



ИНФОРМАЦИОННОЕ ПРИМЕЧАНИЕ К ОБРАЗЦУ ДОКУМЕНТА

Настоящий документ является демонстрационным образцом Положения о комиссии по определению уровня защищённости персональных данных. Публичная версия сокращена и не содержит части рабочих материалов, технических характеристик информационных систем, моделей угроз, сведений о применяемых средствах защиты и иных данных, которые определяются применительно к конкретному оператору.

Документ не является готовым локальным нормативным актом для непосредственного применения без юридической и организационно-технической адаптации. При доработке учитываются фактические информационные системы персональных данных, категории и объём обрабатываемых данных, категории субъектов, актуальные угрозы безопасности, результаты оценки возможного вреда и применимые нормативные требования.

В доработке документа должны участвовать лицо, ответственное за организацию обработки персональных данных, специалисты по информационной безопасности и информационным технологиям, юридическая служба, владельцы соответствующих информационных систем и при необходимости иные профильные специалисты.

[НАИМЕНОВАНИЕ ОРГАНИЗАЦИИ]

УТВЕРЖДАЮ

[Должность руководителя]

_____ / [Ф.И.О.]

«__» _____ 20__ г.

М.П. (при наличии)

ПОЛОЖЕНИЕ О КОМИССИИ ПО ОПРЕДЕЛЕНИЮ УРОВНЯ ЗАЩИЩЁННОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ (демонстрационный образец)

1. Общие положения

1.1. Настоящее Положение определяет статус, задачи, состав, полномочия и порядок работы комиссии по определению уровня защищённости персональных данных при их обработке в информационных системах персональных данных [НАИМЕНОВАНИЕ ОРГАНИЗАЦИИ] (далее соответственно - Комиссия, Оператор, ИСПДн).

1.2. Комиссия является внутренним коллегиальным органом Оператора, создаваемым распорядительным документом руководителя. Создание именно комиссии для определения уровня защищённости персональных данных не установлено Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» или



постановлением Правительства РФ от 01.11.2012 № 1119 как обязательная организационная форма. Оператор вправе использовать комиссионный порядок как внутренний способ подготовки и документирования решения об уровне защищённости ИСПДн.

1.3. Уровень защищённости персональных данных определяется не произвольно и не решением Комиссии по усмотрению, а по условиям, установленным пунктами 8-12 Требований, утверждённых постановлением Правительства РФ от 01.11.2012 № 1119. Комиссия устанавливает фактические исходные данные, сопоставляет их с указанными нормативными критериями и оформляет обоснованный результат.

1.4. Настоящее Положение применяется к ИСПДн Оператора, в которых осуществляется автоматизированная обработка персональных данных. Для обработки персональных данных без использования средств автоматизации применяются требования постановления Правительства РФ от 15.09.2008 № 687 и соответствующие локальные акты Оператора; уровень защищённости по постановлению № 1119 для такой обработки не определяется.

1.5. Настоящее Положение не заменяет документы, определяющие актуальные угрозы безопасности, оценку возможного вреда субъектам персональных данных, состав и архитектуру ИСПДн, перечень допущенных лиц, а также документы, определяющие реализуемые организационные и технические меры защиты.

2. Нормативная основа

Нормативный правовой акт	Значение для настоящего Положения
Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»	Статья 18.1 предусматривает оценку вреда и внутренний контроль, статья 19 устанавливает обязанность принимать правовые, организационные и технические меры и определять угрозы безопасности персональных данных при обработке в ИСПДн.
Постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»	Устанавливает типы актуальных угроз, четыре уровня защищённости персональных данных и условия, при которых требуется каждый уровень. Пункты 7-12 являются непосредственной нормативной основой определения уровня защищённости.
Приказ Роскомнадзора от 27.10.2022 № 178 «Об утверждении Требований к оценке вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона «О персональных данных»»	Определяет порядок оценки вреда и допускает её проведение ответственным за организацию обработки персональных данных либо комиссией, образуемой оператором. Результат оценки оформляется отдельным актом оценки вреда.
Постановление Правительства РФ от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой	Применяется к неавтоматизированной обработке персональных данных и используется для разграничения режимов обработки; уровень защищённости по постановлению № 1119



Нормативный правовой акт	Значение для настоящего Положения
без использования средств автоматизации»	относится к ИСПДн.

3. Задачи Комиссии

3.1. Организация сбора и проверки исходных данных, необходимых для определения уровня защищённости персональных данных в каждой ИСПДн.

3.2. Установление категорий персональных данных, обрабатываемых в ИСПДн: специальных категорий, биометрических персональных данных, персональных данных, полученных из общедоступных источников в предусмотренных законом случаях, либо иных категорий персональных данных.

3.3. Определение состава субъектов персональных данных с разграничением работников Оператора и субъектов, не являющихся его работниками, а также определение количества субъектов в объёме, имеющем значение для применения критериев постановления № 1119.

3.4. Рассмотрение материалов об актуальных угрозах безопасности персональных данных и установление типа угроз, применимого к соответствующей ИСПДн, на основании подготовленных и утверждённых в установленном у Оператора порядке материалов.

3.5. Сопоставление установленных исходных данных с пунктами 9-12 постановления Правительства РФ № 1119 и подготовка вывода о необходимом уровне защищённости персональных данных.

3.6. Документирование решения, указание конкретного пункта и подпункта постановления № 1119, на основании которого определён соответствующий уровень защищённости.

3.7. Инициирование повторного определения уровня защищённости при изменении обстоятельств, способных повлиять на нормативную квалификацию ИСПДн.

4. Состав Комиссии и полномочия её членов

4.1. Персональный состав Комиссии утверждается приказом руководителя Оператора. В состав Комиссии рекомендуется включать председателя, секретаря, лицо, ответственное за организацию обработки персональных данных, представителей подразделений информационной безопасности и информационных технологий, владельца или функционального заказчика ИСПДн, а при необходимости представителя юридической службы.

4.2. Председатель Комиссии организует работу, определяет дату заседания, утверждает повестку, обеспечивает получение необходимых материалов и подписывает итоговые документы в пределах установленной у Оператора процедуры.

4.3. Секретарь Комиссии формирует материалы заседания, ведёт протокол, фиксирует результаты голосования, обеспечивает оформление и хранение документов Комиссии.

4.4. Члены Комиссии обязаны изучить представленные сведения в пределах своей компетенции, заявить о недостаточности или противоречивости исходных данных, участвовать в обсуждении и подписании документов.

4.5. Комиссия вправе запрашивать у структурных подразделений сведения об ИСПДн, обрабатываемых категориях персональных данных, количестве субъектов,



используемом программном обеспечении, архитектуре, местах размещения, способах доступа и иных обстоятельствах, необходимых для применения постановления № 1119.

4.6. Комиссия не вправе изменять критерии определения уровней защищённости, установленные постановлением № 1119, или снижать уровень защищённости исходя из экономической целесообразности, стоимости средств защиты либо иных обстоятельств, не предусмотренных нормативными критериями.

5. Исходные данные для определения уровня защищённости

5.1. До заседания Комиссии по каждой ИСПДн формируется комплект исходных сведений. Он должен позволять однозначно применить критерии пунктов 9-12 постановления № 1119.

Исходный параметр	Что должно быть установлено
Категория персональных данных	Какие категории персональных данных фактически обрабатываются в ИСПДн и имеют значение для классификации по постановлению № 1119.
Категория субъектов	Обрабатываются ли данные работников Оператора либо субъектов, не являющихся его работниками.
Количество субъектов	Количество субъектов, персональные данные которых обрабатываются в ИСПДн, с учётом порогового значения 100 000 субъектов, используемого постановлением № 1119.
Тип актуальных угроз	Тип угроз 1, 2 или 3 в понимании пункта 6 постановления № 1119, определённый на основании материалов об актуальных угрозах.
Оценка возможного вреда	Результаты оценки вреда, проведённой во исполнение пункта 5 части 1 статьи 18.1 Закона № 152-ФЗ и требований приказа Роскомнадзора № 178, если такая оценка относится к рассматриваемому процессу обработки.
Границы ИСПДн	Состав информационной системы, используемые информационные технологии и иные параметры, позволяющие исключить смешение нескольких различных по условиям обработки систем.

ДЕМОНСТРАЦИОННАЯ ВЕРСИЯ

Полная редакция документа должна быть дополнена рабочей формой сбора исходных данных по каждой ИСПДн, перечнем подтверждающих документов и внутренней матрицей сопоставления фактических параметров ИСПДн с подпунктами пунктов 9-12 постановления Правительства РФ № 1119. В публичный образец сведения о конкретной архитектуре, угрозах, средствах защиты и иных параметрах безопасности не включаются.



6. Порядок определения уровня защищённости

6.1. Определение уровня защищённости проводится отдельно в отношении каждой ИСПДн либо группы ИСПДн, только если их объединение обосновано одинаковыми условиями обработки и не приводит к искажению нормативной квалификации.

6.2. Комиссия проверяет полноту и непротиворечивость исходных сведений. При недостаточности материалов вопрос переносится до получения необходимых данных. Определение уровня защищённости на основании предположений не допускается.

6.3. Комиссия последовательно устанавливает категорию обрабатываемых персональных данных, категорию субъектов, количество субъектов и тип актуальных угроз.

6.4. Установленные параметры сопоставляются с условиями пунктов 9, 10, 11 и 12 постановления Правительства РФ № 1119. Итоговый уровень защищённости определяется тем нормативным условием, которое соответствует фактическим параметрам ИСПДн.

6.5. В итоговом документе указывается не только номер уровня защищённости, но и конкретная нормативная связка: установленный тип угроз, категория персональных данных, категория и количество субъектов, а также пункт и подпункт постановления № 1119.

6.6. Если в ИСПДн одновременно присутствуют различные категории данных или условия обработки, Комиссия должна учитывать наиболее требовательное применимое нормативное условие, если разделение обработки на самостоятельные ИСПДн не подтверждено организационно и технически.

6.7. После определения уровня защищённости материалы передаются ответственным подразделениям для определения и реализации организационных и технических мер в соответствии со статьёй 19 Закона № 152-ФЗ, постановлением № 1119 и иными применимыми нормативными правовыми актами.

7. Оформление результатов работы Комиссии

7.1. Заседание Комиссии оформляется протоколом. На основании протокола может составляться отдельный акт определения уровня защищённости либо иной внутренний документ, установленный локальными актами Оператора.

7.2. Итоговый документ должен содержать как минимум: наименование ИСПДн; дату рассмотрения; состав Комиссии; перечень изученных исходных материалов; установленные параметры, влияющие на уровень защищённости; определённый уровень защищённости; точную ссылку на применённый пункт и подпункт постановления № 1119; сведения о наличии особых мнений членов Комиссии.

7.3. Если Комиссии одновременно поручено проведение оценки вреда субъектам персональных данных, результат такой оценки оформляется отдельным актом оценки вреда с соблюдением пунктов 3-6 Требований, утверждённых приказом Роскомнадзора от 27.10.2022 № 178. Протокол определения уровня защищённости не заменяет акт оценки вреда.

7.4. Материалы Комиссии относятся к внутренним документам Оператора. Если они содержат сведения о конфигурации информационных систем, актуальных угрозах, средствах защиты, учётных записях, сетевой инфраструктуре или иные сведения ограниченного доступа, режим доступа к ним определяется соответствующими локальными актами и законодательством Российской Федерации.



8. Основания для повторного рассмотрения

8.1. Повторное определение уровня защищённости проводится при изменении категории обрабатываемых персональных данных, состава субъектов или количества субъектов, если такие изменения могут повлиять на применение критериев постановления № 1119.

8.2. Повторное рассмотрение проводится при изменении актуальных угроз безопасности персональных данных либо условий, на основании которых был определён их тип.

8.3. Основанием также являются существенные изменения архитектуры ИСПДн, состава программного или технического обеспечения, способов обработки, интеграций и границ системы, если эти изменения влияют на исходные параметры определения уровня защищённости.

8.4. Повторное рассмотрение проводится при выявлении ошибки или неполноты в ранее использованных исходных данных, а также при изменении законодательства, непосредственно влияющего на критерии определения уровня защищённости.

9. Порядок заседаний и принятия решений

9.1. Заседание Комиссии правомочно при участии не менее половины утверждённого состава, если приказом о создании Комиссии не установлен более высокий кворум.

9.2. Решение принимается большинством голосов присутствующих членов. При равенстве голосов решающим является голос председателя, если иное не установлено внутренним распорядительным документом.

9.3. Особое мнение члена Комиссии излагается письменно и прилагается к протоколу. Наличие особого мнения не освобождает Оператора от обязанности применять критерии постановления № 1119 в соответствии с фактическими обстоятельствами.

9.4. При выявлении правовой или технической неопределённости Комиссия вправе инициировать получение дополнительного заключения профильного специалиста. Такое заключение является вспомогательным материалом и не подменяет требования нормативных правовых актов.

10. Хранение, актуализация и контроль

10.1. Оригиналы протоколов, актов и материалов Комиссии хранятся в порядке, установленном номенклатурой дел и локальными актами Оператора, с учётом содержащихся в документах сведений ограниченного доступа.

10.2. Ответственный за организацию обработки персональных данных и подразделение, ответственное за информационную безопасность, в пределах закреплённых полномочий контролируют актуальность документов об уровнях защищённости ИСПДн.

10.3. Настоящее Положение подлежит пересмотру при изменении законодательства, структуры и процессов Оператора либо иных обстоятельств, влияющих на установленный порядок определения уровня защищённости.

11. Приложения полной редакции

11.1. К полной редакции Положения рекомендуется предусмотреть следующие рабочие приложения:

- форма приказа о создании Комиссии и утверждении её состава;
- форма карточки исходных данных ИСПДн;
- матрица определения уровня защищённости по пунктам 9-12 постановления № 1119;



- форма протокола заседания Комиссии;
- форма акта определения уровня защищённости персональных данных;
- перечень документов, подтверждающих категорию данных, категорию и количество субъектов и тип актуальных угроз;
- форма листа пересмотра уровня защищённости.

ДЕМОНСТРАЦИОННАЯ ВЕРСИЯ

Полная рабочая матрица определения уровня защищённости, формы технических приложений, сведения о конкретных ИСПДн, актуальных угрозах и реализуемых средствах защиты относятся к полной редакции документа и в публичный демонстрационный образец не включаются.

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 / antagora.pf

Электронная почта: info@antagora.ru

Telegram-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;

Для заказа комплекта документов, консультации и прочим услугам звоните **8 (800) 333-8-222** или пишите info@antagora.ru ещё больше информации и документов на сайте antagora.pf

Образец документа - Страница 7 из 8 - требует проверки и адаптации под организацию.



- 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.