



**ПРАВИТЕЛЬСТВО
МОСКОВСКОЙ ОБЛАСТИ
ПОСТАНОВЛЕНИЕ**

13.02.2026 № 127-ПП

г. Красногорск

Об утверждении Порядка обработки информации ограниченного доступа в центральных исполнительных органах Московской области, государственных органах Московской области и государственных учреждениях Московской области и признании утратившим силу постановления Правительства Московской области от 29.07.2020 № 469/21 «Об утверждении Порядка обработки информации ограниченного доступа в исполнительных органах государственной власти Московской области, государственных органах Московской области и государственных учреждениях Московской области и признании утратившими силу некоторых постановлений Правительства Московской области»

В соответствии с Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Законом Московской области № 80/2009-ОЗ «О государственных информационных системах Московской области и обеспечении доступа к содержащейся в них информации», а также в целях организации системы защиты информации Правительство Московской области постановляет:

1. Утвердить прилагаемый Порядок обработки информации ограниченного доступа в центральных исполнительных органах Московской области, государственных органах Московской области и государственных учреждениях Московской области.

2. Признать утратившим силу постановление Правительства Московской области от 29.07.2020 № 469/21 «Об утверждении Порядка обработки информации ограниченного доступа в исполнительных органах государственной власти Московской области, государственных органах Московской области

070072 *

и государственных учреждениях Московской области и признании утратившими силу некоторых постановлений Правительства Московской области».

3. Министерству информации и молодежной политики Московской области обеспечить официальное опубликование (размещение) настоящего постановления на сайте в Интернет-портале Правительства Московской области (www.mosreg.ru) и на «Официальном интернет-портале правовой информации» (www.pravo.gov.ru).

4. Настоящее постановление вступает в силу на следующий день после дня его официального опубликования.

5. Контроль за выполнением настоящего постановления возложить на Вице-губернатора Московской области Каратаева Р.А.

Первый Вице-губернатор
Московской области – Председатель
Правительства Московской области



И.Н. Габдрахманов

УТВЕРЖДЕН
постановлением Правительства
Московской области
от 13.02.2026 № 127-ПП

ПОРЯДОК
обработки информации ограниченного доступа
в центральных исполнительных органах Московской области, государственных
органах Московской области и государственных учреждениях Московской области

I. Общие положения

1. Настоящий Порядок определяет общий порядок обработки информации ограниченного доступа в центральных исполнительных органах Московской области, государственных органах Московской области и государственных учреждениях Московской области (далее – государственные органы).

В соответствии с Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» информацией ограниченного доступа является информация, доступ к которой ограничен федеральными законами.

Настоящий Порядок не распространяется на порядок обработки информации, содержащей сведения, составляющие государственную тайну.

2. Ограничение доступа к информации устанавливается в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства.

3. Руководители государственных органов обеспечивают организацию работы с информацией ограниченного доступа в соответствии с настоящим Порядком.

4. Термины, применяемые в настоящем Порядке, применяются в значениях, в которых они определены Федеральным законом от 22.10.2004 № 125-ФЗ «Об архивном деле в Российской Федерации», Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» и Законом Московской области № 80/2009-ОЗ «О государственных информационных системах Московской области и обеспечении доступа к содержащейся в них информации».

5. Информационные ресурсы, содержащие информацию ограниченного доступа, сформированные в процессе деятельности государственных органов за счет средств

бюджета Московской области, а также приобретенные в государственную собственность Московской области установленными законодательством Российской Федерации способами, являются государственной собственностью Московской области и не могут быть использованы иначе как с разрешения собственника и в случаях, установленных законодательством Российской Федерации.

6. Обязательность соблюдения конфиденциальности информации ограниченного доступа, а также ответственность за её разглашение, устанавливается федеральными законами.

7. Для отнесения информации к информации ограниченного доступа используется Перечень сведений, отнесенных федеральными законами и актами Президента Российской Федерации к информации ограниченного доступа, согласно приложению к настоящему Порядку (далее – Перечень сведений), составленный на основании законодательства Российской Федерации.

Государственные органы утверждают собственные Перечни сведений, сформированные с учетом федеральных законов и настоящего Порядка, исходя из сфер деятельности.

8. Доступ не может быть ограничен к:

нормативным правовым актам, затрагивающим права, свободы и обязанности человека и гражданина, а также устанавливающим правовое положение организаций и полномочия государственных органов¹, органов местного самоуправления;

информации о состоянии окружающей среды (экологической информации);

информации о деятельности государственных органов и органов местного самоуправления, а также об использовании бюджетных средств (за исключением сведений, составляющих государственную или служебную тайну);

информации, накапливаемой в открытых фондах библиотек, музеев, а также в государственных, муниципальных и иных информационных системах, созданных или предназначенных для обеспечения граждан (физических лиц) и организаций такой информацией;

информации, содержащейся в архивных документах архивных фондов (за исключением сведений и документов, доступ к которым ограничен законодательством Российской Федерации);

иной информации, недопустимость ограничения доступа к которой установлена федеральными законами.

9. Защита информации ограниченного доступа производится на основании федеральных законов, актов Президента Российской Федерации, стандартов, правовых актов и методических документов по защите информации федеральных

¹ В целях настоящего пункта понятие «государственный орган» следует понимать в значении, указанном в пункте 2 статьи 1 Федерального закона от 09.02.2009 № 8-ФЗ «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления».

органов исполнительной власти, уполномоченных в области обеспечения безопасности, противодействия техническим разведкам и технической защиты информации, контроля и надзора за соответствием обработки персональных данных требованиям законодательства Российской Федерации в области персональных данных, правовых актов Правительства Московской области, уполномоченных государственных органов Московской области, рекомендаций Московской областной комиссии по информационной безопасности, а также настоящего Порядка.

II. Обработка информации ограниченного доступа в информационных системах государственных органов

10. Защита информации ограниченного доступа является составной частью работ по созданию, развитию, вводу в эксплуатацию, эксплуатации и выводу из эксплуатации информационных систем государственных органов, располагающих информацией ограниченного доступа, и должна осуществляться в установленном законодательством Российской Федерации порядке.

11. При создании (развитии) информационных систем (до ввода в эксплуатацию) государственные органы определяют перечень требований по защите информации, содержащейся в информационной системе. Требования по защите информации должны устанавливаться при создании (развитии) всех государственных информационных систем независимо от наличия в них информации ограниченного доступа. Указанные требования отражаются в разделе «Требования по защите информации» технических требований (технического задания) на создание (развитие) информационной системы с привлечением структурных подразделений (штатных специалистов), ответственных за обеспечение защиты информации.

С этой целью государственные органы реализуют следующие мероприятия:

определение информации, подлежащей защите от неправомерных доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также иных неправомерных действий в отношении такой информации;

анализ нормативных правовых актов, методических документов и национальных стандартов, которым должна соответствовать информационная система (в части защиты информации);

классификация информационной системы в соответствии с требованиями по защите информации;

определение угроз безопасности информации, реализация которых может привести к нарушению безопасности информации в информационной системе, и разработка на их основе модели угроз безопасности информации;

утверждение должностным лицом государственного органа технического задания на создание (развитие) информационной системы (очереди системы) и модели угроз безопасности информации;

разработка и утверждение организационно-распорядительных документов, регулирующих вопросы обеспечения защиты информации в том числе, локальных актов, определяющих ответственность за защиту информации и функциональные обязанности, права и ответственность пользователей и администраторов информационной системы;

принятие организационных и технических мер защиты информации, направленных на блокирование (нейтрализацию) угроз безопасности информации в информационной системе, в рамках системы (подсистемы) защиты информации. Меры защиты информации ограниченного доступа реализуются, в том числе, посредством применения в информационной системе средств защиты информации, прошедших процедуру оценки соответствия, в случаях, когда применение таких средств необходимо для нейтрализации актуальных угроз безопасности информации. В установленных законодательством Российской Федерации случаях оценка соответствия должна быть проведена в форме сертификации на соответствие требованиям, установленным уполномоченными федеральными органами исполнительной власти. По решению руководителей государственных органов могут быть приняты дополнительные меры по защите информации, обрабатываемой в информационной системе;

аттестация информационной системы по требованиям защиты информации (или оценка эффективности реализованных в рамках системы защиты персональных данных мер по обеспечению безопасности персональных данных), в результате которой подтверждается соответствие защиты информации (персональных данных), содержащейся в информационной системе (информационной системе персональных данных), требованиям, предусмотренным законодательством Российской Федерации в сфере защиты информации и персональных данных.

12. При эксплуатации информационных систем государственные органы осуществляют эксплуатацию системы в соответствии с рабочей документацией (в части защиты информации), а также обеспечивают доступ к информации, содержащейся в системе, в соответствии с установленными правами и (или) правилами доступа к информации.

13. При выводе из эксплуатации информационных систем государственные органы обязаны определить порядок, сроки, режим хранения и дальнейшего использования информационных ресурсов, включая порядок обеспечения доступа к информационным ресурсам и обеспечения защиты информации, содержащейся в системе.

В состав работ по выводу системы из эксплуатации, в том числе, должны быть включены работы по обеспечению хранения и дальнейшего использования информационных ресурсов системы, а также по защите информации в соответствии с эксплуатационной документацией на информационную систему и организационно-распорядительными документами по защите информации. Должны быть проведены мероприятия по архивированию информации, содержащейся в системе, уничтожению (стиранию) данных и остаточной информации с машинных носителей информации и (или) уничтожению машинных носителей информации.

III. Обязанности должностных лиц по защите информации ограниченного доступа и ответственность за ее разглашение

14. Ответственность за организацию работы по защите информации ограниченного доступа возлагается на руководителя государственного органа. Обязанности (функции) и полномочия руководителя должны включать организацию деятельности по защите информации, управлению защитой информации, а также по организации контроля за данной деятельностью.

15. Руководитель государственного органа подписывает (утверждает) локальные правовые акты (организационно-распорядительные документы), устанавливающие организацию защиты информации ограниченного доступа в государственном органе. Руководитель государственного органа создает (определяет) структурное подразделение или назначает отдельных специалистов, на которых возлагаются обязанности (функции) по защите информации (далее – структурное подразделение (штатные специалисты) по защите информации).

16. Контроль за порядком обработки информации ограниченного доступа осуществляют структурные подразделения (штатные специалисты) по защите информации государственных органов. Работники структурного подразделения (штатные специалисты) по защите информации должны обладать компетенциями, необходимыми для выполнения возложенных на них обязанностей (функций) по защите информации. Не менее 30 процентов работников структурного подразделения по защите информации должны иметь профессиональное образование по специальности или направлению подготовки в области информационной безопасности или пройти обучение по программе профессиональной переподготовки в области информационной безопасности.

17. Структурные подразделения (штатные специалисты) по защите информации государственных органов должны обеспечивать защиту информации во взаимодействии с подразделениями (работниками) государственных органов,

использующими информационные системы, и подразделениями (работниками) государственных органов, обеспечивающими эксплуатацию информационных систем.

Структурные подразделения (штатные специалисты) по защите информации государственных органов обязаны:

разрабатывать и планировать мероприятия и меры по защите информации ограниченного доступа;

применять организационные и технические меры по защите информации ограниченного доступа. При этом должны применяться программные, программно-аппаратные средства, позволяющие обеспечить защиту информации, в том числе, по выявлению угроз безопасности информации, обнаружению и предотвращению вторжений, проведению контроля уровня защищенности информации, мониторингу информационной безопасности, выявлению уязвимостей, контролю настроек и конфигураций информационных систем государственных органов, а также использоваться средства и системы, предназначенные для автоматизации и аналитической поддержки деятельности по защите информации ограниченного доступа.

осуществлять методическое обеспечение деятельности специалистов государственных органов, замещающих должности государственной гражданской службы Московской области, должности, не относящиеся к должностям государственной гражданской службы Московской области, государственные должности Московской области (далее – должностных лиц) по вопросам защиты информации ограниченного доступа;

проводить оценку состояния защиты информации и осуществлять контроль эффективности внедрённых мер и средств защиты информации ограниченного доступа;

совершенствовать мероприятия и меры по защите информации ограниченного доступа.

18. Должностные лица несут предусмотренную законодательством Российской Федерации ответственность за:

разглашение информации ограниченного доступа;

нарушение правил (порядка) обработки (обращения) информации ограниченного доступа;

нарушение порядка обращения с материальными и машинными носителями информации ограниченного доступа;

использование в личных целях информации ограниченного доступа, ставшей им известной при выполнении служебных обязанностей, либо передачу такой информации третьим лицам.

О фактах неправомерного распространения информации ограниченного доступа и (или) доступа к средствам её обработки и хранения необходимо незамедлительно проинформировать ответственное должностное лицо.

19. По фактам выявленных нарушений правил (порядка) обработки (обращения) информации ограниченного доступа руководителем государственного органа принимается решение о проведении служебного расследования (разбирательства).

20. Если действиями (бездействием) должностного лица, связанными с нарушением правил (порядка) обработки (обращения) с информацией ограниченного доступа, причинен материальный ущерб, возмещение ущерба производится в порядке, предусмотренном законодательством Российской Федерации.

IV. Особенности обращения с материальными и машинными носителями информации ограниченного доступа

21. Порядок обращения с документами, изданиями (книгами, журналами, брошюрами, почтовыми отправлениями) и другими материальными и машинными носителями информации, содержащими информацию ограниченного доступа, определяется Инструкцией по делопроизводству в исполнительных органах Московской области, государственных органах Московской области.

Съемные машинные носители информации ограниченного доступа, разрешенные для использования в информационных системах государственных органов, подлежат учету и контролю использования. В информационных системах государственных органов должны использоваться зарегистрированные съемные машинные носители информации ограниченного доступа. В случае обнаружения съемного машинного носителя информации ограниченного доступа без регистрационных реквизитов, такой съемный машинный носитель информации ограниченного доступа должен быть передан в структурное подразделение (штатному специалисту) по защите информации для анализа содержащейся на нем информации ограниченного доступа, программ и при необходимости дальнейшего уничтожения. Подключение обнаруженного незарегистрированного съемного машинного носителя информации ограниченного доступа к информационным системам запрещается.

Контроль за порядком обращения с материальными и машинными носителями информации ограниченного доступа, осуществляется структурными подразделениями (штатными сотрудниками) государственных органов по защите информации.

V. Организация работ при обработке информации ограниченного доступа на средствах вычислительной техники

22. Мероприятия по защите информации ограниченного доступа, обрабатываемой на средствах вычислительной техники (далее – СВТ), являются составной частью деятельности государственных органов по защите информации и осуществляются во взаимосвязи с другими мерами защиты информации.

Обработка информации ограниченного доступа на СВТ допускается только в случае включения СВТ в состав информационных систем, прошедших аттестацию по требованиям защиты информации (или оценку эффективности реализованных в информационной системе мер по обеспечению безопасности информации ограниченного доступа) и введенных в эксплуатацию в установленном законодательством порядке. Возможность обработки информации ограниченного доступа на СВТ в составе информационных систем и перечень информации ограниченного доступа (в том числе состав персональных данных (при наличии)), указываются в эксплуатационной документации на информационную систему, в случае если информационная система является государственной информационной системой – в положении о государственной информационной системе.

Необходимость обеспечения защиты информации ограниченного доступа при её обработке на СВТ должна учитываться при разработке:

политик защиты информации государственного органа;

внутренних регламентов по защите информации, в том числе порядка обработки, хранения и обращения с информацией ограниченного доступа;

внутренних стандартов по защите информации, устанавливающих требования к реализации мер по защите информации применительно к особенностям деятельности государственных органов и функционирования информационных систем.

Структурные подразделения (сотрудники), использующие информационные системы и (или) обеспечивающие эксплуатацию информационных систем, должны участвовать в проведении мероприятий и принятии мер по защите информации в объеме, установленном государственным органом во внутренних стандартах и регламентах по защите информации.

23. При необходимости состав проводимых мероприятий по защите информации ограниченного доступа может быть дополнен в соответствии с решаемыми задачами и конкретными условиями применения СВТ.

VI. Порядок обмена информацией ограниченного доступа

24. Государственные органы вправе использовать информацию ограниченного доступа, по своему усмотрению, в том числе передавать другим лицам по договору или на ином установленном законом основании. При этом обязательным является соблюдение конфиденциальности информации ограниченного доступа, а также требований законодательства Российской Федерации о персональных данных (в случае обработки персональных данных).

25. Информация ограниченного доступа, сформированная в процессе деятельности государственных органов, может предоставляться федеральным органам исполнительной власти Российской Федерации, государственным органам и органам местного самоуправления муниципальных образований Московской области. В этом случае информация ограниченного доступа предоставляется на основании решения руководителя государственного органа.

Приложение
к Порядку обработки информации
ограниченного доступа
в центральных исполнительных
органах Московской области,
государственных органах
Московской области
и государственных учреждениях
Московской области

Перечень сведений,
отнесенных федеральными законами и актами Президента Российской Федерации
к информации ограниченного доступа

1. Данный Перечень сведений, отнесенных федеральными законами и актами Президента Российской Федерации к информации ограниченного доступа, для использования в государственных органах (далее – Перечень сведений) составлен на основании федеральных законов, относящих информацию к информации ограниченного доступа.

2. Перечень сведений не является исчерпывающим и в соответствии с Указом Президента Российской Федерации от 06.03.1997 № 188 «Об утверждении перечня сведений конфиденциального характера» доступ к информации, содержащей служебные сведения, сведения, связанные с профессиональной деятельностью, может быть ограничен иными федеральными законами.

3. Конфиденциальность документов, составленных на основании материалов, поступивших из других организаций, определяется степенью конфиденциальности сведений, содержащихся в этих материалах.

№ п/п	Содержание сведений	Основание для включения в Перечень сведений
1.	Сведения о частной жизни, личной и семейной тайне, переписке, телефонных переговорах, почтовых, телеграфных и иных сообщениях	Конституция Российской Федерации, (статьи 23, 24)
2.	Сведения, содержащие персональные данные (за исключением персональных данных общедоступных категорий)	Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»
3.	Сведения, содержащие служебную информацию, ставшую известной государственному гражданскому служащему в связи с исполнением должностных обязанностей	Федеральный закон от 27.07.2004 № 79-ФЗ «О государственной гражданской службе Российской Федерации» (статья 17)
4.	Сведения об абонентах и оказываемых им услугах связи	Федеральный закон от 07.07.2003 № 126-ФЗ «О связи» (статья 53)

№ п/п	Содержание сведений	Основание для включения в Перечень сведений
5.	Сведения, ставшие известными работнику органа записи актов гражданского состояния или работнику многофункционального центра предоставления государственных и муниципальных услуг в связи с государственной регистрацией акта гражданского состояния	Федеральный закон от 15.11.1997 № 143-ФЗ «Об актах гражданского состояния» (статья 6)
6.	Сведения о доходах, об имуществе и обязательствах имущественного характера	Федеральный закон от 27.07.2004 № 79-ФЗ «О государственной гражданской службе Российской Федерации» (статья 20)
7.	Сведения о населении, содержащиеся в переписных листах	Федеральный закон от 25.01.2002 № 8-ФЗ «О Всероссийской переписи населения» (статья 8)
8.	Сведения, содержащиеся в индивидуальных лицевых счетах	Федеральный закон от 01.04.1996 № 27-ФЗ «Об индивидуальном (персонифицированном) учете в системе обязательного пенсионного страхования» (статья 6)
9.	Сведения о страхователе, застрахованном лице и выгодоприобретателе, состоянии их здоровья, а также об имущественном положении этих лиц	Гражданский кодекс Российской Федерации (статья 946)
10.	Сведения, содержащие информацию о новых решениях и технических знаниях, в том числе не защищаемых законом, а также сведения, в отношении которых их обладателем установлен режим коммерческой тайны (за исключением информации, в отношении которой имеется согласие другой стороны на передачу информации третьим лицам)	Гражданский кодекс Российской Федерации (статья 727)
11.	Сведения о частной жизни лица, подавшего жалобу, и других лиц, ставшие известными Уполномоченному по правам человека в субъекте Российской Федерации в процессе рассмотрения жалобы, без их письменного согласия	Федеральный закон от 18.03.2020 № 48-ФЗ «Об уполномоченных по правам человека в субъектах Российской Федерации» (статья 10)
12.	Сведения о местах дислокации или о передислокации органов управления войсками национальной гвардии, объединений, соединений, воинских частей войск национальной гвардии, а также обеспечивается конфиденциальность сведений о военнослужащих (сотрудниках) войск национальной гвардии и членах их семей	Федеральный закон от 03.07.2016 № 226-ФЗ «О войсках национальной гвардии Российской Федерации» (статья 23)
13.	Сведения, содержащие информацию, полученную в ходе действий должностных лиц органа государственного контроля при	Федеральный закон от 18.07.1999 № 183-ФЗ «Об экспортном контроле» (статья 17)

№ п/п	Содержание сведений	Основание для включения в Перечень сведений
	проведении проверок российских участников внешнеэкономической деятельности	
14.	Сведения, касающиеся предмета договора на выполнение научно-исследовательских работ, опытно-конструкторских и технологических работ, хода его исполнения и полученных результатов (в объеме, определенном договором)	Гражданский кодекс Российской Федерации (статья 771)
15.	Сведения, полученные пользователем по договору коммерческой концессии, содержащие секреты производства (ноу-хау) правообладателя и другую полученную от него конфиденциальную коммерческую информацию	Гражданский кодекс Российской Федерации (статья 1032)
16.	Сведения о данных предварительного расследования лицом, предупрежденным в установленном законом порядке о недопустимости их разглашения	Уголовный кодекс Российской Федерации (статья 310) Уголовно-процессуальный кодекс Российской Федерации (статья 161)
17.	Сведения, содержащие: суждения, имевшие место во время совещания суда присяжных заседателей в совещательной комнате; суждения, имевшие место при обсуждении и постановлении приговора	Уголовно-процессуальный кодекс Российской Федерации (статьи 298, 341)
18.	Сведения о мерах безопасности, применяемых в отношении судьи, присяжного заседателя или иного лица, участвующего в отправлении правосудия, судебного пристава, судебного исполнителя, потерпевшего, свидетеля, других участников уголовного процесса, а равно в отношении их близких	Уголовный кодекс Российской Федерации (статья 311)
19.	Сведения о мерах безопасности, применяемых в отношении должностного лица правоохранительного или контролирующего органа, а также его близких	Уголовный кодекс Российской Федерации (статья 320)
20.	Конфиденциальные сведения о музейных предметах, включенных в состав негосударственной части Музейного фонда Российской Федерации	Федеральный закон от 26.05.1996 № 54-ФЗ «О Музейном фонде Российской Федерации и музеях в Российской Федерации» (статья 38)
21.	Первичные статистические данные, содержащиеся в формах федерального статистического наблюдения	Федеральный закон от 29.11.2007 № 282-ФЗ «Об официальном статистическом учете и системе государственной статистики в Российской Федерации» (статья 9)
22.	Сведения, содержащиеся в анкете ребенка, гражданина, желающего принять ребенка на воспитание в свою семью, гражданина,	Федеральный закон от 16.04.2001 № 44-ФЗ «О государственном банке данных о детях, оставшихся без попечения родителей»

№ п/п	Содержание сведений	Основание для включения в Перечень сведений
	лишенного родительских прав или ограниченного в родительских правах, гражданина, отстраненного от обязанностей опекуна (попечителя) за ненадлежащее выполнение возложенных на него законом обязанностей, бывшего усыновителя, если усыновление отменено судом по его вине	(статья 8)
23.	Сведения любого характера (производственные, технические, экономические, организационные и другие), в том числе о результатах интеллектуальной деятельности в научно-технической сфере, а также сведения о способах осуществления профессиональной деятельности, которые имеют действительную или потенциальную коммерческую ценность в силу неизвестности их третьим лицам, к которым у третьих лиц нет свободного доступа на законном основании и в отношении которых обладателем таких сведений введен режим коммерческой тайны	Федеральный закон от 29.07.2004 № 98-ФЗ «О коммерческой тайне» (статья 3)
24.	Сведения о специальных средствах, технических приемах, тактике осуществления мероприятий по борьбе с терроризмом, а также о составе их участников	Федеральный закон от 06.03.2006 № 35-ФЗ «О противодействии терроризму» (статья 2)

