



ИНФОРМАЦИОННОЕ ПРИМЕЧАНИЕ К ОБРАЗЦУ ДОКУМЕНТА

Настоящий документ является демонстрационным образцом внутреннего организационного документа, регулирующего доступ в помещения, в которых размещены информационные системы персональных данных (ИСПДн), их элементы и иные средства обработки персональных данных. Публичная версия не содержит фактических адресов, номеров помещений, схем размещения оборудования, перечней допущенных лиц, сведений о средствах охраны и иных данных, раскрытие которых может снизить уровень защищенности.

Отдельный документ с данным наименованием прямо не установлен Федеральным законом № 152-ФЗ как обязательный для каждого оператора. Вместе с тем пункт 13 постановления Правительства Российской Федерации от 01.11.2012 № 1119 требует организации режима обеспечения безопасности помещений, в которых размещена информационная система, исключающего неконтролируемое проникновение или пребывание лиц, не имеющих права доступа.

Рабочая редакция должна быть адаптирована с учетом фактических помещений, состава ИСПДн, уровня защищенности, режима объекта, технических средств контроля доступа и локальной системы разграничения полномочий. В доработке документа должны участвовать ответственное за организацию обработки персональных данных лицо, подразделение информационной безопасности, ИТ-подразделение, служба безопасности и, при необходимости, юридическая служба.

[НАИМЕНОВАНИЕ ОРГАНИЗАЦИИ]

УТВЕРЖДАЮ

[должность

руководителя]

[Ф.И.О.]

«__» _____ 20__ г.

ПОРЯДОК ДОСТУПА В ПОМЕЩЕНИЯ, В КОТОРЫХ РАЗМЕЩЕНЫ ИСПДн

1. Общие положения

1.1. Настоящий Порядок устанавливает правила допуска работников, посетителей, подрядчиков и иных лиц в помещения [наименование организации], в которых размещены ИСПДн, серверное и сетевое оборудование, рабочие станции, носители персональных данных либо иные элементы инфраструктуры, обеспечивающие обработку персональных данных.

1.2. Цель Порядка состоит в предотвращении неконтролируемого проникновения и пребывания в указанных помещениях лиц, не имеющих права доступа, а также в обеспечении сохранности технических средств и носителей персональных данных.

1.3. Правовую основу составляют Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных», в том числе статья 19, и постановление Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

1.4. В соответствии с подпунктом «а» пункта 13 Требований, утвержденных постановлением Правительства Российской Федерации № 1119, оператор обязан организовать режим обеспечения безопасности помещений, в которых размещена информационная система, препятствующий возможности неконтролируемого проникновения или пребывания лиц, не имеющих права доступа.



1.5. Настоящий Порядок применяется совместно с перечнем лиц, которым доступ к персональным данным необходим для выполнения трудовых обязанностей, правилами пропускного и внутриобъектового режима, положением об обработке и защите персональных данных и иными локальными актами оператора.

2. Категории помещений

2.1. Для целей настоящего Порядка помещения подразделяются на помещения постоянного размещения элементов ИСПДн, помещения временного размещения оборудования или носителей и иные помещения, доступ в которые может повлиять на безопасность персональных данных.

2.2. Перечень таких помещений утверждается или ведется уполномоченным подразделением оператора. В публичную версию настоящего Порядка конкретные адреса, номера и назначение помещений не включаются.

2.3. Для каждого помещения определяются режим доступа, круг допущенных лиц и, при необходимости, дополнительные меры физической защиты.

3. Основания предоставления доступа

3.1. Постоянный доступ предоставляется работникам, которым нахождение в соответствующем помещении необходимо для исполнения трудовых или служебных обязанностей.

3.2. Основанием для предоставления постоянного доступа является утвержденное полномочие, должностная необходимость и включение лица в установленный оператором перечень либо иной документ, подтверждающий право доступа.

3.3. Временный доступ может предоставляться работникам других подразделений, представителям подрядчиков, обслуживающих организаций и иным лицам для выполнения конкретных работ при наличии законного и организационно подтвержденного основания.

3.4. Право доступа подлежит пересмотру при переводе работника, изменении его функций, прекращении договора, увольнении либо иных обстоятельствах, устраняющих необходимость нахождения в помещении.

4. Порядок постоянного доступа

4.1. Допуск осуществляется только в помещения, соответствующие объему полномочий работника.

4.2. Работник обязан использовать предоставленные средства доступа только лично и не передавать их другим лицам.

4.3. При входе и выходе должны соблюдаться установленные оператором правила идентификации, регистрации и контроля доступа, если соответствующие средства применяются.

4.4. Запрещается оставлять двери, контролируемые техническими средствами доступа, в состоянии, позволяющем неконтролируемый проход.

4.5. При выявлении неисправности замка, системы контроля доступа, сигнализации либо иных средств физической защиты работник обязан сообщить уполномоченному лицу.



5. Временный доступ и допуск посетителей

5.1. Временный доступ предоставляется на период и в объеме, необходимых для выполнения конкретной задачи.

5.2. Лица, не имеющие постоянного права доступа, допускаются в помещение, как правило, в сопровождении уполномоченного работника, если иное не установлено внутренними правилами организации.

5.3. До допуска подрядчика или обслуживающего персонала ответственное лицо должно убедиться в наличии основания для проведения работ и определить условия, исключающие неправомерный доступ к персональным данным и средствам их обработки.

5.4. Если в ходе работ существует риск доступа к персональным данным, принимаются дополнительные меры: блокирование сеансов, отключение или изоляция оборудования, удаление доступных носителей, сопровождение работ либо иные меры, соответствующие фактической ситуации.

5.5. Факт временного доступа фиксируется в порядке, установленном оператором, если такая регистрация предусмотрена действующим пропускным или внутриобъектовым режимом.

6. Проведение технических, ремонтных и хозяйственных работ

6.1. Ремонт, техническое обслуживание, уборка, монтаж и иные работы в помещениях с ИСПДн проводятся таким образом, чтобы исключить неконтролируемый доступ к оборудованию, носителям и персональным данным.

6.2. При необходимости выполнения работ лицами, не допущенными к персональным данным, организация обеспечивает наблюдение либо иные компенсирующие меры.

6.3. Передача оборудования, содержащего персональные данные, на внешнее обслуживание допускается только после выполнения предусмотренных оператором мер, исключающих неправомерный доступ к содержащейся информации.

7. Действия при чрезвычайных и аварийных ситуациях

7.1. При пожаре, аварии, угрозе жизни и здоровью людей либо иной чрезвычайной ситуации ограничения доступа применяются с учетом необходимости обеспечения безопасности людей и выполнения законных требований экстренных служб.

7.2. После устранения непосредственной угрозы ответственное лицо организует проверку сохранности оборудования, носителей, состояния средств физической защиты и наличия признаков несанкционированного доступа.

7.3. Выявленные нарушения или инциденты документируются и рассматриваются в соответствии с внутренним порядком реагирования на инциденты безопасности персональных данных.

8. Учет и контроль прав доступа

8.1. Оператор обеспечивает актуальность сведений о лицах, имеющих право доступа в защищаемые помещения.



8.2. Выдача и возврат материальных и электронных средств доступа учитываются в объеме, установленном внутренними правилами организации.

8.3. При утрате ключа, карты, пропуска, идентификатора либо подозрении на их компрометацию работник обязан незамедлительно уведомить уполномоченное лицо.

8.4. Уполномоченное лицо организует блокирование или замену утраченного средства доступа и проверяет необходимость дополнительных мер.

8.5. Контроль соблюдения настоящего Порядка осуществляется в рамках внутреннего контроля и мероприятий по обеспечению безопасности персональных данных.

ДЕМОНСТРАЦИОННАЯ ВЕРСИЯ

В публичный образец не включены перечень конкретных помещений, адреса и номера комнат, схемы размещения ИСПДн, список допущенных лиц, образцы пропусков, номера ключей и идентификаторов, сведения о системах контроля и управления доступом, сигнализации, охране и графиках контроля.

В полной редакции эти сведения оформляются отдельными приложениями или связанными учетными документами с учетом требований информационной безопасности и режима ограниченного доступа.

9. Ответственность

9.1. Работники обязаны соблюдать настоящий Порядок в пределах предоставленных им полномочий.

9.2. Нарушение установленного режима доступа рассматривается в соответствии с законодательством Российской Федерации, трудовыми обязанностями и локальными актами оператора.

9.3. Ответственность определяется с учетом характера нарушения, вины лица и наступивших последствий.

10. Заключительные положения

10.1. Настоящий Порядок вступает в силу с даты его утверждения.

10.2. Порядок подлежит пересмотру при изменении состава ИСПДн, мест их размещения, пропускного режима, применяемых средств физической защиты либо нормативных требований.

10.3. Работники, на которых распространяется настоящий Порядок, знакомятся с ним в объеме, необходимом для исполнения своих обязанностей.

Справочная нормативная основа

- Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»: статья 19.
- Постановление Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»: пункт 13, подпункты «а» и «в»; пункты 14-16 в части дополнительных требований для соответствующих уровней защищенности.
- Локальные акты оператора, регулирующие пропускной и внутриобъектовый режим, разграничение доступа и защиту персональных данных.



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;
- 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.