправомерной или случайной передачи (предоставления, распространения, доступа) персональных данных, повлекшей нарушение прав субъектов персональных данных посредством заполнения соответствующей формы на сайте Роскомнадзора по адресу <https://pd.rkn.gov.ru/incidents/form/>.

4. Информация о произошедшем компьютерном инциденте направляется Обществом в течение двадцати четырех часов с момента инцидента. Указанная информация включает в себя сведения:

— об инциденте и его предполагаемых причинах, повлекших нарушение прав субъектов персональных данных;

— о возможном вреде, причиненном правам субъектов персональных данных;

— о принятых мерах по устранению последствий соответствующего инцидента;

— о лице, уполномоченном Обществом на взаимодействие с Роскомнадзором по вопросам, связанным с инцидентом.

5. Для подготовки к реагированию на компьютерные инциденты и принятию мер по ликвидации их последствий Обществом приняло следующие меры:

— назначило лицо, ответственное за организацию обработки персональных данных;

— утвердило локальные акты, определяющие политику Исполнителя в отношении обработки персональных данных, и обеспечило неограниченный доступ к таким локальным актам;

— обеспечило применение правовых, организационных и технических мер по обеспечению безопасности персональных данных в соответствии со статьей 19 закона «О персональных данных»;

— осуществляет внутренний контроль соответствия обработки персональных данных требованиям законодательства к защите персональных данных, политике Исполнителя в отношении обработки персональных данных, и локальным актам Исполнителя;

— ознакомило работников, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, а также документами, определяющими политику Исполнителя в отношении обработки персональных данных.

6. К локальным актам Общества, определяющим политику в отношении обработки персональных данных и порядок такой обработки персональных данных относятся:

— приказ о назначении лица, ответственного за организацию обработки персональных данных работников (п. 1 ч. 1 ст. 18.1 Закона о персональных данных);

— Положение об обработке и защите персональных данных работников;

— приказ об утверждении перечня лиц, имеющих доступ к персональным данным работников;

— письменные обязательства работников, имеющих доступ к персональным данным, о неразглашении (соблюдении конфиденциальности) персональных данных;

7. Для защиты персональных данных на бумажных носителях Обществом приняты следующие меры:

а) персональные данные на бумажных носителях хранятся в специальных помещениях;

б) материальные носители персональных данных, которые обрабатываются в разных целях, хранятся отдельно;

в) организована охрана и особый режим доступа в помещения хранения персональных данных, а также утвержден перечень лиц, имеющих доступ в данные помещения с учетом требований Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации;

8. Для защиты персональных данных в электронном виде Обществом приняты следующие меры:

а) определен тип угрозы безопасности персональных данных и уровень защищенности персональных данных, исходя из определенного типа угрозы;

б) организована охрана и особый режим доступа в помещения, в которых размещена информационная система, от неконтролируемого проникновения или неправомерного доступа;

в) утвержден перечень лиц, имеющих в силу трудовых обязанностей доступ к персональным данным в информационной системе;

г) приняты меры по обеспечению сохранности носителей персональных данных;

д) обеспечена защита информацию с помощью средств, прошедших процедуру оценки соответствия в случае, когда применение таких средств необходимо для нейтрализации актуальных угроз.

9. Общество не реже одного раза в год организует и проводит тренировки по отработке мероприятий по реагированию на компьютерные инциденты и принятию мер по ликвидации их последствий.

Организация и проведение тренировок возлагаются на лиц, ответственных за проведение мероприятий по реагированию на компьютерные инциденты и принятие мер по ликвидации последствий компьютерных атак.

10. Общество в ходе реагирования на компьютерные инциденты и принятия мер по ликвидации последствий компьютерных атак осуществляет:

— анализ компьютерных инцидентов (включая определение очередности реагирования на них), установление их связи с компьютерными атаками;

— проведение мероприятий по реагированию на компьютерные инциденты и принятию мер по ликвидации их последствий.

11. Перед принятием мер по ликвидации последствий компьютерных атак Общество определяет:

— должностных лиц, ответственных за проведение мероприятий по реагированию на компьютерные инциденты и принятие мер по ликвидации последствий компьютерных атак, и их задачи в рамках принимаемых мер;

— перечень средств, необходимых для принятия мер по ликвидации последствий компьютерных атак;

— очередность объектов информационной инфраструктуры (их структурных элементов), содержащих персональные данные, в отношении которых произошла неправомерная или случайная передача (предоставление, распространение, доступ), повлекшие нарушение прав субъектов персональных данных, в отношении которых будут приниматься меры по ликвидации последствий компьютерных атак;

— перечень мер по восстановлению указанных объектов информационной инфраструктуры.

12. В ходе ликвидации последствий компьютерных атак Обществом принимаются меры по восстановлению функционирования и проверке работоспособности объектов информационной инфраструктуры, содержащих персональные данные, в отношении которых произошла неправомерная или случайная передача (предоставление, распространение, доступ), повлекшие нарушение прав субъектов персональных данных.

13. Информация о результатах внутреннего расследования выявленного инцидента, а также сведения о лицах, действия которых стали причиной выявленного инцидента (при наличии) направляется Обществом в течение семидесяти двух часов с момента инцидента.

**Приложение к Положению** [***указать наименование***]

**о порядке информирования о компьютерных инцидентах**

**Лист ознакомления работников** [***указать наименование***] **с Положением** [***указать наименование***] **о порядке информирования о компьютерных инцидентах**

**от «\_\_\_» \_\_\_\_\_\_\_\_\_ 2022 г.**

Мы, нижеподписавшиеся, своей подписью подтверждаем, что ознакомлены с Положением [***указать наименование***] о порядке информирования о компьютерных инцидентах и обязуемся его соблюдать в полном объеме.

|  |  |  |  |
| --- | --- | --- | --- |
| № п/п | Ф.И.О. субъекта персональных данных | Дата  ознакомления | Подпись |
| 1 |  |  |  |
| 2 |  |  |  |
| 3 |  |  |  |
| 4 |  |  |  |
| 5 |  |  |  |
| 6 |  |  |  |
| 7 |  |  |  |
| 8 |  |  |  |
| 9 |  |  |  |
| 10 |  |  |  |
| 11 |  |  |  |
| 12 |  |  |  |
| 13 |  |  |  |
| 14 |  |  |  |
| 15 |  |  |  |
| 16 |  |  |  |
| 17 |  |  |  |
| 18 |  |  |  |
| 19 |  |  |  |
| 20 |  |  |  |
| 21 |  |  |  |
| 22 |  |  |  |
| 23 |  |  |  |
| 24 |  |  |  |
| 25 |  |  |  |
| 26 |  |  |  |
| 27 |  |  |  |
| 28 |  |  |  |
| 29 |  |  |  |
| 30 |  |  |  |
| 31 |  |  |  |
| 32 |  |  |  |