



## ИНФОРМАЦИОННОЕ ПРИМЕЧАНИЕ К ОБРАЗЦУ ДОКУМЕНТА

Настоящие Правила являются демонстрационным образцом внутреннего организационного документа. Федеральное законодательство не устанавливает обязательный самостоятельный журнал регистрации инцидентов информационной безопасности именно с таким наименованием. Такой журнал может использоваться оператором как способ внутренней регистрации событий и инцидентов, способных повлиять на безопасность персональных данных, контроля реагирования и документирования принятых мер. При инцидентах, повлекших неправомерную или случайную передачу, предоставление, распространение либо доступ к персональным данным, дополнительно применяются требования статьи 21 Федерального закона № 152-ФЗ и соответствующие процедуры взаимодействия с Роскомнадзором и, в применимых случаях, ГосСОПКА.

**УТВЕРЖДЕНЫ**

приказом [НАИМЕНОВАНИЕ ОРГАНИЗАЦИИ]

от «\_\_» \_\_\_\_\_ 20\_\_ г. № \_\_\_\_

## ПРАВИЛА

### формирования и ведения журнала регистрации инцидентов информационной безопасности

#### 1. Общие положения

1.1. Журнал ведётся в целях регистрации инцидентов информационной безопасности, затрагивающих или способных затронуть обработку и защиту персональных данных в ИСПДн.

1.2. Ведение журнала осуществляется [ОТВЕТСТВЕННЫМ ЛИЦОМ / ДОЛЖНОСТЬЮ], определённым локальными актами оператора.

1.3..

1.4..

#### 2. Регистрация инцидентов

2.1. При регистрации инцидента фиксируются дата и время выявления, общий характер события, затронутая область и статус реагирования в объёме, необходимом для внутреннего учёта.

2.2. Если инцидент связан с неправомерной или случайной передачей, предоставлением, распространением либо доступом к персональным данным, сведения о нём обрабатываются также в порядке, установленном для выполнения обязанностей оператора по Федеральному закону № 152-ФЗ.

2.3..

2.4..

2.5..

#### 3. Контроль и закрытие инцидента

3.1. Закрытие записи об инциденте производится после фиксации результатов реагирования и принятого решения уполномоченным лицом.

3.2..

3.3..

## ДЕМОНСТРАЦИОННАЯ ВЕРСИЯ

В публичную версию намеренно не включены конкретные ИСПДн, IP-адреса, узлы, учетные записи, уязвимости, технические индикаторы компрометации, детальные сценарии реагирования, маршруты эскалации, результаты расследований, сведения об уведомлении регуляторов и полный состав граф журнала. Ниже приведён только условный фрагмент формы.

### Пример фрагмента журнала

| № | Дата / время   | Тип события | Область   | Ответственный | Статус   |
|---|----------------|-------------|-----------|---------------|----------|
| 1 | [ДАТА / ВРЕМЯ] | [ТИП]       | [ОБЛАСТЬ] | [ДОЛЖНОСТЬ]   | [СТАТУС] |
| 2 |                |             |           |               |          |
| 3 |                |             |           |               |          |
| 4 |                |             |           |               |          |

### Справочная нормативная основа

1. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных», статьи 19 и 21.

2. Приказ Роскомнадзора от 14.11.2022 № 187 - в части взаимодействия по инцидентам в области персональных данных.

3. Приказ ФСБ России от 13.02.2023 № 77 - в применимых случаях компьютерных инцидентов, повлекших неправомерную передачу, предоставление, распространение или доступ к ПДн.



Посетите **Telegram**-канал **Антагора** и подпишитесь, чтобы следить за новостями, изменениями законодательства и практическими обзорами по ПДн, ИБ, КИИ, АТЗ, БПЛА, комплаенсу и защите бизнеса.

Читайте нас в Telegram: [@antagora](https://t.me/antagora)

### Нужна адаптация документа под вашу организацию?

Группа компаний **АНТАГОРА**

Телефон: **8 (800) 333-8-222**

Сайт: [antagora.ru](https://antagora.ru) / [antagora.pf](https://antagora.pf)

Электронная почта: [info@antagora.ru](mailto:info@antagora.ru)

Телеграм-канал: [@antagora](https://t.me/antagora)

Перед применением образец необходимо проверить и адаптировать под вашу деятельность, реальные процессы, используемые системы, состав информации, сайт, каналы связи, договоры, локальные документы, обязанности работников и требования законодательства.

#### Мы можем помочь:

- оценить, подходит ли образец именно вам;
- адаптировать текст под вашу организацию;
- подготовить полный или минимально необходимый комплект документов;
- проверить связку документов между собой;
- найти пробелы и противоречия;
- подготовить документы по персональным данным (ПДн), информационной безопасности (ИБ), критической информационной инфраструктуре (КИИ), по АТЗ и противодействию БПЛА, противодействию коррупции, комплаенсу и защите бизнеса.

Если после скачивания шаблона стало понятно, что просто заменить название организации недостаточно, обратитесь к нам. Мы разберем вашу ситуацию и предложим нормальный состав работ.