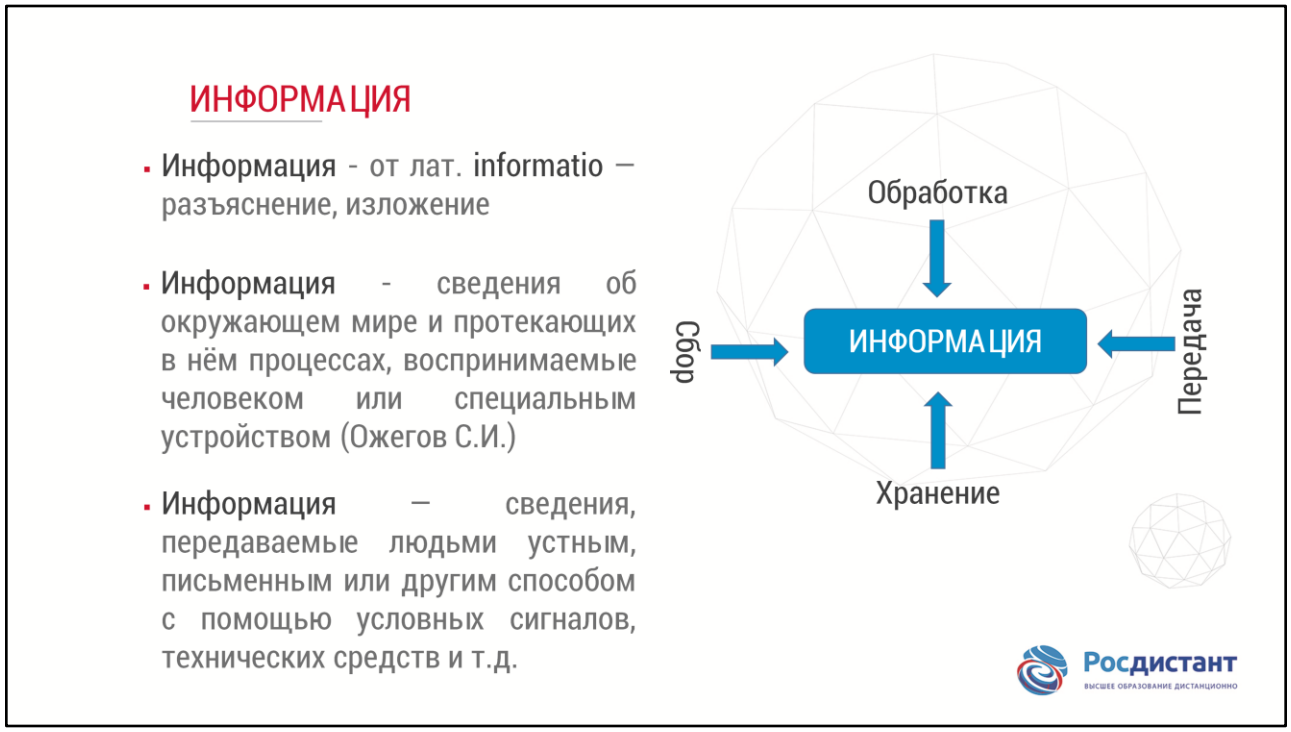

Росдистант
ВЫСШЕЕ ОБРАЗОВАНИЕ ДИСТАНЦИОННО
ЦИФРОВАЯ
КУЛЬТУРА
3 ЧАСТЬ




**Слайд 32**

**Тема 1. Введение в цифровую культуру**

**Лекция 1.3. Безопасность цифровой среды**

С середины двадцатого века информация является общенаучным понятием, включающим в себя:

- сведения, передаваемые между людьми, человеком и автоматом, автоматом и автоматом;
- сигналы в животном и растительном мире;
- признаки, передаваемые от клетки к клетке, от организма к организму;

и так далее.

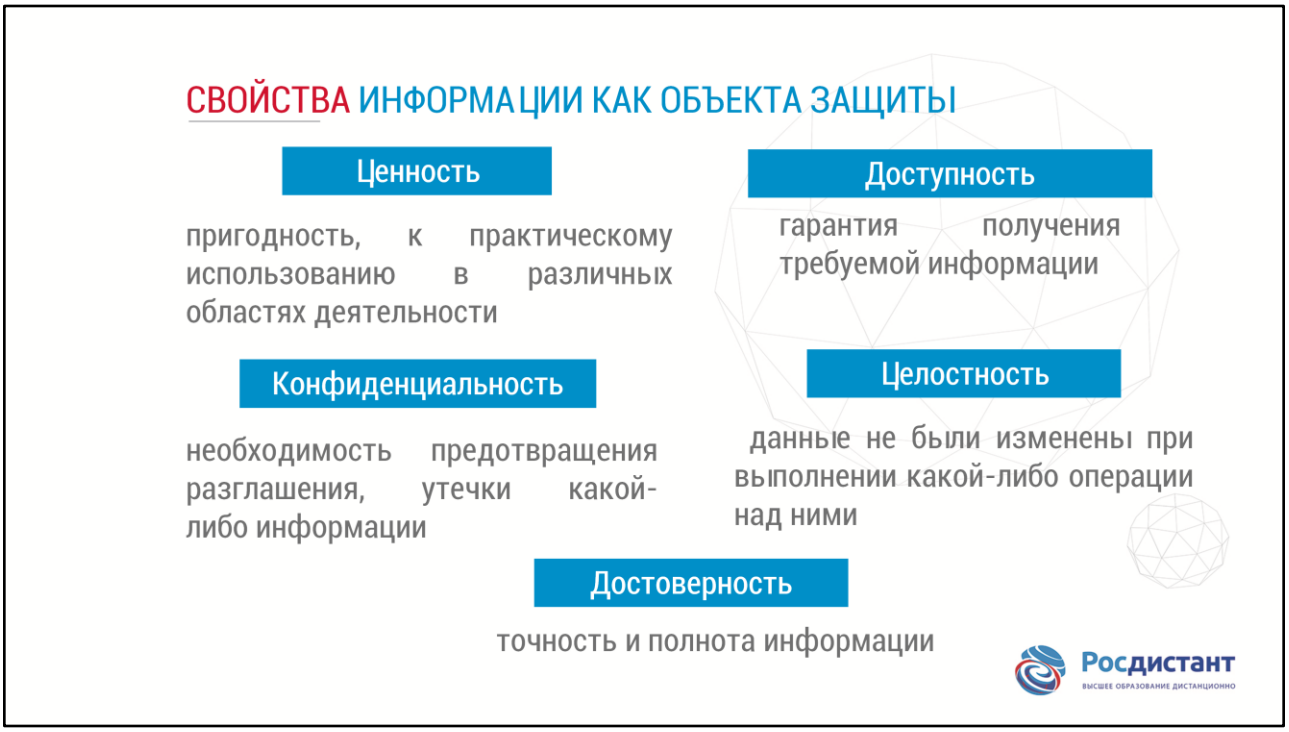
Информация как объект познания имеет ряд особенностей:

- она нематериальна по своей природе, отображается в виде символов на носителях;
- после записи на носитель информация приобретает определённые параметры и может быть измерена в объеме;
- информация, записанная на материальный носитель, может храниться, обрабатываться, передаваться по различным каналам связи;
- перемещаясь по линиям связи, информация создает физические поля, которые отражают ее содержание.

Другими словами, информация носит фундаментальный и универсальный характер, являясь многозначным понятием.

В рамках рассматриваемой дисциплины, под информацией мы будем понимать

сведения, являющиеся объектом сбора, хранения, обработки, непосредственного использования и передачи в информационных системах. Опираясь на это определение информации, будем рассматривать основные понятия информационной безопасности и защиты информации.




**Слайд 33**

Информация как объект защиты обладает множеством свойств. Перечислим важнейшие из них.

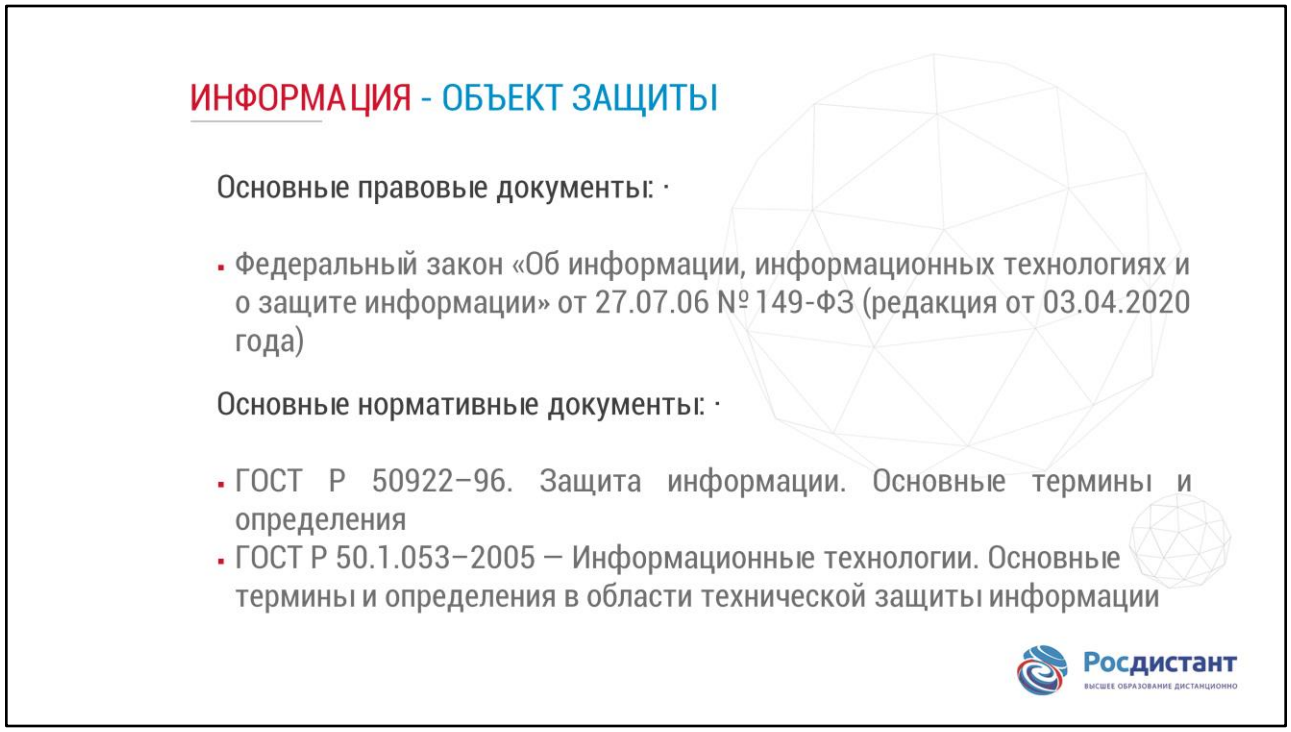
Ценность. Как предмет собственности информация имеет определенную ценность. Именно потому, что информация имеет ценность, ее необходимо защищать.

Конфиденциальность информации – субъективно определяемая характеристика информации, указывающая на необходимость введения ограничений на круг субъектов, имеющих доступ к данной информации. Эта характеристика обеспечивается способностью системы сохранять указанную информацию втайне от субъектов, не имеющих полномочий на доступ к ней.

Целостность информации – свойство информации существовать в неискаженном виде.

Достоверность информации – адекватность, то есть полнота и точность отображения состояния предметной области и непосредственно целостности информации, то есть ее не искаженности. Вопросы обеспечения адекватности отображения выходят за рамки проблемы обеспечения информационной безопасности.

Доступность информации – свойство системы, в которой циркулирует информация, обеспечивать своевременный беспрепятственный доступ субъектов к интересующей их информации.




**Слайд 34**

Основные понятия по информационной безопасности регламентируются нормативными и правовыми документами.

В российском законодательстве базовым законом в области защиты информации является Федеральный закон «Об информации, информационных технологиях и о защите информации».

Поэтому основные понятия и решения, закрепленные в законе, требуют пристального рассмотрения.

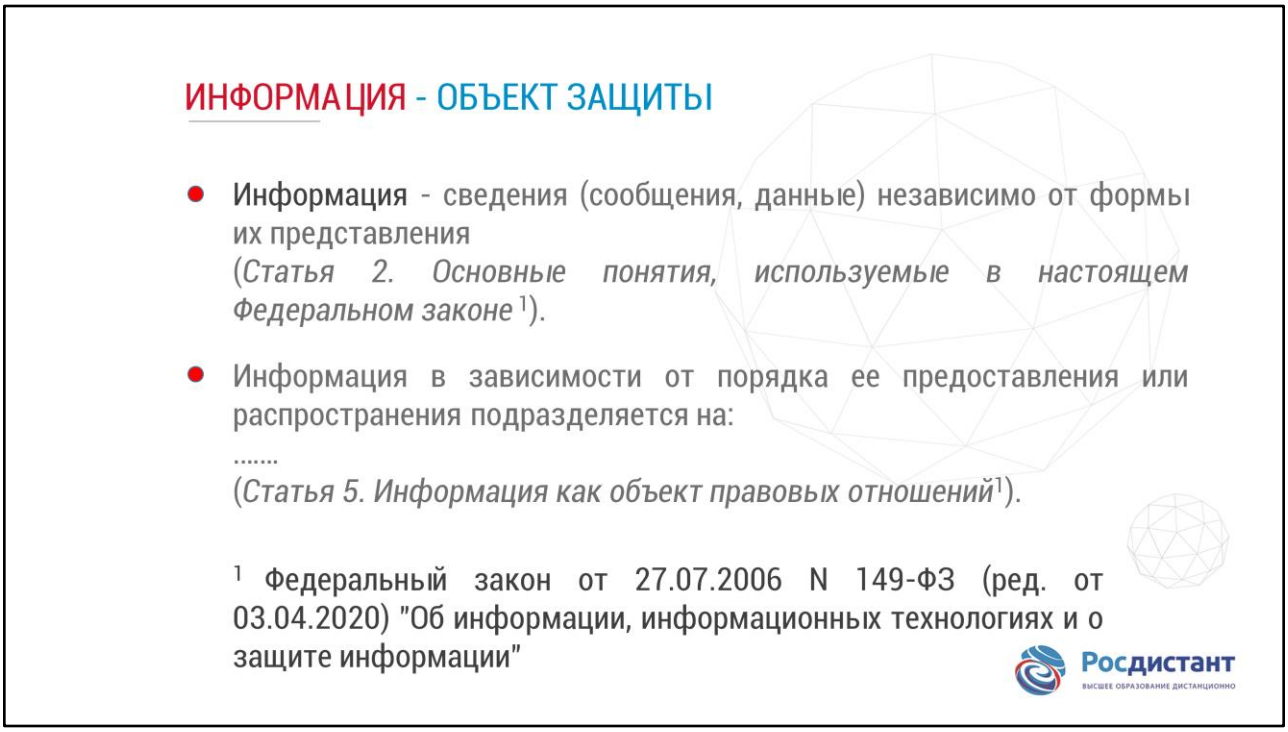
Закон дает основные определения в области защиты информации.

Настоящий Федеральный закон регулирует отношения, возникающие:

- при осуществлении права на поиск, получение, передачу, производство и распространение информации;
- применении информационных технологий;
- обеспечении защиты информации.

Положения настоящего Федерального закона не распространяются на отношения, возникающие при правовой охране результатов интеллектуальной деятельности и приравненных к ним средств индивидуализации.

За исключением случаев, предусмотренных настоящим Федеральным законом.



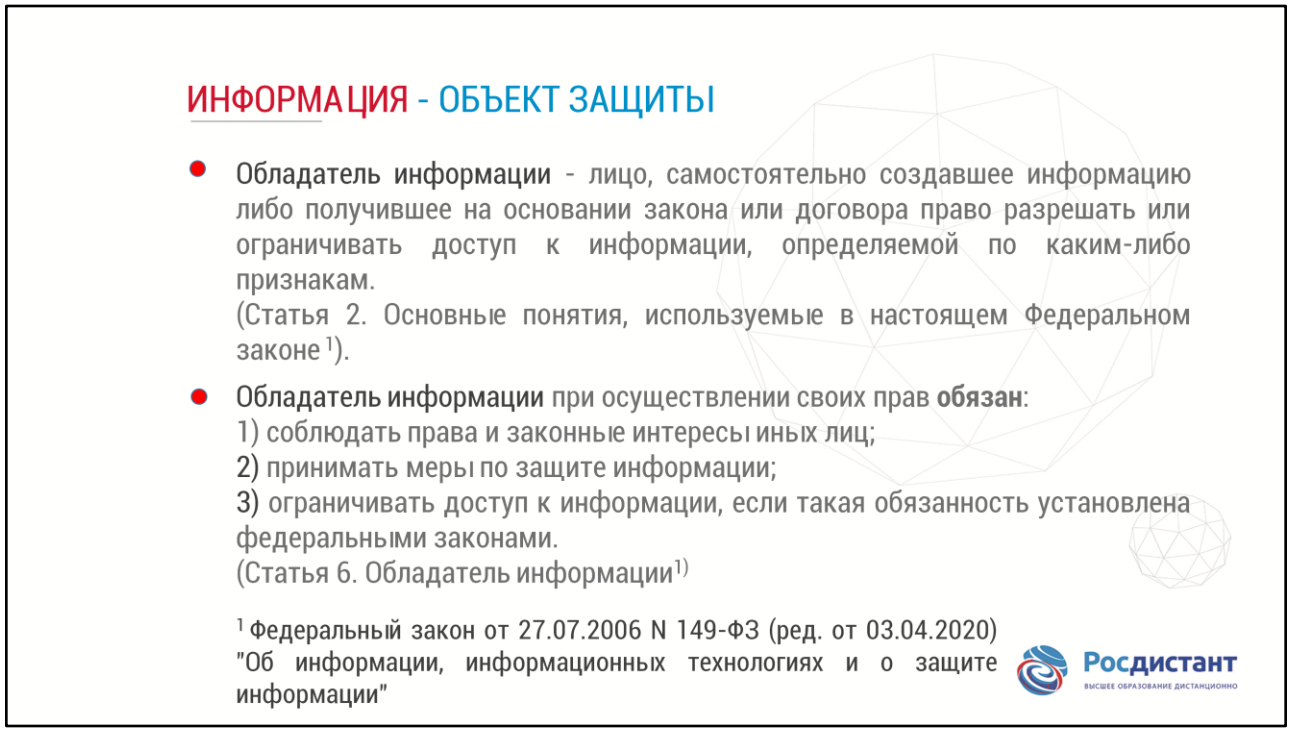

**Слайд 35**

Информация может являться объектом публичных, гражданских и иных правовых отношений.

Информация может свободно использоваться любым лицом и передаваться одним лицом другому лицу, если федеральными законами не установлены ограничения доступа к информации либо иные требования к порядку ее предоставления или распространения.

Информация в зависимости от порядка ее предоставления или распространения подразделяется:

- на информацию, свободно распространяемую;
- информацию, предоставляемую по соглашению лиц, участвующих в соответствующих отношениях;
- информацию, которая в соответствии с федеральными законами подлежит предоставлению или распространению;
- информацию, распространение которой в Российской Федерации ограничивается или запрещается.



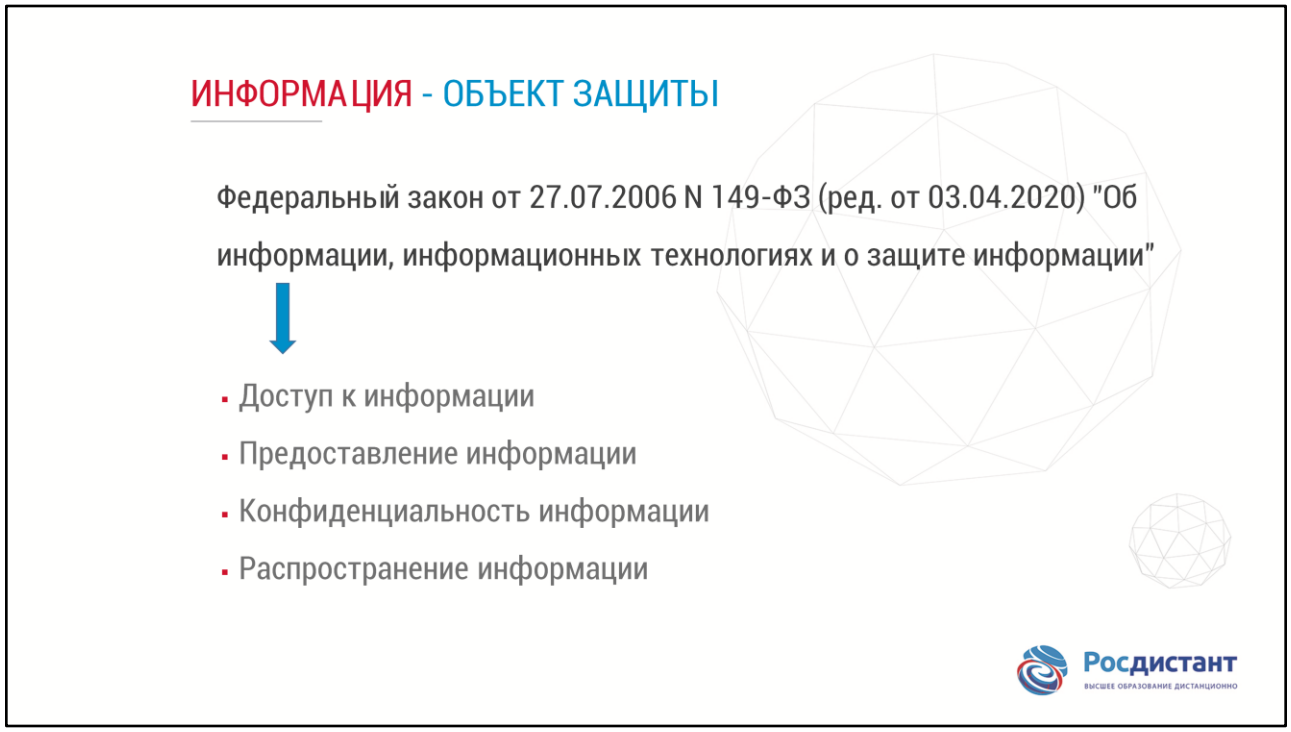

**Слайд 36**

Обладателем информации может быть:

- гражданин, то есть физическое лицо;
- организации, то есть юридическое лицо;
- Российская Федерация;
- субъект Российской Федерации;
- муниципальное образование.

Обладатель информации, если иное не предусмотрено федеральными законами, вправе:

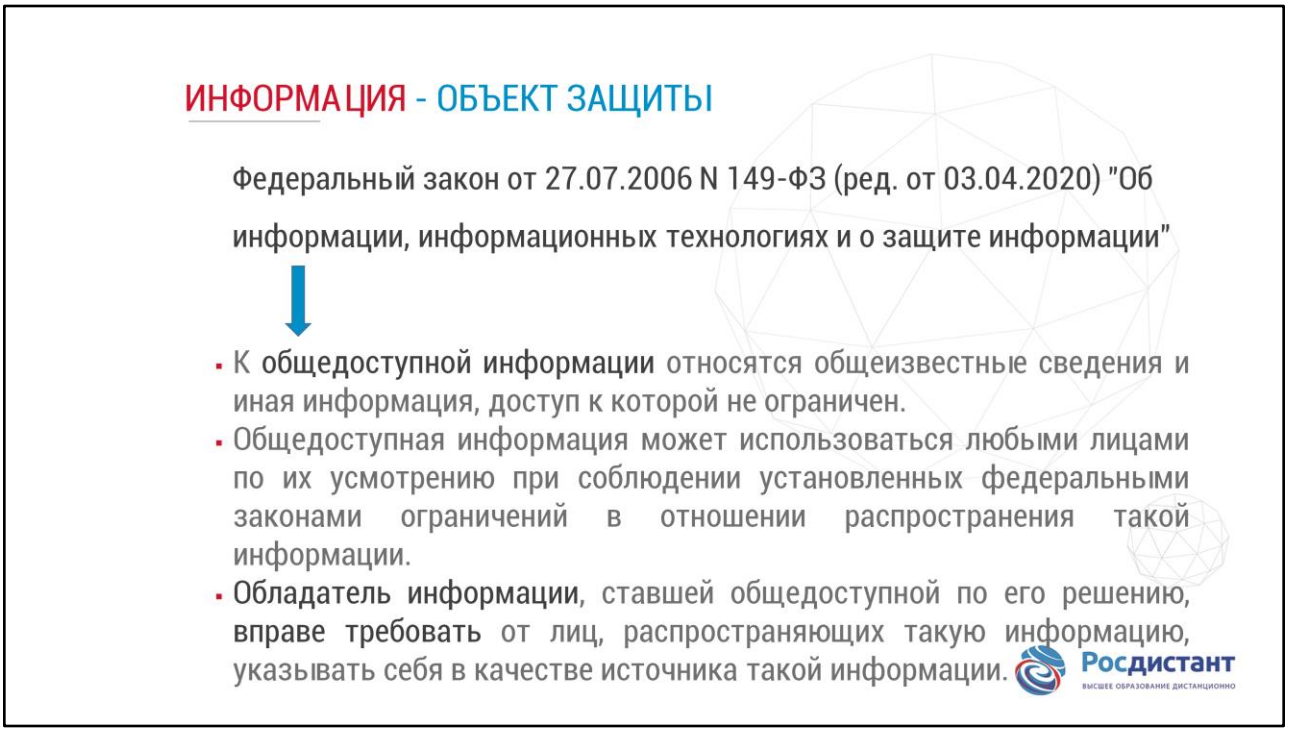
- разрешать или ограничивать доступ к информации, определять порядок и условия такого доступа;
- использовать информацию, в том числе распространять ее, по своему усмотрению;
- передавать информацию другим лицам по договору или на ином установленном законом основании;
- защищать установленными законом способами свои права в случае незаконного получения информации или ее незаконного использования иными лицами;
- осуществлять иные действия с информацией или разрешать осуществление таких действий.




**Слайд 37**

В статье 2 Федерального закона «Об информации, информационных технологиях и о защите информации» определены следующие понятия:

- доступ к информации – это возможность получения информации и ее использования;
- конфиденциальность информации – обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя;
- предоставление информации – действия, направленные на получение информации определенным кругом лиц или передачу информации определенному кругу лиц;
- распространение информации – действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц.

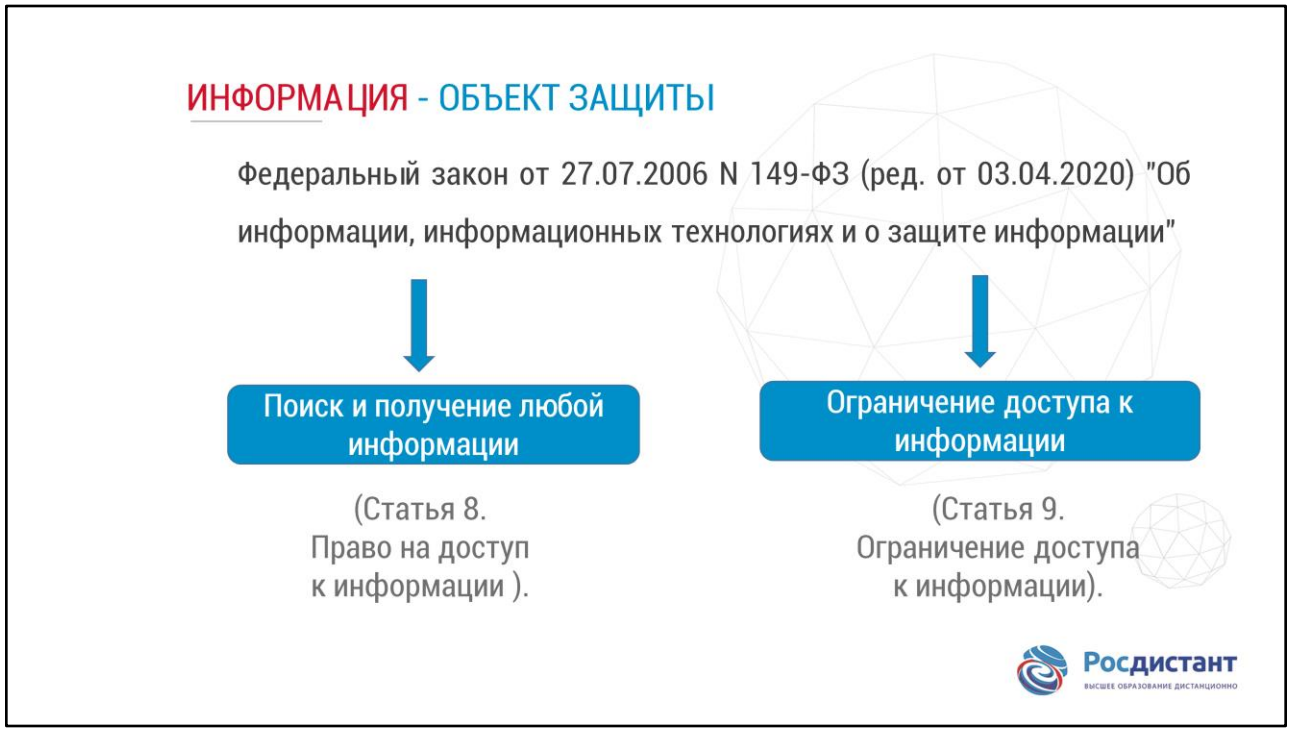



**Слайд 38**

В статье 7 Федерального закона «Об информации, информационных технологиях и о защите информации» определены также положения:

- общедоступная информация может использоваться любыми лицами по их усмотрению при соблюдении установленных федеральными законами ограничений в отношении распространения такой информации;
- обладатель информации, ставшей общедоступной по его решению, вправе требовать от лиц, распространяющих такую информацию, указывать себя в качестве источника такой информации;
- информация, размещаемая ее обладателями в сети Интернет в формате, допускающем автоматизированную обработку без предварительных изменений человеком в целях повторного ее использования, является общедоступной информацией.

Эта информация размещается в форме открытых данных.




**Слайд 39**

Граждане и организации вправе осуществлять поиск и получение любой информации в любых формах и из любых источников при условии соблюдения требований, установленных настоящим Федеральным законом и другими федеральными законами.

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

Обязательным является соблюдение конфиденциальности информации, доступ к которой ограничен федеральными законами.

Запрещается требовать от гражданина предоставления информации о его частной жизни, в том числе информацию, составляющей личную тайну.

Получать такую информацию помимо воли гражданина запрещается, если иное не предусмотрено федеральными законами.

Порядок доступа к персональным данным граждан устанавливается федеральным законом о персональных данных.


**Слайд 40**

Необходимость обеспечения безопасности персональных данных в наше время – объективная реальность.

Современный человек не может самостоятельно противодействовать посягательству на его частную жизнь.

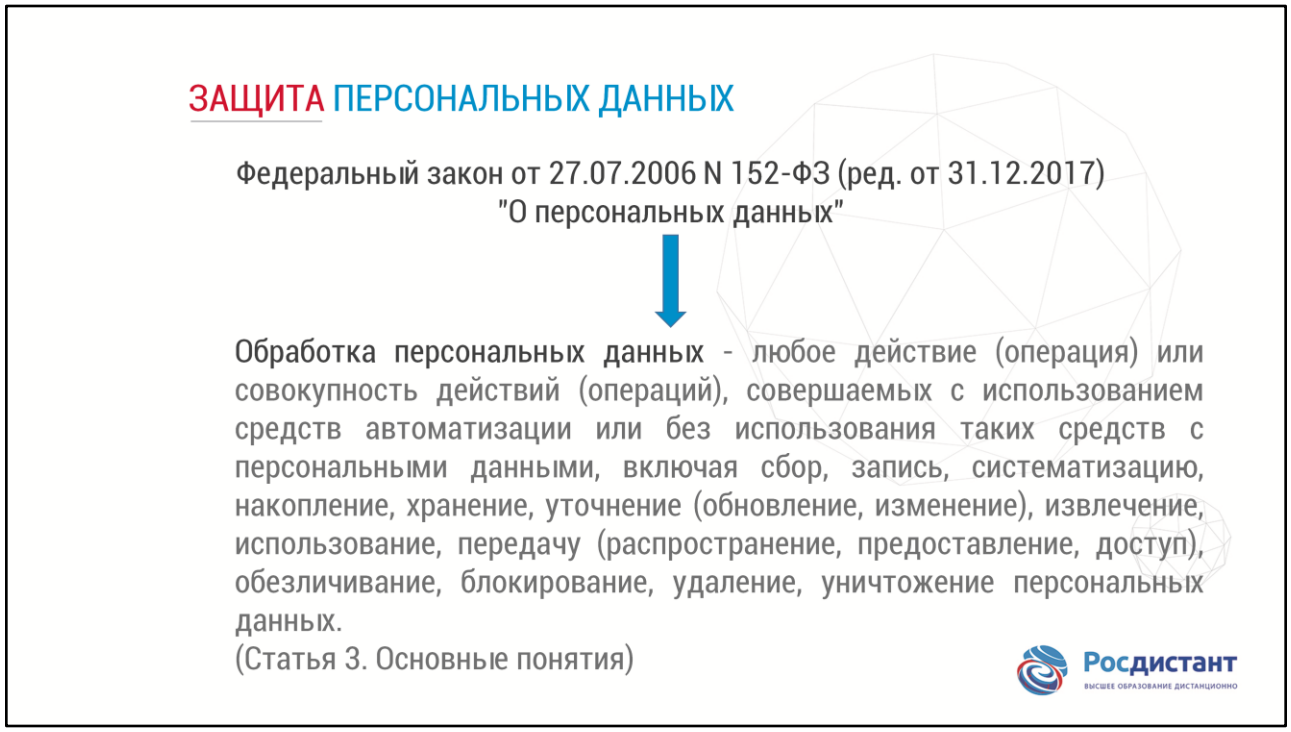
Возросшие технические возможности по сбору и обработке персональной информации, развитие средств электронной коммерции и социальных сетей делают необходимым принятие мер по защите персональных данных.

Рассмотрим пример из повседневной жизни, когда нарушаются права человека на конфиденциальность персональных данных. Например, покупатель в магазине оформляет дисконтную карту. При оформлении карты он указывает следующие сведения: фамилию, номер телефона, электронный адрес, а затем получает сообщения и письма совершенно из других магазинов, в которых даже никогда не бывал. То есть магазин без согласия покупателя передал его данные третьим лицам.

Кража персональных данных может нанести правообладателю ощутимый материальный ущерб, если речь идет о кредитных картах или информации о сбережениях в банке. Злоумышленники, обладающие достаточными техническими знаниями, похищают реквизиты банковских карт – это ски́мминг. Имитируют сайты финансовых учреждений, чтобы заставить пользователя показать свою личную информацию – фи́шинг.

На самом деле зачастую даже трудно установить источник утечки персональных

данных вследствие высокой информатизации современного общества.




**Слайд 41**

Основополагающим законом в области защиты персональных данных является Федеральный закон «О персональных данных», который вступил в силу с 26 января 2007 года. Закон определяет:

- основные понятия, связанные с обработкой персональных данных;
- принципы и условия обработки персональных данных;
- обязанности оператора персональных данных;
- права субъекта персональных данных.

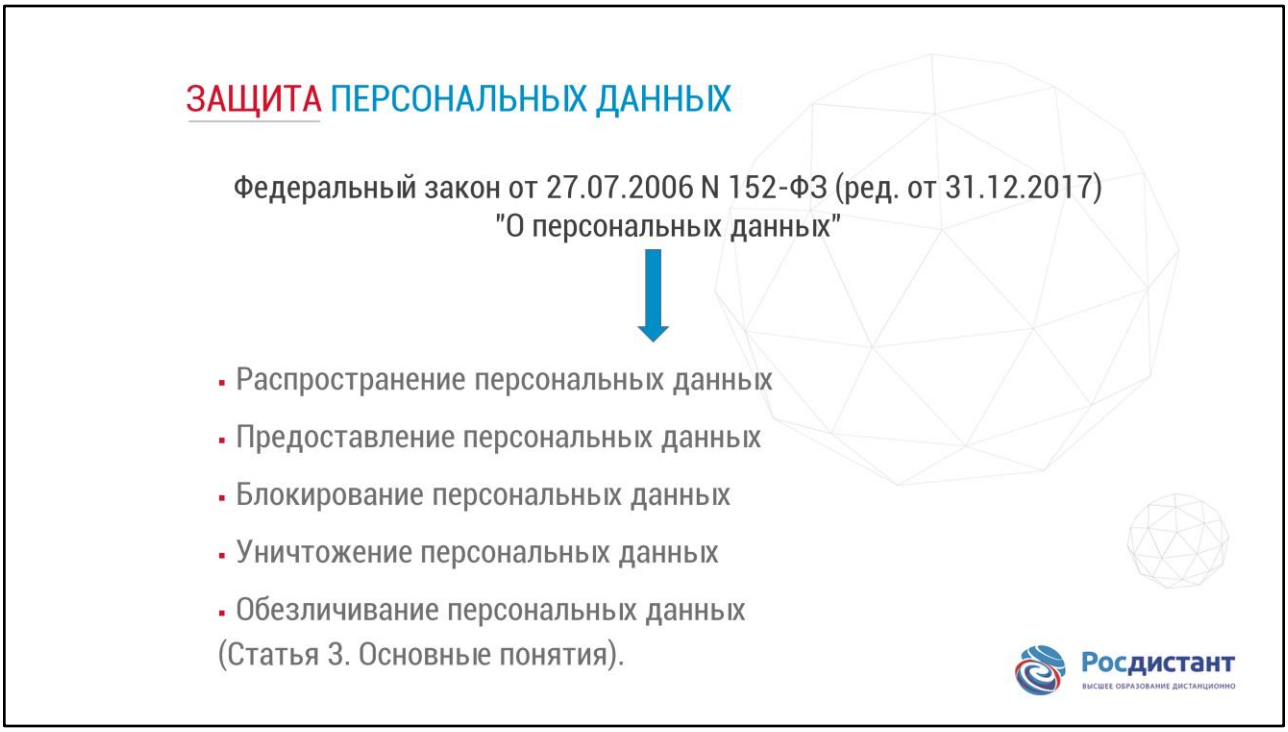
А также:

- виды ответственности за нарушение требований федерального закона;
- государственные органы, осуществляющие контроль соблюдения требований федерального закона.

Персональные данные могут обрабатываться в следующих случаях и при выполнении любого из условий:

- если есть согласие субъекта. Согласие не обязательно может быть письменным. Достаточно поставить галочку на сайте или ответить на вопрос по телефону;
- вы заключили или собираетесь заключить договор с субъектом – даже если это оферта на веб-сайте и для заключения не нужна подпись. В таком случае даже согласия не нужно;
- обработка персональных данных работников организации. Здесь согласие также не нужно;

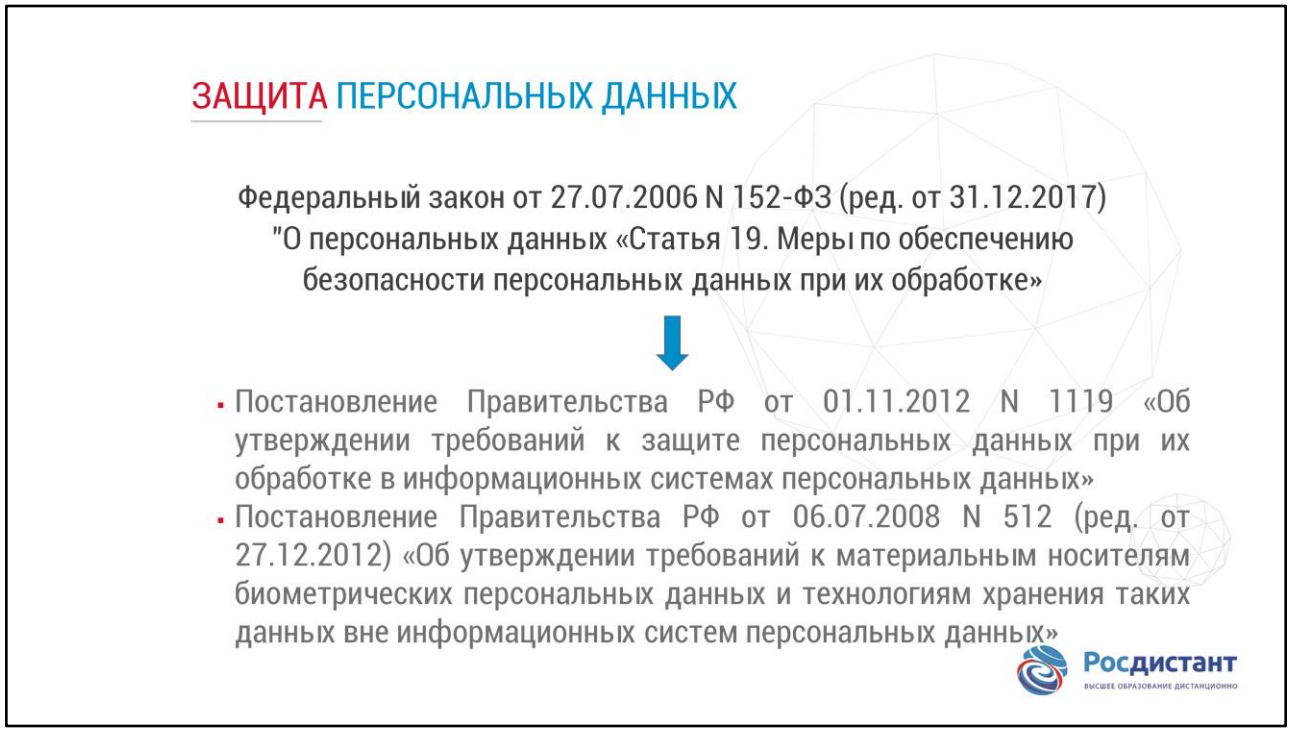
- в иных специфических случаях, они указаны в Законе о персональных данных и достаточно редки.




**Слайд 42**

В целях настоящего Федерального закона используются следующие основные понятия:

- распространение персональных данных – это действия, направленные на раскрытие персональных данных неопределенному кругу лиц;
- предоставление персональных данных – это действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц;
- блокирование персональных данных – это временное прекращение обработки персональных данных, за исключением случаев, если обработка необходима для уточнения персональных данных;
- уничтожение персональных данных – это действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных. К уничтожению персональных данных относятся уничтожение материальных носителей персональных данных;
- обезличивание персональных данных – это действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.

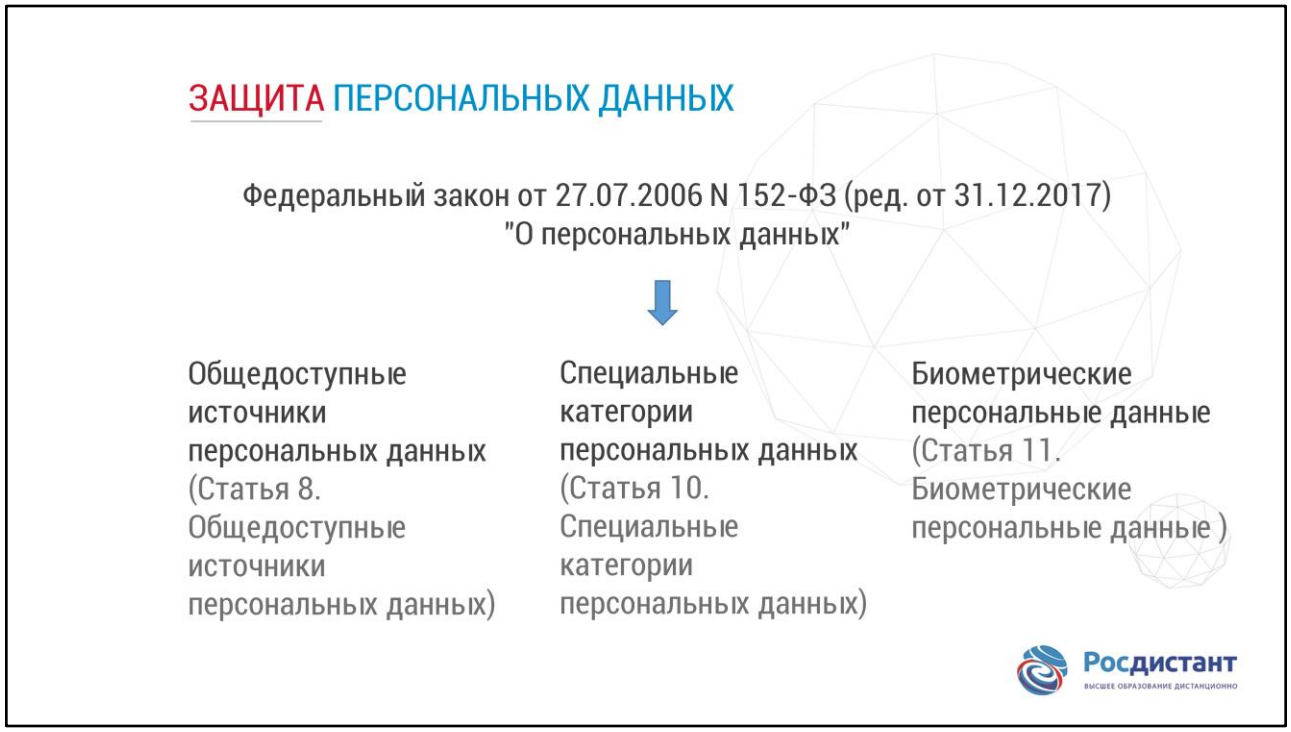



Государство на законодательном уровне требует от организаций и физических лиц, обрабатывающих персональные данные, обеспечить их защиту.

В статье 19 указано, что Правительство Российской Федерации устанавливает:

- уровни защищенности персональных данных при их обработке в информационных системах персональных данных в зависимости от угроз безопасности этих данных;
- требования к защите персональных данных при их обработке в информационных системах персональных данных, исполнение которых обеспечивает установленные уровни защищенности персональных данных;
- требования к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных.

Требования к защите персональных данных устанавливаются с учетом возможного вреда субъекту персональных данных, объема и содержания обрабатываемых данных и вида деятельности.




**Слайд 44**

Федеральный закон «О персональных данных» выделяет категории персональных данных.

Первое. В общедоступные источники персональных данных с письменного согласия субъекта персональных данных могут включаться:

- фамилия, имя, отчество;
- год и место рождения;
- адрес, абонентский номер;
- сведения о профессии.

Сюда также могут быть добавлены и иные персональные данные, предоставленные субъектом персональных данных.

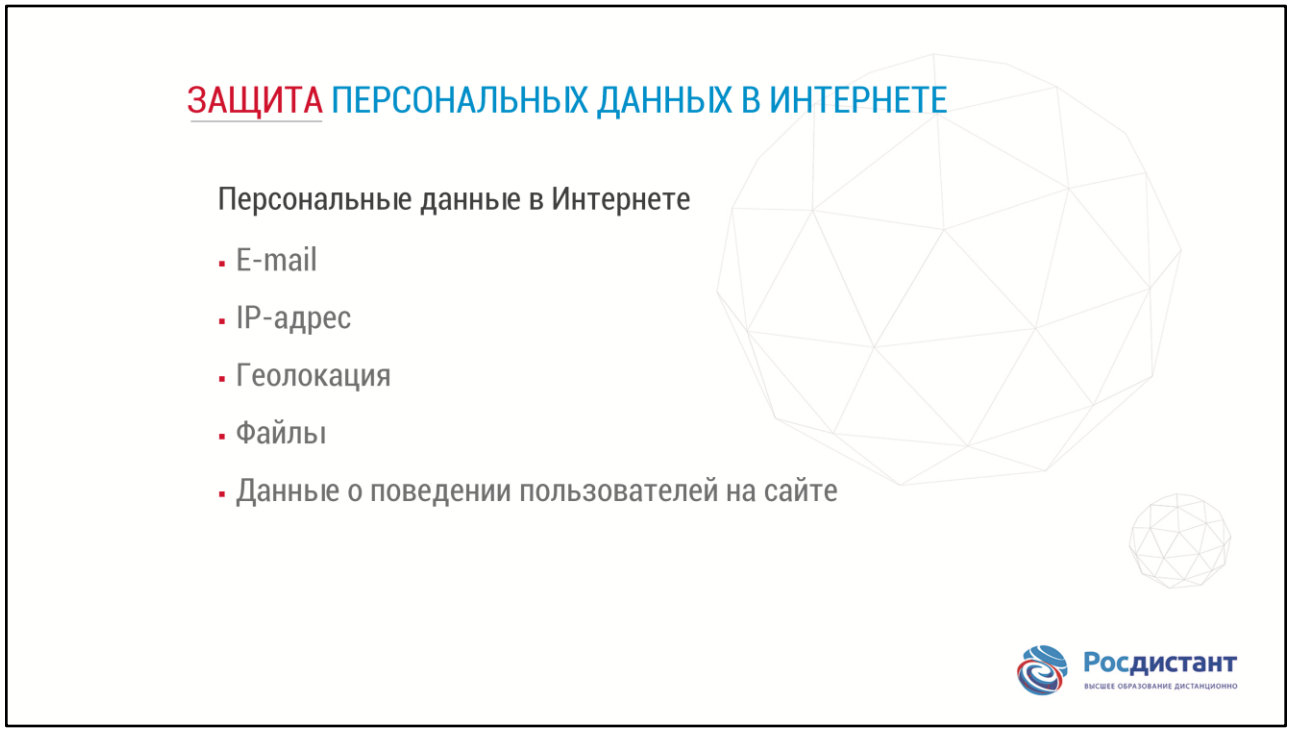
Сведения о субъекте персональных данных должны быть в любое время исключены из общедоступных источников персональных данных по требованию субъекта персональных данных либо по решению суда или иных уполномоченных государственных органов.

Второе. Специальные категории персональных данных, которые представляют собой сведения:

- о расовой и национальной принадлежности;
- политической, религиозной, философской принадлежности;
- состоянии здоровья;
- личной жизни.

Третье. Биометрические персональные данные, которые представляют собой

сведения, характеризующие физиологические особенности человека, и на основе которых можно установить его личность. Они могут обрабатываться только при наличии согласия в письменной форме субъекта персональных данных.




**Слайд 45**

Федеральный закон «О персональных данных» определяет сведения, позволяющие идентифицировать человека по его персональным данным. Согласно данному закону к персональным данным относятся – фамилия, имя, отчество, полная дата рождения, место жительства, серия и номер паспорта, место работы.

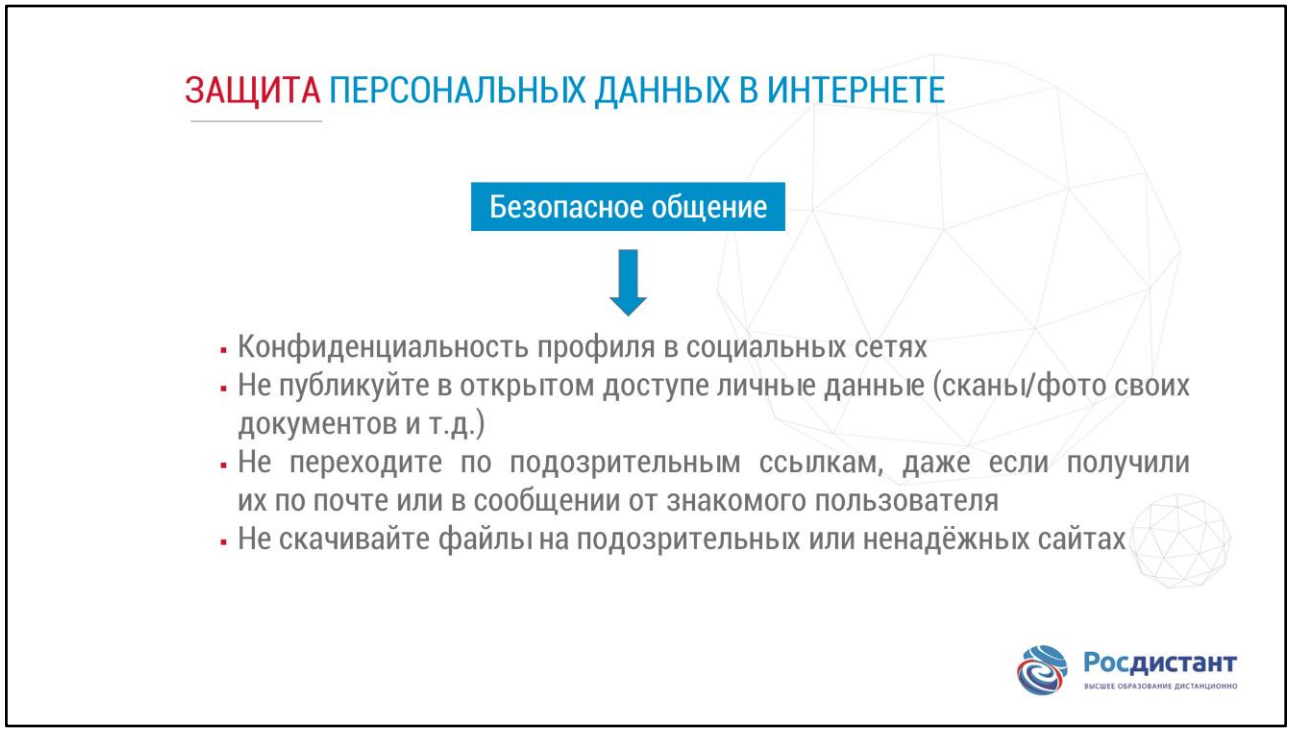
А вот пароль от интернет-акка́унта к персональным данным не относится, поскольку личность пользователя не идентифицирует.

Серверы большинства интернет-компаний расположены в США.

Изменения, внесенные в Федеральный закон «О персональных данных», обязали компании обеспечить хранение данных российских пользователей Интернета в пределах страны. Поэтому ожидается увеличение количества российских дата-центров.

К категории персональных данных в Интернет, которые прямо не указаны законом, могут быть отнесены данные, которые владельцы сайтов получают от пользователей, заходящих на ресурс:

- электронная почта;
- IP-адрес;
- геолокация;
- файлы;
- данные о поведении пользователей на сайте.




**Слайд 46**

Сайты, приложения, социальные сети и поисковые системы постоянно занимаются тем, что собирают информацию о пользователях.

Полученные данные используются для анализа интересов посетителей страниц, их покупательной активности и спроса, для изучения целевой аудитории и настроек рекламы.

Этими данными легко могут воспользоваться злоумышленники. Ваш аккаунт могут взломать, а личные данные передать третьим лицам, которые используют их в мошеннических или других преступных целях. Чтобы этого не произошло, соблюдайте несколько простых правил защиты персональных данных в сети Интернет.

Безопасное общение.

Соцсеть – это источник информации для злоумышленников, собирающих персональные данные, которые они затем используют для мошенничества. Поэтому важно правильно настроить конфиденциальность своего профиля в соцсети.

Не публикуйте в социальных сетях фотографии документов, билетов, платежных чеков и других документов.

Не стоит в соцсетях публиковать информацию о том, когда и где Вы собираетесь провести свой отпуск. Эти данные очень интересуют как кибермошенников, охотящихся за чужими финансами, так и обычных домушников, ждущих, когда люди уйдут куда-нибудь надолго.

Пароли.
Избегайте ненадежных паролей. Создавайте сложные пароли и чаще их меняйте.
Не используйте для паролей информацию, которую злоумышленники могут найти самостоятельно – дату рождения, номера документов, телефонов, имена ваших друзей и родственников, адрес и так далее.
Не используйте одинаковые пароли на разных сайтах.
Регулярно меняйте пароли.


**Слайд 47**

Электронная почта.

В почте хранятся ключи от большинства учетных записей пользователя. Например, процедура восстановления пароля. Поэтому заведите несколько почтовых ящиков – к основному почтовому адресу будет привязан интернет-банк и самые важные для пользователя сайты, а к дополнительному – развлечения.

Использовать двухфакторную авторизацию – привязка аккаунта к номеру телефона.

Wi-Fi.

Не используйте открытые Wi-Fi-сети. Общественные Wi-Fi-сети – это не только выход в Интернет, но и большие шансов слить свои пароли киберпреступникам. В общественном месте не заходите на сайты, которые требуют ввода паролей и личных данных, делайте это по мобильной сети или через домашний Wi-Fi.


**Слайд 48**

Политика конфиденциальности.

Прежде чем установить приложение или браузерное расширение, воспользоваться онлайн-сервисом или зарегистрироваться в социальной сети, обязательно изучите политику конфиденциальности.

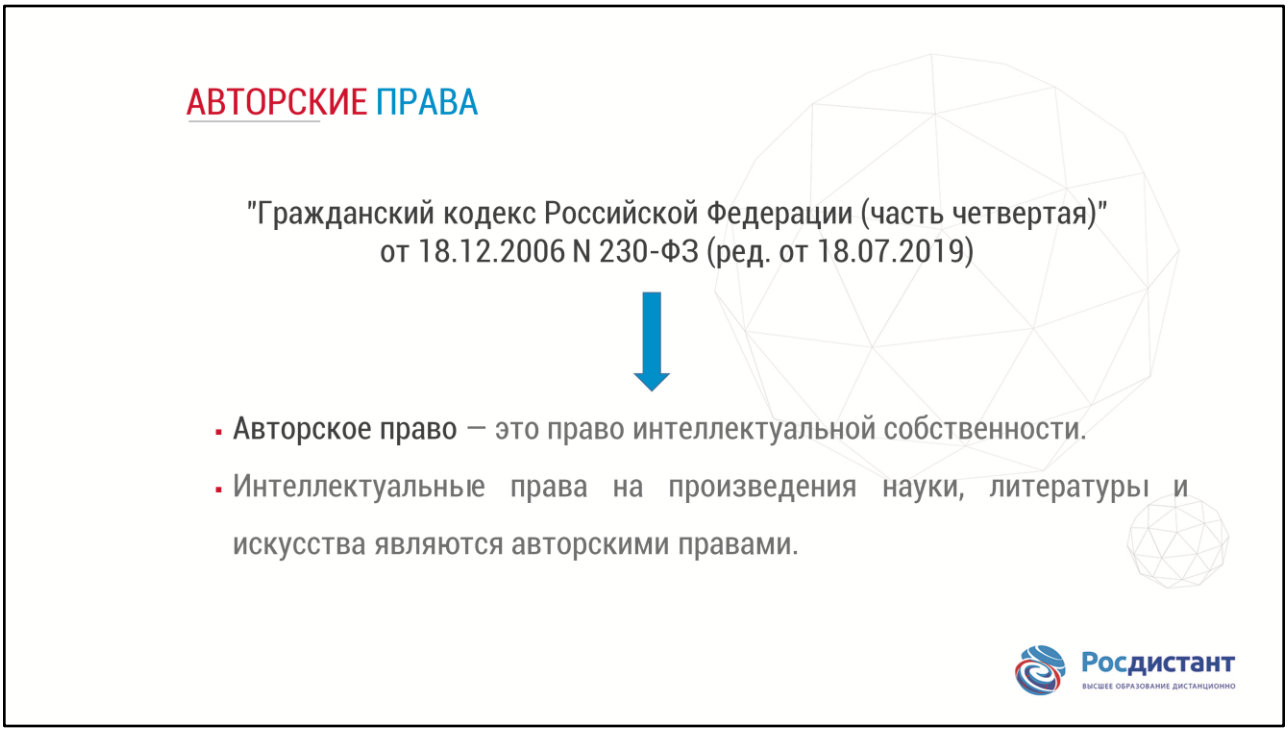
Убедитесь, что приложение или сайт не получает права распоряжаться вашими личными данными – фотографиями, электронным адресом или номером телефона.

Многие приложения запрашивают данные об электронной почте или доступ к камере и микрофону. Не выдавайте разрешений автоматически, следите за тем, какую информацию запрашивает приложение. В некоторых случаях разумнее вообще отказаться от его использования, чтобы не передавать личные данные о себе неизвестным лицам.

Контроль доступа сервисов к личной информации. Включайте на устройстве – смартфоне, планшете, ноутбуке, компьютере функцию разрешения или запрета получения приложением персональных данных.

Не разрешайте браузеру автоматически запоминать пароли к личным сайтам и страницам, а лучше отключите эту опцию в настройках. Особенно это касается сайтов, где необходимо вводить номера документов или банковской карты.

Отключите синхронизацию браузера на компьютере и в смартфоне – при утере телефона все личные страницы и аккаунты станут доступны для посторонних.

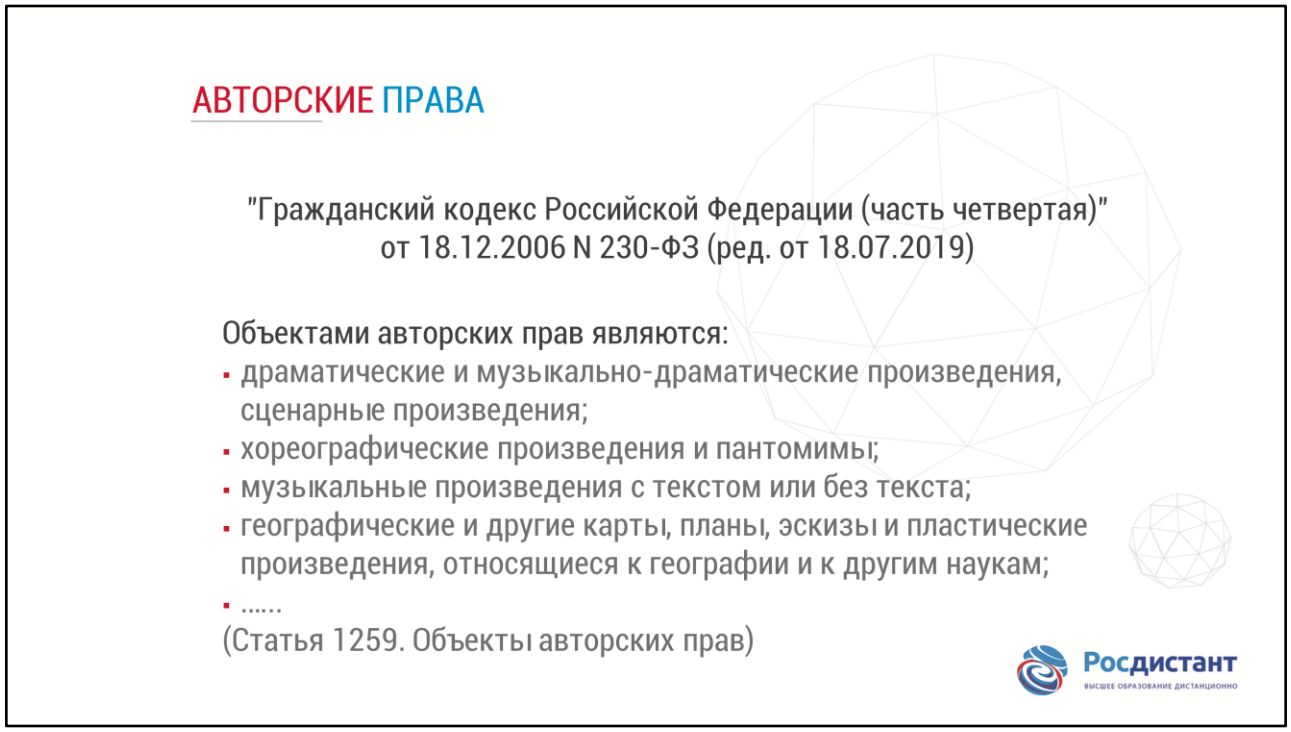



**Слайд 49**

Авторское право – это закрепленная законом совокупность имущественных и неимущественных прав, принадлежащих человеку в рамках того, что он создал. Согласно Гражданскому кодексу Российской Федерации Интеллектуальные права на произведения науки, литературы и искусства являются авторскими правами.

Автору произведения принадлежат следующие права:

- исключительное право на произведение;
- право авторства;
- право автора на имя;
- право на неприкосновенность произведения;
- право на обнародование произведения.




**Слайд 50**

Большинство пользователей Интернет размещают на ресурсах свои материалы – статьи, фотографии, посты в социальной сети и так далее.

Автором произведения считается его создатель, а права вступают в силу с момента его появления. За кражу любого имущества предусмотрена ответственность. Авторское право защищает все виды контента, и это указано в статье 1259 Гражданского кодекса Российской Федерации.

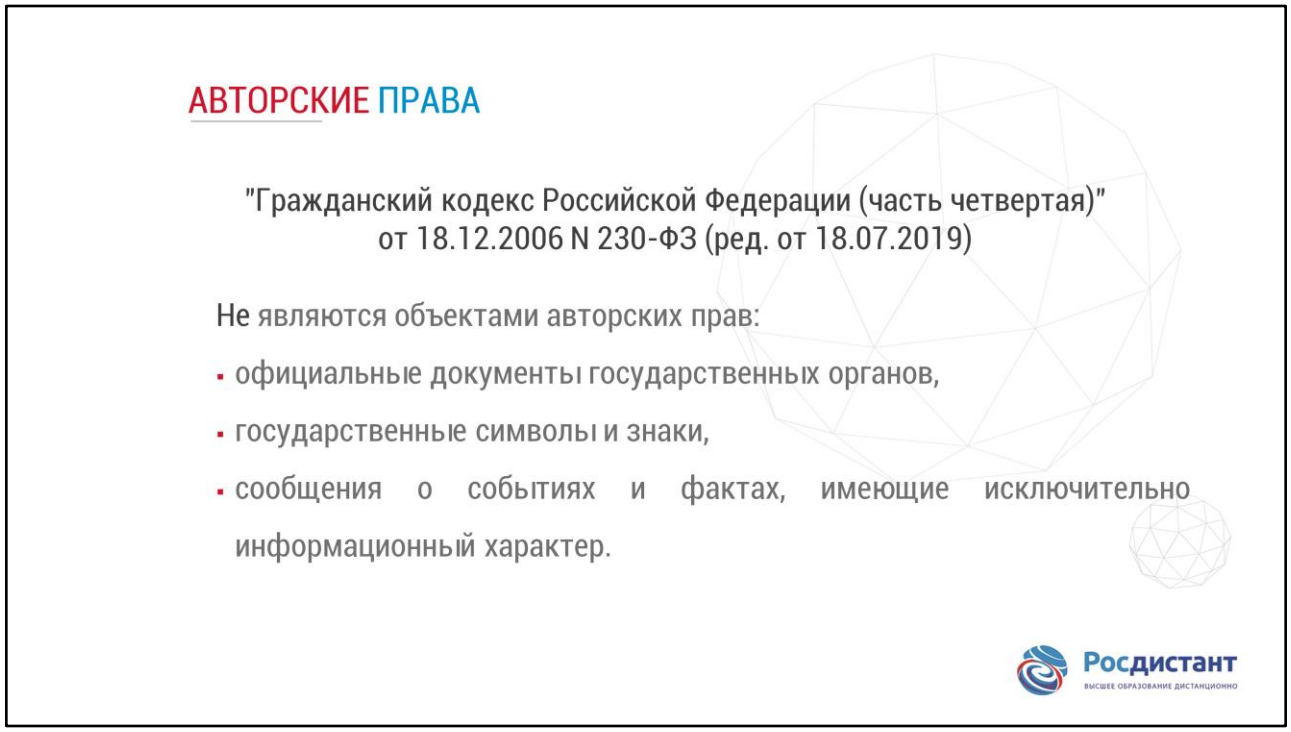
Согласно статье 1259 к объектам авторских прав относятся:

- литературные произведения;
- аудиовизуальные произведения;
- произведения графики;
- дизайна;
- фотографические произведения и произведения, полученные способами, аналогичными фотографии.

А также:

- географические и другие карты;
- планы, эскизы и пластические произведения, относящиеся к географии и к другим наукам и другие произведения.

К объектам авторских прав также относятся программы для электронно-вычислительных машин, которые охраняются как литературные произведения.




**Слайд 51**

Авторские права не распространяются:

- на идеи;
- концепции;
- принципы;
- методы.

А также:

- на процессы;
- системы;
- способы;
- решения технических, организационных или иных задач.

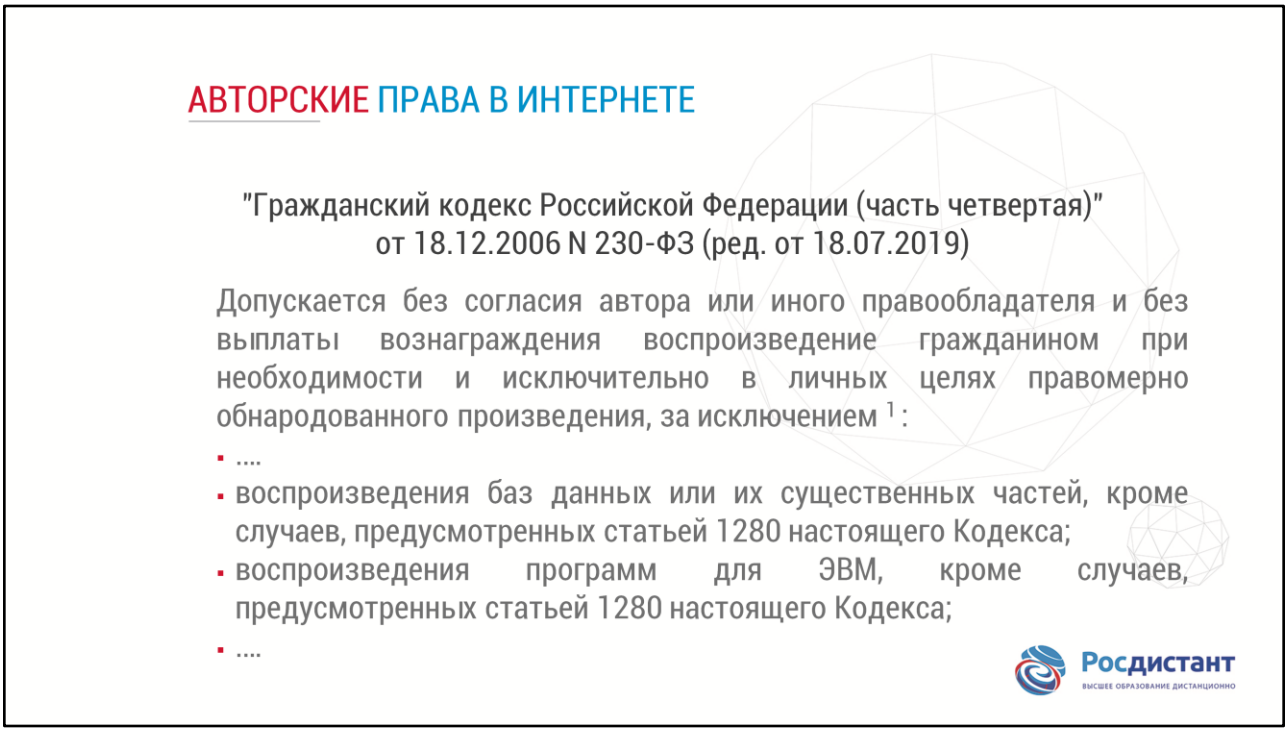
Кроме того:

- на открытия;
- факты;
- языки программирования;
- геологическую информацию о недрах.

К объектам авторских прав не относятся:

- официальные документы государственных органов и органов местного самоуправления муниципальных образований. В том числе законы, другие нормативные акты, судебные решения, иные материалы законодательного, административного и судебного характера, официальные документы международных организаций, а также их официальные переводы;

- государственные символы и знаки – флаги, гербы, ордена, денежные знаки и тому подобное. А также символы и знаки муниципальных образований;
- произведения народного творчества, не имеющие конкретных авторов;
- сообщения о событиях и фактах, имеющие исключительно информационный характер. Например, сообщения о новостях дня, программы телепередач, расписания движения транспортных средств и тому подобное.



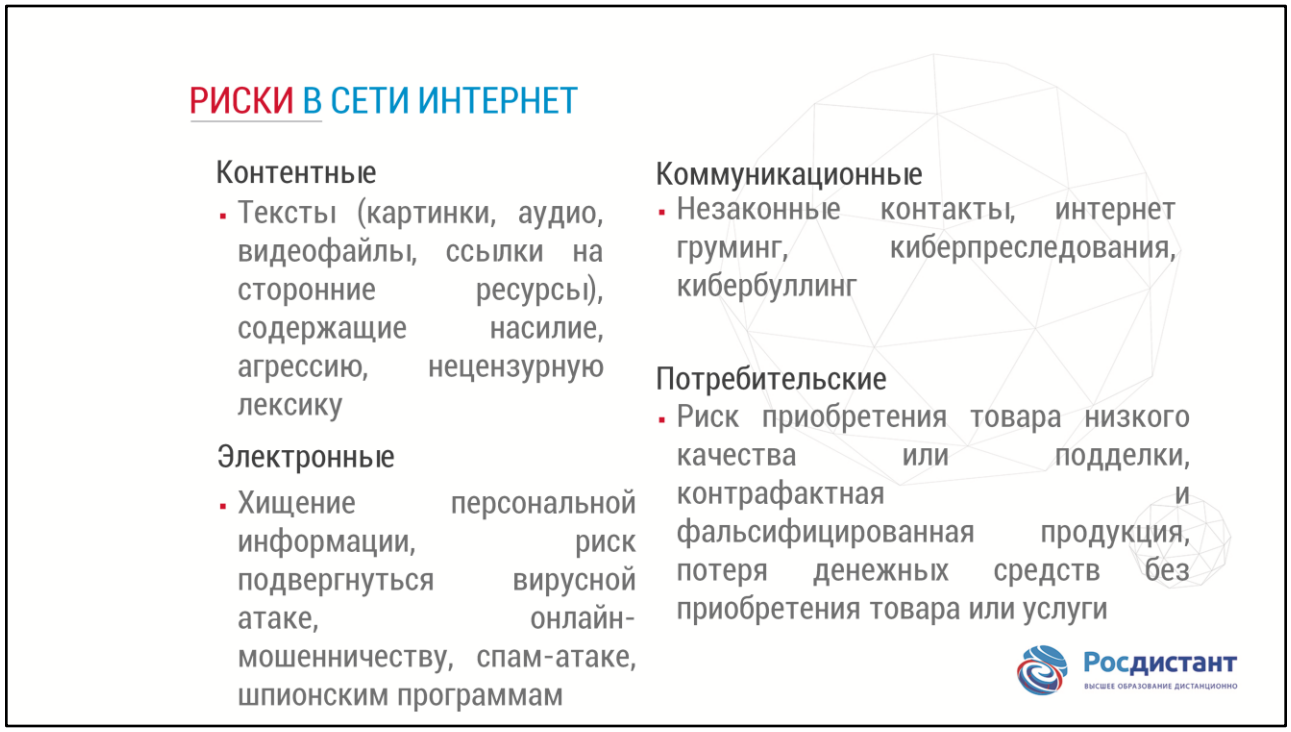

**Слайд 52**

Ежедневно в Интернете мы просматриваем новости, общаемся в социальных сетях, переписываемся, работаем, ищем необходимую информацию. Практически у каждого пользователя интернета есть аккаунты в социальных сетях, интернет-сообществах, форумах, блогах и так далее. Активные интернет-пользователи выкладывают фотографии, картинки, видео, статьи, аудио файлы, научные работы – контент собственного производства. Но мы редко задумываемся о том, что на контент в Интернете распространяется действие общих правил авторского права.

Для возникновения авторских прав не требуется официальной регистрации произведения. Важно лишь, чтобы оно было обнародовано.

Что же можно делать без согласия автора, а чего нельзя?

Согласно статье 1273 Гражданского кодекса допускается без согласия автора или иного правообладателя и без выплаты гонорара воспроизведение гражданином обнародованного произведения исключительно в личных целях, для себя. Воспроизведением считается изготовление одного или нескольких экземпляров произведения или его части в любой материальной форме.




**Слайд 53**

Риски, с которыми сталкивается пользователь Интернета, многообразны. Их несет на себе разнообразная информация, размещаемая в Сети. В ряду актуальных для сегодняшней интернет-среды рисков, связанных с использованием интернета, специалисты выделяют следующие.

Контентные риски.

Контентные риски связаны с материалами, содержащими:

- насилие;
- агрессию;
- порнографию;
- нецензурную лексику.

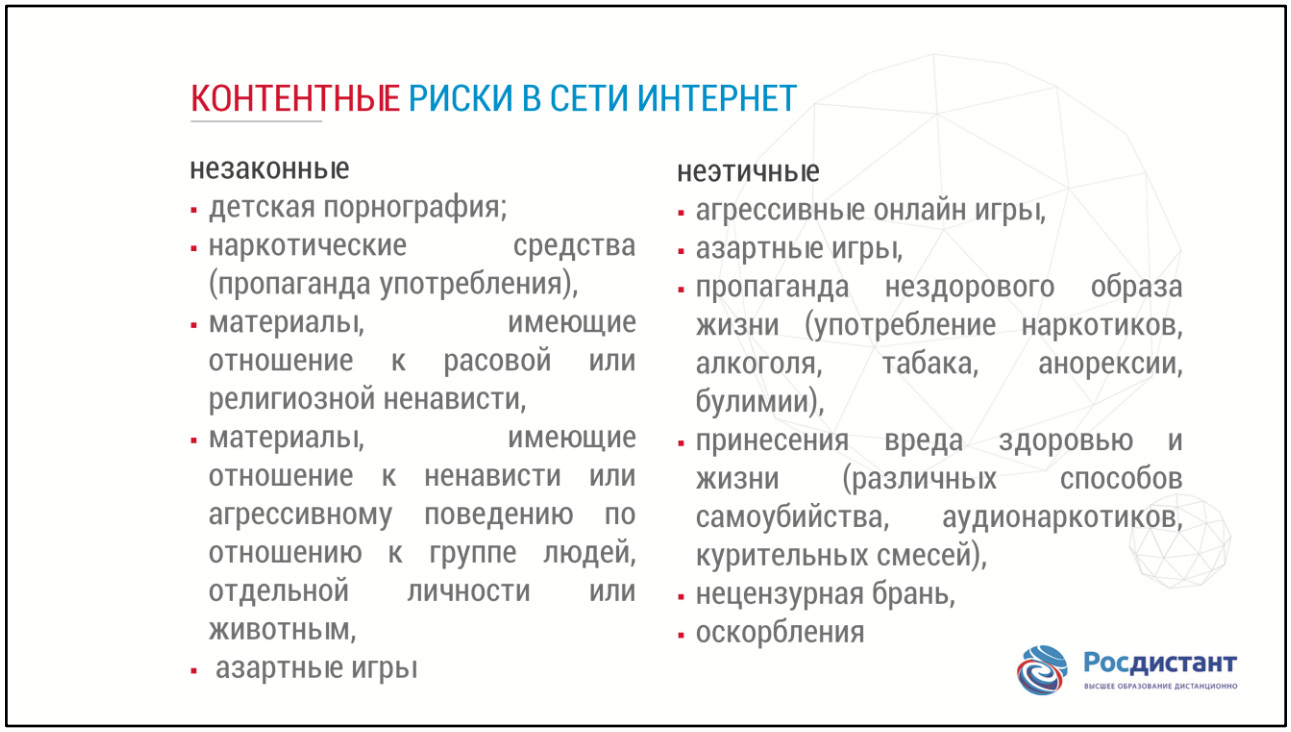
А также:

- информацию, разжигающую расовую ненависть;
- пропаганду анорексии и булимии;
- суицида;
- азартных игр;
- наркотических веществ.

Коммуникационные риски.

Коммуникационные риски связаны с межличностными отношениями интернет-пользователей и включают в себя риск подвергнуться оскорблениям и нападкам со стороны других. Для подобных целей используются различные чаты, онлайн-мессенджеры, социальные сети, сайты знакомств, форумы, блоги и так далее.

Электронные или киберриски.
Вредоносное программное обеспечение использует множество методов для распространения и проникновения в компьютеры через электронную почту посредством спама или скачанных из Интернета файлов. Также взлом страниц в социальных сетях превратился в один из основных способов распространения спама в Интернете.
Потребительские риски.
Потребительские риски связаны со злоупотреблением в интернете правами потребителя.
Интернет-зависимость. Это навязчивое желание войти в Интернет и невозможность выйти из Интернета, а также патологическая непреодолимая тяга к Интернету, оказывающая пагубное воздействие на бытовую, учебную, социальную, семейную или психологическую сферы деятельности.



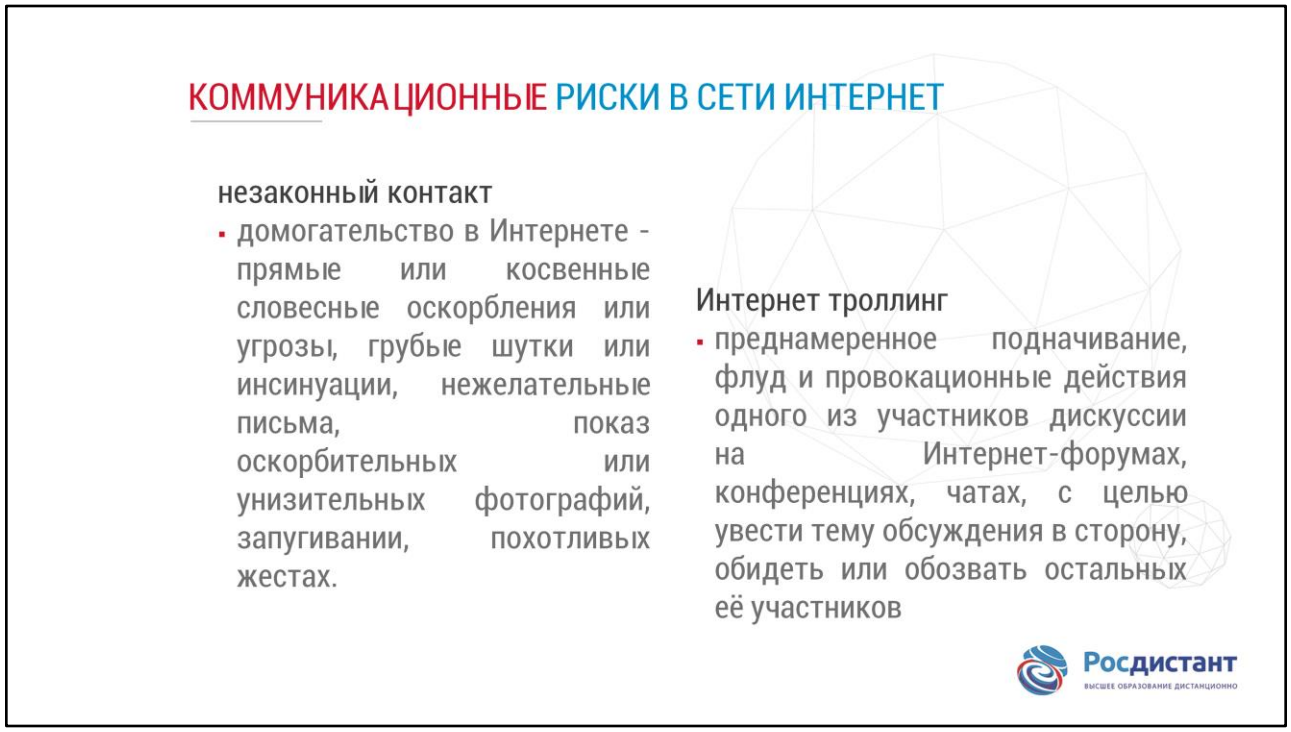

**Слайд 54**

Сегодня мы можем наблюдать, с какой бешеной скоростью идет развитие Интернета. Ежесекундно на просторах Интернета появляется новая информация – статьи, видеоролики, фильмы, реклама и так далее. И весь этот материал называется контент.

Негативный контент условно можно разделить на незаконный и неэтичный. Неэтичный контент противоречит принятым в обществе нормам морали и социальным нормам. Неэтичные материалы не попадают под действие Уголовного Кодекса, однако они могут оказывать негативное влияние на психику человека, особенно ребенка.

Информация, относящаяся к категории неэтичной, может быть также направлена на манипулирование сознанием и действиями различных групп людей.

Внутреннее законодательство каждой страны предусматривает различные виды наказания за распространение такой информации. В Российском законодательстве есть возможность привлечь к административной и уголовной ответственности за распространение подобного негативного контента владельцев сайтов, а также авторов таких электронных текстов и видеопродукции.




**Слайд 55**

Столкнуться с коммуникационными рисками можно в чатах, онлайн-мессенджерах, социальных сетях, сайтах знакомств, форумах, блогов и так далее.

Даже если большинство пользователей обладает добрыми намерениями, существует, к сожалению, растущее число людей, использующих эти беседы со злым умыслом. Оказаться жертвой намного проще, чем кажется. Каждый участник той или иной социальной сети может признаться, что хотя бы один раз ему приходило непристойное предложение от неизвестного человека.

Коммуникационные риски включают в себя незаконный контакт и киберпреследование или кибербуллинг.

Незаконный контакт включает в себя такие интернет-преступления, как домогательство и интернет-гру́минг.

Домогательство – причиняющее неудобство или вред поведение, нарушающее неприкосновенность частной жизни лица.

Интернет-гру́минг – установление дружеских отношений взрослого с ребенком с целью совращения. Злоумышленник нередко общается в интернете с ребенком, выдавая себя за ровесника либо немного старше. Он знакомится в чате, на форуме или в социальной сети с жертвой, пытается установить с ним дружеские отношения и перейти на личную переписку. Общаясь лично, то есть в прива́те, он входит в доверие к ребенку, пытается узнать номер мобильного телефона и договориться о встрече.

Хе́йтинг – проявление оскорбительного отношения, ненависти к другому человеку.
Кибербу́ллинг – агрессивное, умышленное действие, совершаемое группой лиц или одним лицом с использованием электронных форм контакта, повторяющееся неоднократно и продолжительное во времени, в отношении жертвы.
Киберпреследование может принимать такие формы, как обмен информацией, контактами; запугивание; подражание; интернет-троллинг; социальное бойкотирование. По форме кибербуллинг может быть не только словесным оскорблением. Это могут быть фотографии, изображения или видео жертвы, отредактированные так, чтобы быть более унизительными.