МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное
учреждение высшего образования
«Уральский государственный лесотехнический университет»
(УГЛТУ)

И. В. Щепеткина
А. В. Андреев
Е. Н. Щепеткин

ПРАВОВОЕ РЕГУЛИРОВАНИЕ В ИНФОРМАЦИОННОЙ СФЕРЕ

Учебное пособие

Екатеринбург
УГЛТУ
2025

УДК 005.95/.96(075.8)
ББК 65.291.6-21я73
Щ56

Рецензенты:

кафедра конституционного права Федерального государственного бюджетного учреждения высшего образования «Уральский государственный юридический университет», доц., канд. юридически наук *А. В. Сивопляс*;

В. И. Овсянников, директор Автономной некоммерческой профессиональной образовательной организации «Уральский промышленно-экономический техникум»

Щепеткина, Инна Вадимовна.

Щ56 Правовое регулирование в информационной сфере : учебное пособие / И. В. Щепеткина, А. В. Андреев, Е. Н. Щепеткин ; Министерство науки и высшего образования Российской Федерации, Уральский государственный лесотехнический университет. – Екатеринбург : УГЛТУ, 2025. – 174 с.

ISBN 978-5-94984-948-4

Целью учебного пособия является формирование у обучающихся знаний, умений и компетенций в области правового регулирования в информационной сфере. Авторами рассматривается правовое регулирование основных правовых институтов информационного права. В частности, раскрываются понятие и виды информации, правовые режимы общедоступной информации и информации ограниченного доступа, анализируется право на доступ к информации о деятельности органов государственной власти и органов местного самоуправления, раскрывается правовое регулирование электронного документооборота, создания и эксплуатации информационных систем и т. д.

Пособие окажет студентам помощь в выборе и выполнении различных видов самостоятельной учебной и научно-исследовательской работы.

Предназначено для обучающихся всех направлений подготовки, изучающих дисциплины «Правовые основы защиты информации», «Правовое регулирование в информационной сфере», «Информационное право» и др.

Издается по решению редакционно-издательского совета Уральского государственного лесотехнического университета.

УДК 005.95/.96(075.8)
ББК 65.291.6-21я73

ISBN 978-5-94984-948-4

ОГЛАВЛЕНИЕ

ИНФОРМАЦИЯ: ПОНЯТИЕ, ВИДЫ, ПОЛУЧЕНИЕ И РАСПРОСТРАНЕНИЕ

Информация является важнейшей составляющей нашей повседневной жизни, это сырье, которое помогает нам принимать решения, учиться и развиваться, а также общаться друг с другом. По сути, информация – это строительный материал знаний, и без нее нам было бы трудно понимать окружающий мир.

Информация существует в различных формах, включая письменный текст, изображения, видео и аудиозаписи. К ней можно получить доступ по разным каналам, таким как книги, Интернет и социальные сети.

Развитие цифровых технологий произвело революцию в том, как мы производим, потребляем и распространяем информацию, сделав доступ к огромным объемам данных из любой точки мира проще, чем когда-либо.

Важность информации выходит далеко за рамки нашей личной жизни. Это важнейший ресурс для бизнеса, правительств и организаций, помогающий им принимать обоснованные решения и оставаться конкурентоспособными в быстро меняющемся мире. Информация играет ключевую роль в обеспечении прогресса и инноваций во всех сферах жизни общества, от научных исследований до финансового анализа.

По мере того, как мы продолжаем разбираться в сложностях цифровой эпохи, понимание природы и силы информации как никогда важно. Используя ее потенциал и применяя его с умом, мы можем открыть для себя новые возможности и решить некоторые из самых насущных мировых проблем.

Информация – это совокупность данных, которые были обработаны, систематизированы или структурированы для передачи знаний, идей или инструкций. Она может передаваться с помощью различных средств: книги, веб-сайты и социальные сети.

По сути, ***информация*** – это отражение реальности, она используется для передачи знаний об окружающем нас мире. Она может быть фактической, субъективной или даже вымышленной и принимать различные формы в зависимости от цели и аудитории.

Качество и достоверность информации могут существенно повлиять на индивидуальные и коллективные результаты, поэтому крайне важно критически оценивать и проверять источники и надежность информации, которую мы потребляем.

Ценность информации заключается в ее способности помогать нам принимать обоснованные решения, решать проблемы и эффективно общаться с другими людьми. Это важнейший ресурс для отдельных людей, организаций и общества в целом, который играет жизненно важную роль в развитии и внедрении инноваций во всех сферах человеческой деятельности.

По мере развития технологий объем доступной нам информации растет в геометрической прогрессии. Это создает новые проблемы, связанные с доступом к информации, ее обработкой и эффективным использованием. Однако с помощью правильных инструментов и стратегий мы можем использовать силу информации для позитивных изменений и достижения наших целей.

Информация бывает разных видов.

Дэвид Б. Герц и Альберт Б. Рубенштейн выделили шесть типов информации: концептуальную, процедурную, стимулирующую, политическую, эмпирическую, описательную.

1. ***Концептуальная информация*** – это информация, связанная с абстрактными или теоретическими идеями, концепциями или принципами. Она часто используется в академическом или философском контексте для обсуждения более широких идей или концепций, не связанных с конкретными примерами или случаями.

Примерами концептуальной информации могут служить теории психологии, философские (справедливость или мораль) или математические концепции (исчисление или теория вероятностей).

Концептуальная информация часто используется для создания основы или фундамента для понимания более конкретной информации. Ее также можно использовать для объяснения сложных идей или для установления связей между, казалось бы, не связанными между собой темами.

2. ***Эмпирическая информация*** – это данные, полученные в результате наблюдений, экспериментов или непосредственного опыта. Она основана на данных, которые можно измерить или проверить с помощью объективных и систематических методов.

Эмпирическая информация часто используется в научных исследованиях, она собирается с помощью экспериментов, опросов или других форм сбора данных.

Примерами эмпирической информации могут служить результаты клинических испытаний, данные о последствиях изменения климата или наблюдения за поведением животных.

Эмпирическая информация ценится, потому что она основана на объективных доказательствах и может быть воспроизведена и проверена другими. Она часто используется для принятия решений, а также для подтверждения или опровержения теорий или гипотез.

3. ***Процедурная информация*** – это информация, которая содержит инструкции, указания или шаги по выполнению задачи или завершению процесса. Она часто представлена в виде руководства, инструкции или стандартной операционной процедуры.

Процедурная информация широко используется в производстве, здравоохранении и транспортной отрасли, где точные и последовательные процедуры имеют решающее значение для обеспечения безопасности, качества и эффективности.

Примерами процедурной информации могут быть инструкции по эксплуатации оборудования, рекомендации по введению лекарств или пошаговое руководство по проведению медицинской процедуры.

Процедурная информация должна быть понятной, краткой и простой для восприятия. Она может включать наглядные пособия (схемы или иллюстрации), которые помогают прояснить последовательность действий.

4. ***Стимулирующая информация*** – это информация, предназначенная для того, чтобы вызвать ответную реакцию аудитории. Этот тип информации часто используется в рекламных, маркетинговых или PR-кампаниях, цель которых – привлечь внимание аудитории и побудить ее к действию.

Стимулирующая информация может быть направлена на то, чтобы вызвать определенную эмоцию, например волнение, страх или любопытство, или на то, чтобы бросить вызов аудитории или вдохновить ее на нестандартное мышление.

Примерами стимулирующей информации могут служить провокационная реклама, политические кампании, использующие эмоционально заряженные слоганы, или мотивационные речи, вдохновляющие людей на действия.

Стимулирующая информация может влиять на поведение; вызывать споры или разногласия в зависимости от контекста и передаваемого сообщения.

5. ***Политическая информация*** – это информация, относящаяся к государственной политике, законам, постановлениям и рекомендациям, которые влияют на отдельных людей, организации и общество в целом. Она включает в себя информацию о целях политики, процессах, результатах, реализации политики и данные об оценке.

Политическая информация часто используется для принятия решений и мониторинга эффективности политики с течением времени.

Примерами политической информации могут служить отчеты о влиянии экологических норм, данные об эффективности мер по охране здоровья населения или анализ экономических последствий налоговой политики.

Информация о политике необходима для обеспечения прозрачности и подотчетности при принятии государственных решений, а также для содействия участию общественности и ее влиянию на процессы разработки политики. Она часто распространяется через официальные правительственные веб-сайты, общедоступные документы и СМИ.

6. ***Описательная информация*** относится к информации, которая подробно описывает конкретный объект, человека, событие или ситуацию. Это может включать внешний вид, размер, форму, цвет, текстуру или поведение. Описательная информация часто используется для создания мысленного образа или картины чего-либо, или для обеспечения полного понимания конкретной темы или концепции.

Примеры описательной информации могут включать описания продуктов в электронной коммерции, свидетельства очевидцев преступления или несчастного случая, или подробные отчеты об исторических событиях или культурных феноменах.

Описательная информация облегчает общение и взаимопонимание между людьми и группами, а также предоставляет контекстную и справочную информацию в различных областях, таких как литература, искусство и наука.

Также выделяют информацию о прошлом.

Информация о прошлом – это сведения о событиях, ситуациях или обстоятельствах, которые произошли в прошлом. К ней относятся исторические записи, архивы и артефакты, документирующие прошлое, а также личные воспоминания, предания и устные истории.

Информация о прошлом важна, потому что она дает нам ощущение непрерывности и помогает понять, как прошлое повлияло на настоящее. Она также позволяет учиться на прошлых ошибках, выявлять закономерности и тенденции и принимать обоснованные решения о будущем. Примерами информации из прошлого могут служить исторические документы, археологические артефакты, фотографии, фильмы и личные воспоминания. Информация из прошлого может использоваться в различных областях науки (история, социология, антропология и психология) для получения представлений о человеческом поведении, культурных практиках и социальных тенденциях в динамике.

Преимущества информации:

знания: с помощью информации мы можем узнавать новое, расширять свое понимание и приобретать опыт в различных областях;

принятие решений: имеет решающее значение для принятия обоснованных решений. Помогает оценивать варианты, риски и преимущества и выбирать наилучший вариант действий;

инновации: ключевой фактор инноваций. Вдохновляет на новые идеи, позволяет находить новые возможности и способствует разработке новых продуктов, услуг и технологий;

сотрудничество: способствует сотрудничеству и взаимодействию отдельных людей и групп. Помогает обмениваться идеями, координировать усилия и работать сообща для достижения общих целей;

расширение возможностей: расширяет возможности людей, предоставляя им доступ к знаниям, ресурсам и возможностям. Позволяет контролировать свою жизнь, делать осознанный выбор и достигать своих целей и стремлений;

экономический рост: является важнейшим фактором экономического роста и развития. Помогает выявлять рыночные возможности, оптимизировать производственные процессы и создавать новые товары и услуги, отвечающие потребностям потребителей;

личностное развитие: способствует личностному развитию, предоставляя новые перспективы, идеи и мысли. Помогает развивать навыки критического мышления, расширять мировоззрение и повышать креативность и способность решать проблемы.

Наш век называют информационным. Информация – это уникальный капитал, который приумножается, если делиться им с другими.

В свободном демократическом обществе человек имеет практически неограниченный доступ к любой информации.

Информация	– сведения (сообщения, данные) независимо от формы их представления (ст. 2 Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»)

С 1.01.2008 законодатель из ст. 128 Гражданского кодекса Российской Федерации от 30.11.1994 № 51-ФЗ (далее – ГК РФ) вывел информацию из числа объектов гражданских прав, тем не менее оперирует этим термином в ряде статей ГК РФ, свидетельствующих о том, что в этих объектах и отношениях можно выделить информационную составляющую (например, статьи 19, 67, 495, 726, 727,857, 946, 1045 ГК РФ).

Информация – объект 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.

Виды информации в зависимости от категории доступа к ней

Общедоступная информация	– общеизвестные сведения и иная информация, доступ к которой не ограничен
Информация ограниченного доступа (информация доступ к которой ограничен федеральными законами)	– персональные данные; тайна следствия и судопроизводства; служебная тайна; профессиональная тайна; коммерческая тайна; сведения о сущности изобретения

Виды информации в зависимости от порядка ее предоставления или распространения

Законодательством Российской Федерации могут быть установлены виды информации в зависимости от ее содержания или обладателя.

Свойства информации:

– *Достоверность* – степень близости используемой информации к реальному объекту, явлению или процессу;

– *Точность* – это степень соответствия информации текущей ситуации. Поскольку информационные процессы растянуты во времени,

достоверная и адекватная, но устаревшая информация может привести к ошибочным решениям;

– *Полнота информации* – достаточность для принятия решений. Она зависит как от полноты данных, так и от наличия необходимых методов;

– *Стабильность информации* – это способность реагировать на изменения исходных данных без нарушения необходимой точности. Стабильность информации, как и репрезентативность, обусловлена выбранной методикой ее отбора и формирования.

– *Своевременность информации* означает ее доступность заранее, не позднее назначенного момента времени, согласованного со временем решения задачи.

В соответствии со статьей 6 Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», *обладателем информации может быть* гражданин (физическое лицо), юридическое лицо, Российская Федерация, субъект Российской Федерации, муниципальное образование.

От имени Российской Федерации, субъекта Российской Федерации, муниципального образования правомочия обладателя информации осуществляются соответственно государственными органами и органами местного самоуправления в пределах их полномочий, установленных соответствующими нормативными правовыми актами.

Обладатель информации имеет права и обязанности (табл. 1).

Таблица 1

Права и обязанности обладателя информации

Права обладателя информации	Обязанности обладателя информации
Разрешать или ограничивать доступ к информации, определять порядок и условия такого доступа	Соблюдать права и законные интересы иных лиц
Использовать информацию, в том числе распространять ее по своему усмотрению	Принимать меры по защите информации
Передавать информацию другим лицам по договору или на ином установленном законом основании	Ограничивать доступ к информации, если такая обязанность установлена федеральными законами

Окончание табл. 1

Права обладателя информации	Обязанности обладателя информации
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	–

Граждане (физические лица) и организации (юридические лица) вправе осуществлять поиск и получение любой информации в любых формах и из любых источников при условии соблюдения требований, установленных Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» и другими федеральными законами.

Гражданин (физическое лицо) имеет право на получение от государственных органов, органов местного самоуправления, их должностных лиц в порядке, установленном законодательством Российской Федерации, информации, непосредственно затрагивающей его права и свободы.

Организация имеет право на получение от государственных органов, органов местного самоуправления информации, непосредственно касающейся прав и обязанностей этой организации, а также информации, необходимой в связи с взаимодействием с указанными органами при осуществлении этой организацией своей уставной деятельности.

Информация, к которой не может быть ограничен доступ

- Нормативные правовые акты, затрагивающие права, свободы и обязанности человека и гражданина, а также устанавливающие правовое положение организаций и полномочия государственных органов, органов местного самоуправления
- Информация о состоянии окружающей среды (экологическая информация)
- Информация о деятельности государственных органов и органов местного самоуправления, а также об использовании бюджетных средств (за исключением сведений, составляющих государственную или служебную тайну)
- Информация, накапливаемая 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
- Информация, содержащаяся в архивных документах архивных фондов (за исключением сведений и документов, доступ к которым ограничен законодательством Российской Федерации)
- Иная информация, недопустимость ограничения доступа к которой установлена федеральными законами.

Государственные органы и органы местного самоуправления обязаны обеспечивать доступ, в том числе с использованием информационно-телекоммуникационных сетей, в том числе сети «Интернет», к информации о своей деятельности на русском языке и государственном языке соответствующей республики в составе Российской Федерации в соответствии с федеральными законами, законами субъектов Российской Федерации и нормативными правовыми актами органов местного самоуправления. Лицо, желающее получить доступ к такой информации, не обязано обосновывать необходимость ее получения.

Решения и действия (бездействие) государственных органов и органов местного самоуправления, общественных объединений, должностных лиц, нарушающие право на доступ к информации, могут быть обжалованы в вышестоящий орган или вышестоящему должностному лицу либо в суд.

В случае, если в результате неправомерного отказа в доступе к информации, несвоевременного ее предоставления, предоставления заведомо недостоверной или не соответствующей содержанию запроса информации были причинены убытки, такие убытки подлежат возмещению в соответствии с гражданским законодательством.

Предоставляется бесплатно информация:

– о деятельности государственных органов и органов местного самоуправления, размещенная такими органами в информационно-телекоммуникационных сетях;

– затрагивающая права и установленные законодательством Российской Федерации обязанности заинтересованного лица;

– иная установленная законом информация.

Установление платы за предоставление государственным органом или органом местного самоуправления информации о своей деятельности возможно только в случаях и на условиях, которые установлены федеральными законами.

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, размещаемой в форме открытых данных.

Информация в форме открытых данных размещается в сети «Интернет» с учетом требований законодательства Российской Федерации о государственной тайне. В случае, если размещение информации в форме открытых данных может привести к распространению сведений, составляющих государственную тайну, размещение указанной информации в форме открытых данных должно быть прекращено по требованию органа, наделенного полномочиями по распоряжению такими сведениями.

В случае, если размещение информации в форме открытых данных может повлечь за собой нарушение прав обладателей информации, доступ к которой ограничен в соответствии с федеральными законами, или нарушение прав субъектов персональных данных, размещение

указанной информации в форме открытых данных должно быть прекращено по решению суда.

В случае, если размещение информации в форме открытых данных осуществляется с нарушением требований Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», размещение информации в форме открытых данных должно быть приостановлено или прекращено по требованию уполномоченного органа по защите прав субъектов персональных данных.

В Российской Федерации распространение информации осуществляется свободно при соблюдении требований, установленных законодательством Российской Федерации.

Информация, распространяемая без использования средств массовой информации, должна включать в себя достоверные сведения о ее обладателе или об ином лице, распространяющем информацию, в форме и в объеме, которые достаточны для идентификации такого лица.

Владелец сайта в сети «Интернет» обязан разместить на принадлежащем ему сайте информацию о своих наименовании, месте нахождения и адресе, адресе электронной почты для направления заявления, указанного в ст. 15.7 Федерального закона «Об информации, информационных технологиях и о защите информации», а также вправе предусмотреть возможность направления этого заявления посредством заполнения электронной формы на сайте в сети «Интернет».

При использовании для распространения информации средств, позволяющих определять получателей информации, в том числе почтовых отправлений и электронных сообщений, лицо, распространяющее информацию, обязано обеспечить получателю информации возможность отказа от такой информации. Предоставление информации осуществляется в порядке, который устанавливается соглашением лиц, участвующих в обмене информацией.

Случаи и условия обязательного распространения информации или предоставления информации, в том числе предоставление обязательных экземпляров документов, устанавливаются федеральными законами.

Запрещается распространение информации, которая направлена на пропаганду войны, разжигание национальной, расовой или религиозной ненависти и вражды, а также иной информации, за распространение которой предусмотрена уголовная или административная ответственность.

Запрещается распространение материалов, производимых и (или) распространяемых иностранным агентом в связи с осуществлением им вида деятельности, установленного ст. 4 Федерального закона от 14.07.2022 № 255-ФЗ «О контроле за деятельностью лиц, находящихся под иностранным влиянием», а также информации, касающейся вида деятельности, установленного ст. 4 Федерального закона от 14.07.2022 № 255-ФЗ «О контроле за деятельностью лиц, находящихся под иностранным влиянием», без указания на то, что эти материалы (информация) произведены и (или) распространены иностранным агентом.

ИНФОРМАЦИОННОЕ ОБЩЕСТВО И ЦИФРОВАЯ ТРАНСФОРМАЦИЯ

В последнее время цифровая трансформация является горячей темой. Наша зависимость от экранного времени, наш ненасытный аппетит к новым гаджетам и устройствам, наши пугающе быстрые темпы внедрения новых цифровых инструментов рано или поздно имеют тенденцию распространяться по всему миру.

Изменение, получившее название «цифровая трансформация», является результатом стратегии, направленной на перевод политических, экономических, бизнес-процессов в цифровую сферу. Это означает внедрение цифровых инструментов, приложений и рабочих процессов для повышения эффективности, результативности и снижения частоты ошибок при выполнении различных функций.

Несмотря на эти успехи, цифровая трансформация, пожалуй, является самым трудным решением, которое приходится принимать органам управления в той или иной сфере.

Многие компании не готовы к сбоям из-за устаревшей системы мышления, разрозненных организационных структур и неспособности учитывать общую ситуацию.

Неудивительно, что цифровая трансформация – это деятельность, которая сталкивается с определенной долей организационного сопротивления. Чтобы преодолеть это сопротивление, обычно требуется план, процесс, который обычно сопровождается внешней помощью.

Полезно рассматривать цифровую трансформацию как технологический и культурный сдвиг, который распространяется на все сферы деловой активности. Вступление на путь цифровой трансформации – это не спринт, а марафон, основанный на постоянно меняющемся контексте тенденций клиентов, рабочего места и рынка в данной отрасли.

Информационно-коммуникационные технологии являются основой стратегического развития в современном мире.

В целях укрепления технологического суверенитета в Российской Федерации уделяется повышенное внимание реализации комплекса мер поддержки российского сектора информационно-коммуникационных технологий и его основных сегментов, медиаотрасли.

Продолжается работа по дальнейшему динамичному развитию инфраструктуры связи и телекоммуникаций, информационной безопасности, импортозамещению, развитию сфер искусственного

интеллекта, цифрового государственного управления и перевода государственных и муниципальных услуг в электронный вид, а также по кадровому обеспечению отрасли информационных технологий.

Постановлением Правительства РФ от 15.04.2014 № 313 утверждена государственная программа Российской Федерации «Информационное общество».

Развитие и модернизация современной инфраструктуры создают условия для обеспечения доступности услуг электросвязи для всех слоев населения на территории Российской Федерации.

Развитие информационно-телекоммуникационной инфраструктуры позволяет расширять возможности использования средств электросвязи, радиочастотного спектра для повышения эффективности государственного управления, нужд обороноспособности и безопасности государства и обеспечения правопорядка.

В течение последних лет ключевые показатели отрасли информационных технологий в Российской Федерации поступательно увеличиваются. Продолжается внедрение информационных технологий в социально-экономическую сферу, государственное управление и бизнес, что оказывает влияние на рост производительности труда и качество жизни населения, повышается эффективность технологических, производственных и управленческих процессов любой отрасли экономики и уровень обороноспособности страны.

Масштабное распространение информационных технологий наблюдается в здравоохранении, образовании, науке, культуре, обеспечении безопасности, промышленности, сельском хозяйстве, финансовой сфере и на транспорте.

Одними из ключевых факторов развития информационного общества в Российской Федерации являются доступность и качество контента в современном информационном пространстве.

С целью обеспечения доступного и качественного контента в информационном пространстве в настоящее время Министерством цифрового развития, связи и массовых коммуникаций Российской Федерации реализуется ряд приоритетных задач в медиаотрасли (телерадиовещание, печатные СМИ, книгоиздание и сеть «Интернет»).

Указами Президента Российской Федерации от 7.05.2018 № 204 «О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года», от 21.07.2020 № 474 «О национальных целях развития Российской Федерации на период до 2030 года», от 2.07.2021 г. № 400 «О Стратегии национальной безопасности Российской Федерации», от 5.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации»

и с учетом положений иных документов стратегического планирования определены *приоритеты государственной программы «Информационное общество»*.

Приоритеты государственной программы «Информационное общество»

- Повышение благосостояния, качества жизни и работы граждан
- Улучшение доступности и качества государственных услуг
- Повышение степени информированности и цифровой грамотности
- Развитие экономического потенциала страны с использованием современных информационных, телекоммуникационных и цифровых технологий
- Обеспечение свободы выбора средств получения знаний при работе с информацией
- Обеспечение прав граждан на доступ к информации
- Сохранение традиционных и привычных для граждан (отличных от цифровых) форм получения товаров и услуг
- Приоритет традиционных российских духовно-нравственных ценностей и соблюдение основанных на этих ценностях норм поведения при использовании информационных и коммуникационных технологий
- Защита личности, общества и государства от внутренних и внешних информационных угроз
- Обеспечение государственной защиты интересов российских граждан в информационной сфере

Национальными целями развития Российской Федерации на период до 2030 г., установленными Указом Президента Российской Федерации от 21.07.2020 № 474 «О национальных целях развития Российской Федерации на период до 2030 года», *определяющими приоритеты государственной политики, вклад в реализацию которых вносят*

мероприятия государственной программы «Информационное общество», являются:

– цифровая трансформация;

– возможности для самореализации и развития талантов;

– сохранение населения, здоровье и благополучие людей;

– достойный, эффективный труд и успешное предпринимательство.

С учетом положений стратегических документов определены следующие ***цели государственной программы «Информационное общество»:***

– повышение уровня «цифровой зрелости» ключевых отраслей экономики и социальной сферы, в том числе здравоохранения и образования, а также государственного управления (достижение указанной цели обеспечивается путем увеличения численности специалистов, интенсивно использующих информационно-коммуникационные технологии, расходов организаций на внедрение и использование современных цифровых решений);

– увеличение доли массовых социально значимых услуг, доступных в электронном виде (достижение данной цели обеспечивается путем повышения удовлетворенности граждан при получении услуг в электронном виде и упрощения процедуры их получения, цифровизации деятельности органов власти);

– рост доли домохозяйств, которым обеспечена возможность широкополосного доступа к сети «Интернет» (достижение данной цели способствует обеспечению жителей равными возможностями доступа в сети «Интернет»: к электронным государственным услугам; к качественному контенту в сфере образования и культуры; к удаленной занятости; к увеличению вложений в отечественные решения в сфере информационных технологий);

– повышение доступности финансирования для стартапов, разрабатывающих решения в сфере информационных технологий, реализация программ высшего, среднего и дополнительного профессионального образования по наиболее востребованным или ранее отсутствовавшим направлениям и специальностям в сфере информационных технологий, что позволит удовлетворить растущие потребности рынка в специалистах такого профиля;

– получение доступного и качественного контента в условиях развития информационного пространства (достижение указанной цели обеспечивается путем формирования информационного пространства с учетом потребностей граждан и общества).

Для эффективного достижения национальной цели развития Российской Федерации на период до 2030 г. «Цифровая трансформация» распоряжением Правительства Российской Федерации от 6.10.2021 № 2816-р утвержден перечень инициатив социально-экономического развития Российской Федерации до 2030 г. ***Такими инициативами являются:***

– доступ к сети «Интернет»;
– цифровой профиль гражданина;
– госуслуги онлайн;
– электронный документооборот;
– подготовка кадров для ИТ.

В этой связи в состав государственной программы «Информационное общество» включены ***мероприятия, направленные на достижение следующих целей:***

– дополнительное развитие и модернизация всей телекоммуникационной инфраструктуры Российской Федерации с целью создания равных возможностей для доступа к цифровым технологиям всем жителям Российской Федерации, в том числе посредством создания спутниковой группировки быстрого доступа в сеть «Интернет»;

– повышение скорости обслуживания граждан и создание комфортных условий для бизнеса при оказании государственных, муниципальных и иных услуг, а также цифровая трансформация услуг и взаимоотношений в обществе;

– повышение качества и удобства предоставляемых органами государственной власти государственных услуг, а также расширение количества государственных услуг, которые граждане и организации смогут получить в электронном виде;

– создание возможности для перехода на цифровое взаимодействие граждан, бизнеса и государства;

– поддержание баланса спроса и предложения на рынке труда в ИТ-отрасли.

В рамках государственной программы «Информационное общество» для достижения национальной цели «Цифровая трансформация» поставлены следующие задачи:

– достижение «цифровой зрелости»;
– увеличение доли массовых социально значимых услуг, доступных в электронном виде;
– обеспечение роста доли домохозяйств, которым обеспечена возможность широкополосного доступа к сети «Интернет»;

– обеспечение увеличения вложений в отечественные решения в сфере информационных технологий.

Приоритеты государственной политики субъектов Российской Федерации в сфере реализации государственной программы «Информационное общество»

- Содействие расширению доступа населения к медиасреде и поддержка развития региональных средств массовой информации
- Поддержка развития и координации цифровизации субъектов РФ
- Развитие сервисов электронного правительства, переход к оказанию государственных (муниципальных) услуг (функций), иных услуг (сервисов) и сведений в электронном виде, расширение использования информационно-телекоммуникационных технологий для предоставления государственных и муниципальных услуг бюджетными учреждениями, а также социально значимых услуг государственными и муниципальными предприятиями
- Снижение барьеров, формирование условий и стимулирование развития инфраструктуры связи в субъектах РФ
- Создание условий для развития отрасли информационных технологий, включая поддержку цифровой трансформации важнейших отраслей экономики
- Развитие среднего профессионального образования в сфере информационных технологий
- Создание и обеспечение функционирования в субъектах РФ центров управления регионов

Для достижения иных национальных целей Программой поставлены следующие задачи:

– возможности для самореализации и развития талантов – развитие социально значимых проектов в медиасреде, в том числе в печатных и электронных средствах массовой информации;

– сохранение населения, здоровье и благополучие людей – стимулирование занятий граждан физической культурой и спортом путем создания цифровых платформ и приложений, стимулирующих заниматься физической культурой и спортом и агрегирующих данные

о двигательной активности населения, в том числе единой цифровой платформы «Физическая культура и спорт»;

– достойный, эффективный труд и успешное предпринимательство – внедрение цифровых технологий и платформенных решений в сферах государственного управления и оказания государственных услуг, в том числе в интересах населения, субъектов малого и среднего предпринимательства, включая индивидуальных предпринимателей.

В бизнес-среде выделяют следующие преимущества цифровой трансформации:

– ***улучшение качества обслуживания клиентов***. Технологический прогресс изменил ожидания потребителей в отношении брендов. Теперь компании могут предлагать последовательный опыт, строить долгосрочные отношения и повышать лояльность своих клиентов. Цифровая трансформация позволяет компаниям выделяться среди конкурентов;

– ***создание лучшей рабочей среды.*** Помимо клиентов, сотрудники также осведомлены о новых технологиях. Переход на цифровизацию – это не только повышение производительности и эффективности труда, но и творческое решение проблем компании. Когда сотрудники мотивированы и выбирают новые пути, они находятся в состоянии постоянного обучения;

– ***конкурентоспособность.*** Быть в авангарде цифровых тенденций позволяет быстрее реагировать на изменения на рынке, что дает преимущество компании в той отрасли, в которой она работает;

– ***повышение прибыльности бизнеса.*** По мере того, как улучшается качество обслуживания клиентов, повышается лояльность и вовлеченность в бизнес, цифровая трансформация открывает двери для новых сегментов рынка, каналов продаж и других путей получения прибыли.

В целях формирования нормативной базы правовой информатизации России и обеспечения выполнения Указа Президента Российской Федерации от 23.04.1993 № 477 «О мерах по ускорению создания центров правовой информации», Указом Президента РФ от 28.06.1993 № 966 была утверждена ***Концепция правовой информатизации России.***

Данная Концепция правовой информатизации России разработана по инициативе Государственно-правового управления Президента Российской Федерации, осуществляющего в соответствии с Указом Президента Российской Федерации от 4.04.1992 № 363 функции генерального заказчика систем правовой информации, в целях активизации

процесса создания государственных правовых информационных систем.

Стремительное качественное обновление общества, становление рыночной экономики, построение демократического правового государства – эти и многие другие проблемы выдвигают на первый план решение глобальной задачи – формирования в России единого информационно-правового пространства, обеспечивающего правовую информированность всех структур общества и каждого гражданина в отдельности, ибо правовая образованность необходима, чтобы расти в условиях демократии.

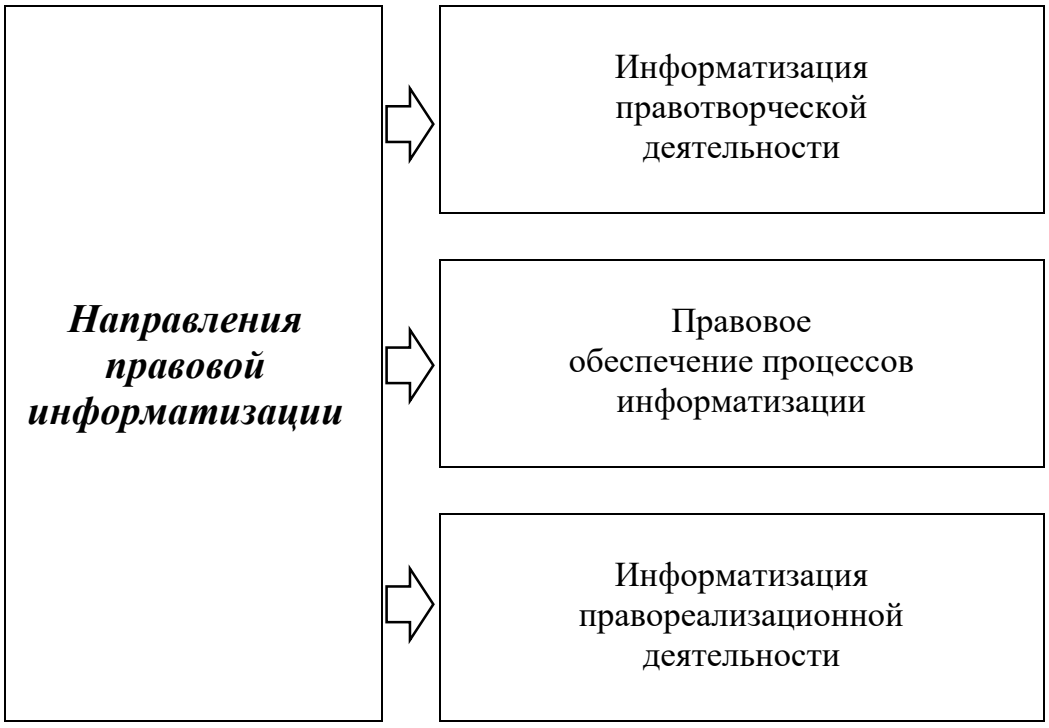
Удобное распределение и использование информации для удовлетворения социальных потребностей является едва ли не главнейшим достоинством в окружающем нас мире, и, как следствие, в результате совершенствования информационных коммуникаций внутри и между различными социальными группами общество может развиваться более динамично.

Поступательное развитие демократии возможно лишь тогда, когда между гражданами существует более или менее прочное согласие, когда их сближают общие взгляды, установки, информация.

Современная информационная система должна давать гражданам уверенность в качестве своих знаний, в реальной способности влиять на общественные процессы.

Решения, оказавшиеся неверными, чаще всего бывают следствием недостатка объективной информации, а не отсутствия компетентности или неэффективного использования той имеющейся информации, которая попала в официальные информационные каналы.

Пути совершенствования процесса правовой информатизации общества многообразны, поэтому необходимо четкое определение целей, методов организационных форм решения поставленной задачи, т. е. формирование ее научных основ.



ИНФОРМАЦИЯ ОГРАНИЧЕННОГО ДОСТУПА

Понятие и назначение информации ограниченного доступа

В соответствии со ст. 9 Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», *ограничение доступа к информации устанавливается федеральными законами и актами Президента Российской Федерации* 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 и актами Президента Российской Федерации.

Порядок идентификации информационных ресурсов в целях принятия мер ограничения доступа к информационным ресурсам, требования к способам (методам) ограничения такого доступа, применяемым в соответствии с законом, а также *требования к размещаемой информации об ограничении доступа к информационным ресурсам определяются* федеральным органом исполнительной власти, осуществляющим функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи (Приказ Роскомнадзора от 11.02.2019 № 21 «Об утверждении Порядка идентификации информационных ресурсов в целях принятия мер по ограничению доступа к информационным ресурсам»; Приказ Роскомнадзора от 14.12.2017 № 249 «Об утверждении требований к способам (методам) ограничения доступа к информационным ресурсам, а также требований к размещаемой информации об ограничении доступа к информационным ресурсам»).

Защита информации, составляющей государственную тайну, осуществляется в соответствии с законодательством Российской Федерации о государственной тайне.

Федеральными законами устанавливаются условия отнесения информации к сведениям, составляющим коммерческую тайну, служебную тайну и иную тайну, обязательность соблюдения конфиденциальности такой информации, а также ответственность за ее разглашение.

Информация, полученная гражданами (физическими лицами) при исполнении ими профессиональных обязанностей или организациями

при осуществлении ими определенных видов деятельности (профессиональная тайна), подлежит защите в случаях, если на эти лица федеральными законами возложены обязанности по соблюдению конфиденциальности такой информации (табл. 2).

Таблица 2

Перечень некоторых нормативных актов,
относящих сведения к категории ограниченного доступа

Сведения, отнесенные к категории ограниченного доступа	Основания отнесения сведений к категории ограниченного доступа
Государственная тайна	Ст. 5 Закона РФ от 21.07.1993 № 5485-1 «О государственной тайне»
	Указ Президента РФ от 30.11.1995 № 1203 «Об утверждении Перечня сведений, отнесенных к государственной тайне»
	Ст. 12 Федерального закона от 12.08.1995 № 144-ФЗ «Об оперативно-розыскной деятельности»
	Ст. 17, 19 Федерального закона от 03.04.1995 № 40-ФЗ «О федеральной службе безопасности»
	Ст. 26 Федерального закона от 03.07.2016 № 226-ФЗ «О войсках национальной гвардии Российской Федерации»
	Ст. 18 и 19 Федерального закона от 10.01.1996 № 5-ФЗ «О внешней разведке»
Коммерческая тайна	Федеральный закон от 29.07.2004 № 98-ФЗ «О коммерческой тайне»
	Ст. 14.7 Федерального закона от 26.07.2006 № 135-ФЗ «О защите конкуренции»
Конфиденциальная информация, полученная в ходе переговоров о заключении договора от другой стороны	Ст. 434.1 Гражданского кодекса РФ (часть первая)
Персональные данные (любая информация, относящаяся прямо или косвенно к определенному или определяемому физическому лицу (субъекту персональных данных))	Ст. 7 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»
	Ст. 88 Трудового кодекса РФ
	Ст. 13 Закона РФ от 20.07.2012 № 125-ФЗ «О донорстве крови и ее компонентов»
	Ст. 12 Федерального закона от 25.07.1998 № 128-ФЗ «О государственной дактилоскопической регистрации в Российской Федерации»
	Ст. 92 Федерального закона от 21.11.2011 № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации»
Налоговая тайна	Ст. 102, 142.5 и 313 Налогового кодекса РФ

Окончание табл. 2

Сведения, отнесенные к категории ограниченного доступа	Основания отнесения сведений к категории ограниченного доступа
Банковская тайна	Ст. 857 Гражданского кодекса РФ (часть вторая)
	Ст. 26 Федерального закона от 02.12.1990 № 395-1 «О банках и банковской деятельности»
	Ст. 57 Федерального закона от 10.07.2002 № 86-ФЗ «О Центральном банке Российской Федерации (Банке России)»
Врачебная тайна	Ст. 13 Федерального закона от 21.11.2011 № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации»
	Ст. 9 Закона РФ от 02.07.1992 № 3185-1 «О психиатрической помощи и гарантиях прав граждан при ее оказании»
Нотариальная тайна	Ст. 16, 28 и 34.1 Основ законодательства Российской Федерации о нотариате от 11.02.1993 № 4462-1
Адвокатская тайна	Ст. 8 и 39.5 Федерального закона от 31.05.2002 № 63-ФЗ «Об адвокатской деятельности и адвокатуре в Российской Федерации»
Тайна связи	Ст. 23 Конституции РФ
	Ст. 53 и 63 Федерального закона от 07.07.2003 № 126-ФЗ «О связи»
	Ст. 15 Федерального закона от 17.07.1999 № 176-ФЗ «О почтовой связи»
	Ст. 10.1 Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»
Тайна завещания	Ст. 1123 Гражданского кодекса РФ (часть третья)
Тайна усыновления	Ст. 139 Семейного кодекса РФ
Тайна исповеди	Ст. 3 Федерального закона от 26.09.1997 № 125-ФЗ «О свободе совести и о религиозных объединениях»
Конфиденциальная информация о детях, оставшихся без попечения родителей, гражданах, желающих принять детей на воспитание в свои семьи, гражданах, лишенных родительских прав и т.д.	Ст. 8 Федерального закона от 16.04.2001 № 44-ФЗ «О государственном банке данных о детях, оставшихся без попечения родителей»
Тайна следствия	Ст. 161 Уголовно-процессуального кодекса РФ
	Ст. 20 Федерального закона от 10.06.2008 № 76-ФЗ «Об общественном контроле за обеспечением прав человека в местах принудительного содержания и о содействии лицам, находящимся в местах принудительного содержания»

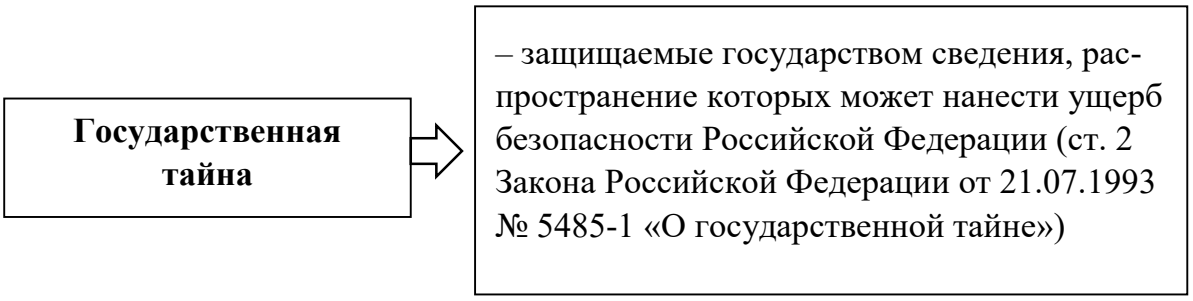
Информация, составляющая профессиональную тайну, может быть предоставлена третьим лицам в соответствии с федеральными законами и (или) по решению суда.

Срок исполнения обязанностей по соблюдению конфиденциальности информации, составляющей профессиональную тайну, может быть ограничен только с согласия гражданина (физического лица), предоставившего такую информацию о себе.

Запрещается требовать от гражданина (физического лица) предоставления информации о его частной жизни, в том числе информации, составляющей личную или семейную тайну, и получать такую информацию помимо воли гражданина (физического лица), если иное не предусмотрено федеральными законами.

Порядок доступа к персональным данным граждан (физических лиц) устанавливается федеральным законом о персональных данных (Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»).

Государственная тайна



Законом Российской Федерации от 21.07.1993 №5485-1 «О государственной тайне» определены полномочия органов государственной власти и должностных лиц в области отнесения сведений к государственной тайне и их защиты.

К полномочиям Палат Федерального Собрания Российской Федерации относятся:

– осуществление законодательного регулирования отношений в области государственной тайны;

– рассмотрение статей федерального бюджета в части средств, направляемых на реализацию государственных программ в области защиты государственной тайны;

– определение полномочий должностных лиц в аппаратах палат Федерального Собрания по обеспечению защиты государственной тайны в палатах Федерального Собрания.

Полномочия Президента РФ в области отнесения сведений к государственной тайне и их защиты

- Утверждение государственных программ в области защиты государственной тайны
- Утверждение по представлению Правительства РФ состава, структуры межведомственной комиссии по защите государственной тайны и положения о ней
- Определение полномочий должностных лиц по обеспечению защиты государственной тайны и порядок обеспечения режима секретности в Администрации Президента РФ, включая вопросы оформления, переоформления и прекращения допуска должностных лиц к государственной тайне, доступа к сведениям, составляющим государственную тайну
- Утверждение по представлению Правительства РФ Перечня должностных лиц органов государственной власти и организаций, наделяемых полномочиями по отнесению сведений к государственной тайне
- Заключение международных договоров РФ о совместном использовании и защите сведений, составляющих государственную тайну
- Решение иных вопросов, возникающих в связи с отнесением сведений к государственной тайне, их засекречиванием или рассекречиванием и их защитой (в пределах своих полномочий)

Полномочия Правительства РФ в области отнесения сведений к государственной тайне и их защиты

- Организация исполнения Закона РФ «О государственной тайне»
- Представление на утверждение Президенту РФ состав, структуру межведомственной комиссии по защите государственной тайны и положение о ней

- Установление порядка оформления, переоформления и прекращения допуска должностных лиц и граждан РФ, в том числе имеющих гражданство (подданство) иностранного государства, лиц без гражданства, иностранных граждан к государственной тайне, а также их доступа к сведениям, составляющим государственную тайну
- Организация разработки и выполнение государственных программ в области защиты государственной тайны
- Установление порядка разработки Перечня сведений, отнесенных к государственной тайне
- Установление порядка обеспечения режима секретности в Российской Федерации
- Издание актов по вопросам, связанным с выездом из Российской Федерации граждан РФ, допущенных или ранее допускавшихся к государственной тайне
- Установление порядка организации и проведения работ по противодействию иностранным техническим разведкам и технической защите информации, содержащей сведения, составляющие государственную тайну
- Решение иных вопросов, возникающих в связи с отнесением сведений к государственной тайне, их засекречиванием или рассекречиванием и их защитой (в пределах своих полномочий)

Полномочия Органов судебной власти в области отнесения сведений к государственной тайне и их защиты

- Рассмотрение уголовных, гражданских и административных дел о нарушениях законодательства РФ о государственной тайне
- Обеспечение судебной защиты граждан, органов государственной власти, предприятий, учреждений и организаций в связи с их деятельностью по защите государственной тайны
- Обеспечение в ходе рассмотрения указанных дел защиты государственной тайны
- Определение полномочий должностных лиц по обеспечению защиты государственной тайны в органах судебной власти

В соответствии со ст. 5 Закона Российской Федерации от 21.07.1993 №5485-1 «О государственной тайне», государственную тайну составляют:

1) сведения в военной области

– о содержании стратегических и оперативных планов, документов боевого управления по подготовке и проведению операций, стратегическому, оперативному и мобилизационному развертыванию Вооруженных Сил Российской Федерации, других войск, воинских формирований и органов, предусмотренных Федеральным законом от 31.05.1996 №61-ФЗ «Об обороне», об их боевой и мобилизационной готовности, о создании и об использовании мобилизационных ресурсов;

– о планах строительства Вооруженных Сил Российской Федерации, других войск Российской Федерации, о направлениях развития вооружения и военной техники, о содержании и результатах выполнения целевых программ, научно-исследовательских и опытно-конструкторских работ по созданию и модернизации образцов вооружения и военной техники;

– о разработке, технологии, производстве, об объемах производства, о хранении, об утилизации ядерных боеприпасов, их составных частей, делящихся ядерных материалов, используемых в ядерных боеприпасах, о технических средствах и (или) методах защиты ядерных боеприпасов от несанкционированного применения, а также о ядерных энергетических и специальных физических установках оборонного значения;

– о тактико-технических характеристиках и возможностях боевого применения образцов вооружения и военной техники, о свойствах, рецептурах или технологиях производства новых видов ракетного топлива или взрывчатых веществ военного назначения;

– о дислокации, назначении, степени готовности, защищенности режимных и особо важных объектов, об их проектировании, строительстве и эксплуатации, а также об отводе земель, недр и акваторий для этих объектов;

– о дислокации, действительных наименованиях, об организационной структуре, о вооружении, численности войск и состоянии их боевого обеспечения, а также о военно-политической и (или) оперативной обстановке;

2) сведения в области экономики, науки и техники

– о содержании планов подготовки Российской Федерации и ее отдельных регионов к возможным военным действиям, о мобилизационных мощностях промышленности по изготовлению и ремонту

вооружения и военной техники, об объемах производства, поставок, о запасах стратегических видов сырья и материалов, а также о размещении, фактических размерах и об использовании государственных материальных резервов;

– об использовании инфраструктуры Российской Федерации в целях обеспечения обороноспособности и безопасности государства;

– о силах и средствах гражданской обороны, о дислокации, предназначении и степени защищенности объектов административного управления, о степени обеспечения безопасности населения, о функционировании транспорта и связи в Российской Федерации в целях обеспечения безопасности государства;

– об объемах, о планах (заданиях) государственного оборонного заказа, о выпуске и поставках (в денежном или натуральном выражении) вооружения, военной техники и другой оборонной продукции, о наличии и наращивании мощностей по их выпуску, о связях предприятий по кооперации, о разработчиках или об изготовителях указанных вооружения, военной техники и другой оборонной продукции;

– о достижениях науки и техники, о научно-исследовательских, об опытно-конструкторских, о проектных работах и технологиях, имеющих важное оборонное или экономическое значение, влияющих на безопасность государства;

– о запасах платины, металлов платиновой группы, природных алмазов в Государственном фонде драгоценных металлов и драгоценных камней Российской Федерации, Центральном банке Российской Федерации, а также об объемах запасов в недрах, добычи, производства и потребления стратегических видов полезных ископаемых Российской Федерации;

3) сведения в области внешней политики и экономики

– о внешнеполитической, внешнеэкономической деятельности Российской Федерации, преждевременное распространение которых может нанести ущерб безопасности государства;

– о финансовой политике в отношении иностранных государств (за исключением обобщенных показателей по внешней задолженности), а также о финансовой или денежно-кредитной деятельности, преждевременное распространение которых может нанести ущерб безопасности государства;

4) сведения в области разведывательной, контрразведывательной и оперативно-розыскной деятельности, а также в области противодействия терроризму и в области обеспечения безопасности лиц, в отношении которых принято решение о применении мер государственной защиты:

– о силах, средствах, об источниках, о методах, планах и результатах разведывательной, контрразведывательной, оперативно-розыскной деятельности и деятельности по противодействию терроризму, а также данные о финансировании этой деятельности, если эти данные раскрывают перечисленные сведения;

– о силах, средствах, об источниках, о методах, планах и результатах деятельности по обеспечению безопасности лиц, в отношении которых принято решение о применении мер государственной защиты, данные о финансировании этой деятельности, если эти данные раскрывают перечисленные сведения, а также отдельные сведения об указанных лицах;

– о лицах, сотрудничающих или сотрудничавших на конфиденциальной основе с органами, осуществляющими разведывательную, контрразведывательную и оперативно-розыскную деятельность;

– об организации, о силах, средствах и методах обеспечения безопасности объектов государственной охраны, а также данные о финансировании этой деятельности, если эти данные раскрывают перечисленные сведения;

– о системе президентской, правительственной, шифрованной, в том числе кодированной и засекреченной, связи, о шифрах, о разработке, об изготовлении шифров и обеспечении ими, о методах и средствах анализа шифровальных средств и средств специальной защиты, об информационно-аналитических системах специального назначения;

– о методах и средствах защиты секретной информации;

– об организации обеспечения режима секретности и о фактическом состоянии защиты государственной тайны;

– о защите Государственной границы Российской Федерации, исключительной экономической зоны и континентального шельфа Российской Федерации;

– о расходах федерального бюджета, связанных с обеспечением обороны, безопасности государства и правоохранительной деятельности в Российской Федерации;

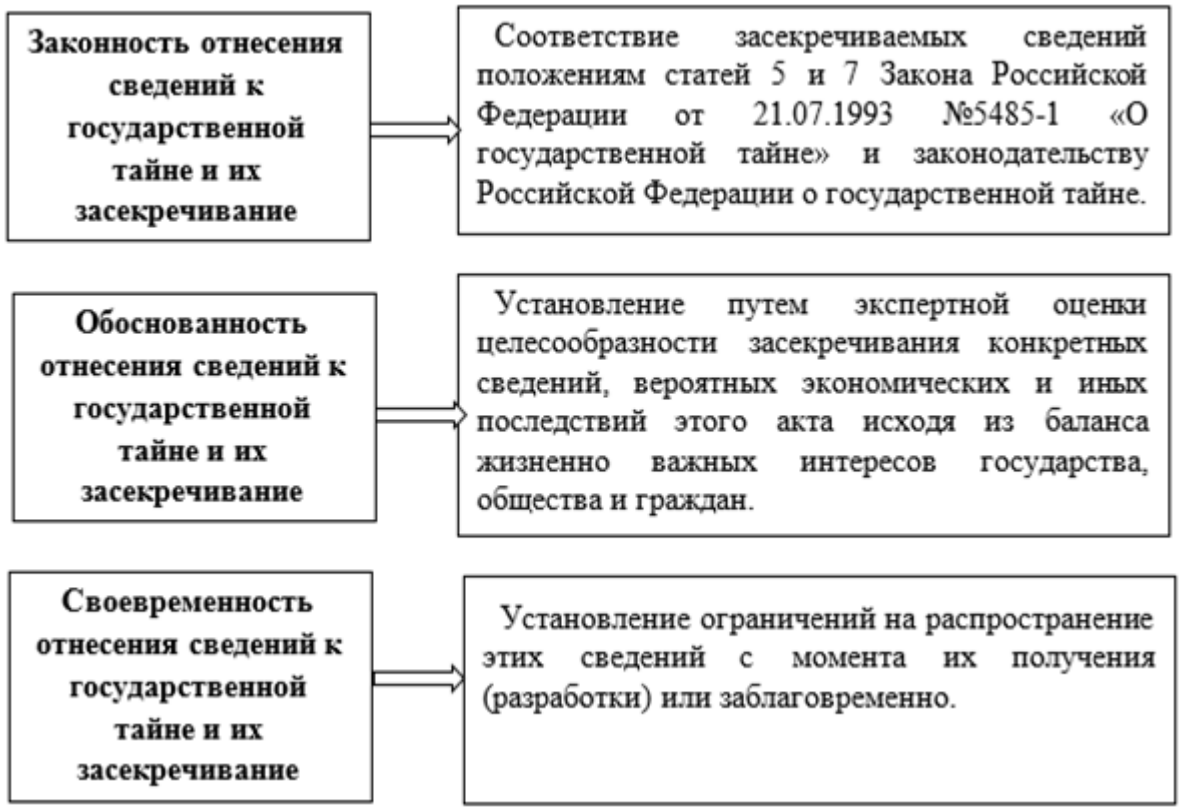
– о подготовке кадров, раскрывающие мероприятия, проводимые в целях обеспечения безопасности государства;

– о мерах по обеспечению защищенности критически важных объектов и потенциально опасных объектов инфраструктуры Российской Федерации от террористических актов;

– о результатах финансового мониторинга в отношении организаций и физических лиц, полученных в связи с проверкой их возможной причастности к террористической деятельности;

– о мерах по обеспечению безопасности критической информационной инфраструктуры Российской Федерации и о состоянии ее защищенности от компьютерных атак.

Основные принципы отнесения сведений к государственной тайне и засекречивания этих сведений



Сведения, не подлежащие засекречиванию

- Сведения о чрезвычайных происшествиях и катастрофах, угрожающих безопасности и здоровью граждан, и их последствиях, а также о стихийных бедствиях, их официальных прогнозах и последствиях
- Сведения о состоянии здравоохранения, санитарии, демографии, образования, культуры, сельского хозяйства, а также о состоянии преступности
- Сведения о привилегиях, компенсациях и социальных гарантиях, предоставляемых государством гражданам, должностным лицам, предприятиям, учреждениям и организациям
- Сведения о фактах нарушения прав и свобод человека и гражданина
- Сведения о состоянии здоровья высших должностных лиц РФ
- Сведения о фактах нарушения законности органами государственной власти и их должностными лицами
- Сведения, составляющие информацию о состоянии окружающей среды (экологическую информацию)

Должностные лица, принявшие решения о засекречивании перечисленных сведений либо о включении их в этих целях в носители сведений, составляющих государственную тайну, несут уголовную, административную или дисциплинарную ответственность в зависимости от причиненного обществу, государству и гражданам материального и морального ущерба.

Граждане вправе обжаловать такие решения в суд.

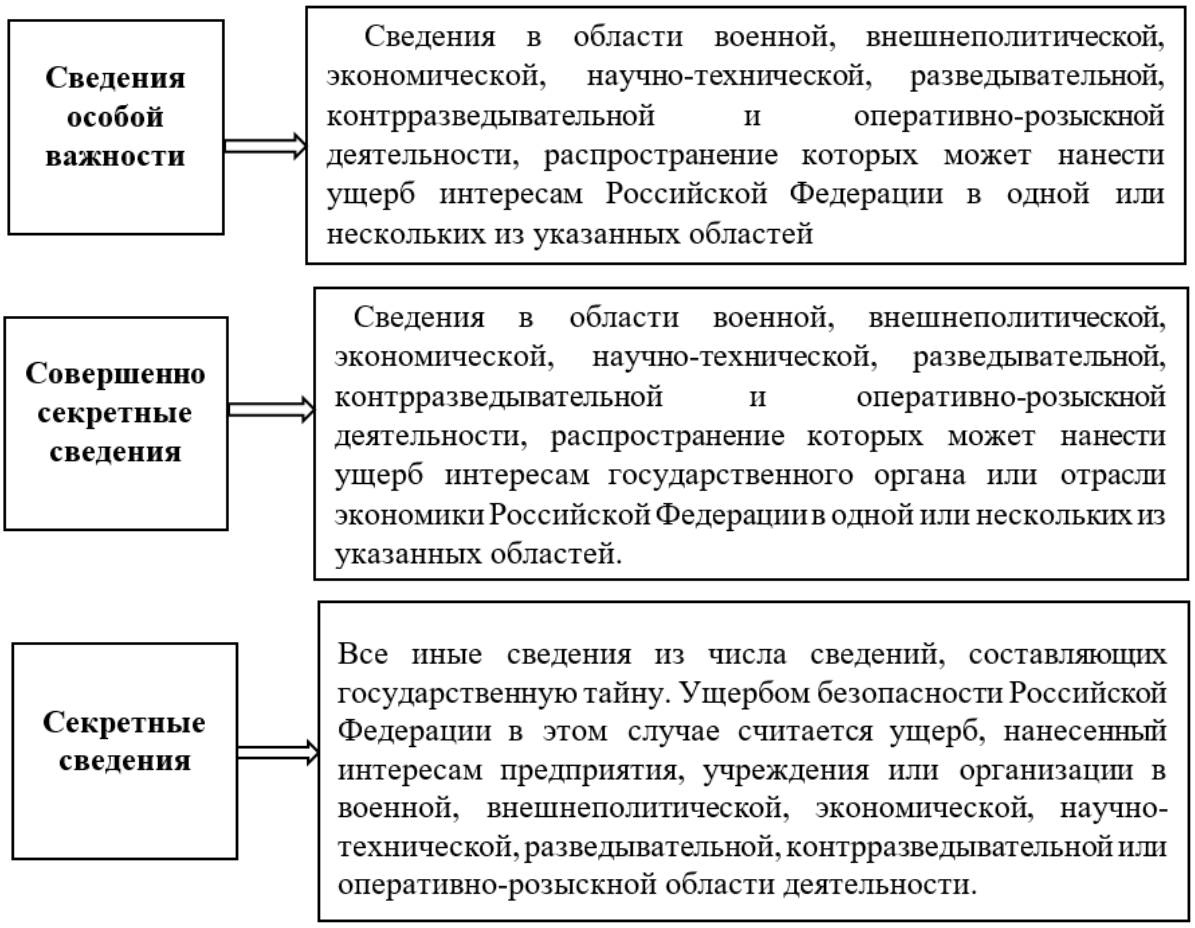
Степень секретности сведений, составляющих государственную тайну, должна соответствовать степени тяжести ущерба, который может быть нанесен безопасности Российской Федерации вследствие распространения указанных сведений.

Устанавливаются три степени секретности сведений, составляющих государственную тайну, и соответствующие этим степеням грифы секретности для носителей указанных сведений: «особой важности», «совершенно секретно» и «секретно».

Порядок определения размеров ущерба, который может быть нанесен безопасности Российской Федерации вследствие распространения сведений, составляющих государственную тайну, и правила отнесения указанных сведений к той или иной степени секретности

устанавливаются Правительством Российской Федерации (Постановление Правительства РФ от 04.09.1995 № 870 «Об утверждении Правил отнесения сведений, составляющих государственную тайну, к различным степеням секретности»).

Грифы секретности



Использование перечисленных грифов секретности для засекречивания сведений, не отнесенных к государственной тайне, не допускается.

Отнесение сведений к государственной тайне осуществляется в соответствии с их отраслевой, ведомственной или программно-целевой принадлежностью, а также в соответствии с Законом Российской Федерации «О государственной тайне».

Обоснование необходимости отнесения сведений к государственной тайне в соответствии с принципами засекречивания сведений возлагается на органы государственной власти, предприятия, учреждения и организации, которыми эти сведения получены (разработаны).

Отнесение сведений к государственной тайне осуществляется в соответствии с их отраслевой, ведомственной или программно-целевой принадлежностью, а также в соответствии с Законом Российской Федерации «О государственной тайне».

Обоснование необходимости отнесения сведений к государственной тайне в соответствии с принципами засекречивания сведений возлагается на органы государственной власти, предприятия, учреждения и организации, которыми эти сведения получены (разработаны).

Для осуществления единой государственной политики в области засекречивания сведений межведомственная комиссия по защите государственной тайны формирует по предложениям органов государственной власти и в соответствии с Перечнем сведений, составляющих государственную тайну, Перечень сведений, отнесенных к государственной тайне (Указ Президента РФ от 30.11.1995 № 1203 «Об утверждении Перечня сведений, отнесенных к государственной тайне»).

В этом Перечне указываются органы государственной власти, наделяемые полномочиями по распоряжению данными сведениями.

Указанный Перечень подлежит открытому опубликованию и пересматривается по мере необходимости.

Рассекречивание сведений и их носителей ⇨ - снятие ранее введенных в предусмотренном данным законом порядке ограничений на распространение сведений, составляющих государственную тайну, и на доступ к их носителям (ст. 13 Закона Российской Федерации от 21.07.1993 №5485-1 «О государственной тайне»)

Основания для рассекречивания сведений

⇩ Взятие на себя Российской Федерацией международных обязательств по открытому обмену сведениями, составляющими в Российской Федерации государственную тайну

⇩ Изменение объективных обстоятельств, вследствие которого дальнейшая защита сведений, составляющих государственную тайну, является нецелесообразной

Органы государственной власти, руководители которых наделены полномочиями по отнесению сведений к государственной тайне, обязаны периодически, но не реже чем через каждые пять лет, пересматривать содержание действующих в органах государственной власти, на предприятиях, в учреждениях и организациях перечней сведений, подлежащих засекречиванию в части обоснованности засекречивания сведений и их соответствия установленной ранее степени секретности.

Срок засекречивания сведений, составляющих государственную тайну, не должен превышать 30 лет. В исключительных случаях этот срок может быть продлен по заключению межведомственной комиссии по защите государственной тайны.

Правом изменения действующих в органах государственной власти, на предприятиях, в учреждениях и организациях перечней сведений, подлежащих засекречиванию, наделяются утвердившие их руководители органов государственной власти, которые несут персональную ответственность за обоснованность принятых ими решений по рассекречиванию сведений.

Решения указанных руководителей, связанные с изменением перечня сведений, отнесенных к государственной тайне, подлежат согласованию с межведомственной комиссией по защите государственной тайны, которая вправе приостанавливать и опротестовывать эти решения.

Ст. 20 Закона Российской Федерации от 21.07.1993 № 5485-1 «О государственной тайне» определяет органы защиты государственной тайны (табл. 3)

Таблица 3

Органы защиты государственной тайны и их назначение

Органы	Назначение
Межведомственная комиссия по защите государственной тайны	Является коллегиальным органом, координирующим деятельность органов государственной власти по защите государственной тайны в интересах разработки и выполнения государственных программ, нормативных и методических документов, обеспечивающих реализацию законодательства РФ о государственной тайне

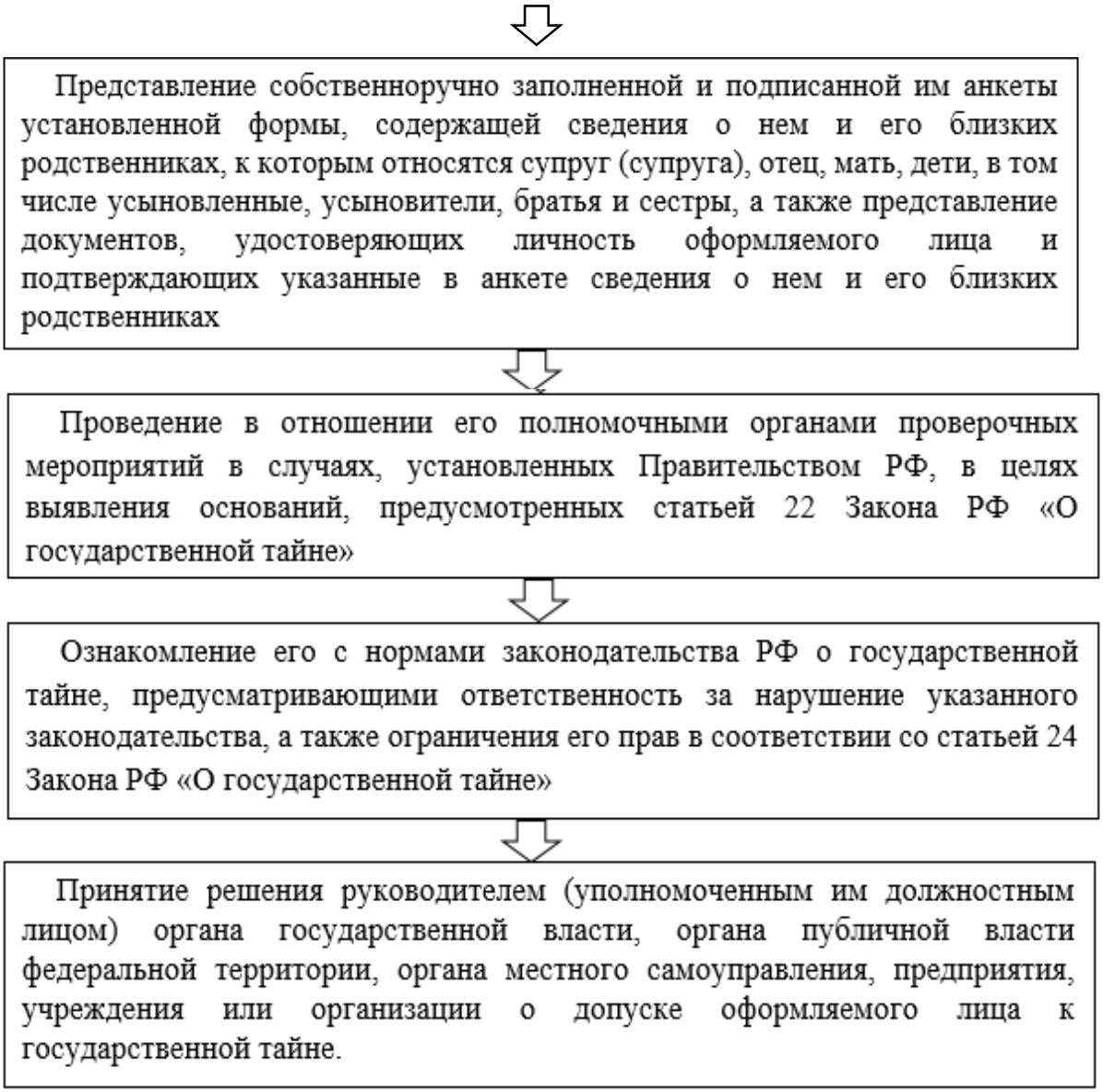
Окончание табл. 3

Органы	Назначение
Федеральные органы исполнительной власти, уполномоченные в области обеспечения безопасности, в области обороны, в области внешней разведки, в области противодействия техническим разведкам и технической защиты информации, и их территориальные органы	Организуют и обеспечивают защиту государственной тайны в соответствии с функциями, возложенными на них законодательством РФ
Органы государственной власти, предприятия, учреждения и организации	Обеспечивают защиту сведений, составляющих государственную тайну, в соответствии с возложенными на них задачами и в пределах своей компетенции

В зависимости от объема работ с использованием сведений, составляющих государственную тайну, руководителями органов государственной власти, предприятий, учреждений и организаций создаются структурные подразделения по защите государственной тайны, функции которых определяются указанными руководителями в соответствии с нормативными документами, утверждаемыми Правительством РФ, и с учетом специфики проводимых ими работ.

Защита государственной тайны является видом основной деятельности органа государственной власти, предприятия, учреждения или организации.

Процедура оформления допуска должностного лица или гражданина к государственной тайне



В отношении граждан, призванных на военную службу или военные сборы, представление собственноручно заполненной анкеты установленной формы и получение их согласия на оформление допуска к государственной тайне не являются обязательными.

Проверочные мероприятия, связанные с допуском должностных лиц и граждан к государственной тайне, проводятся федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, и (или) его территориальными органами.

Проверочные мероприятия проводятся в соответствии с законодательством РФ.

Объем проверочных мероприятий зависит от степени секретности сведений, к которым будет допускаться оформляемое лицо (табл. 4).

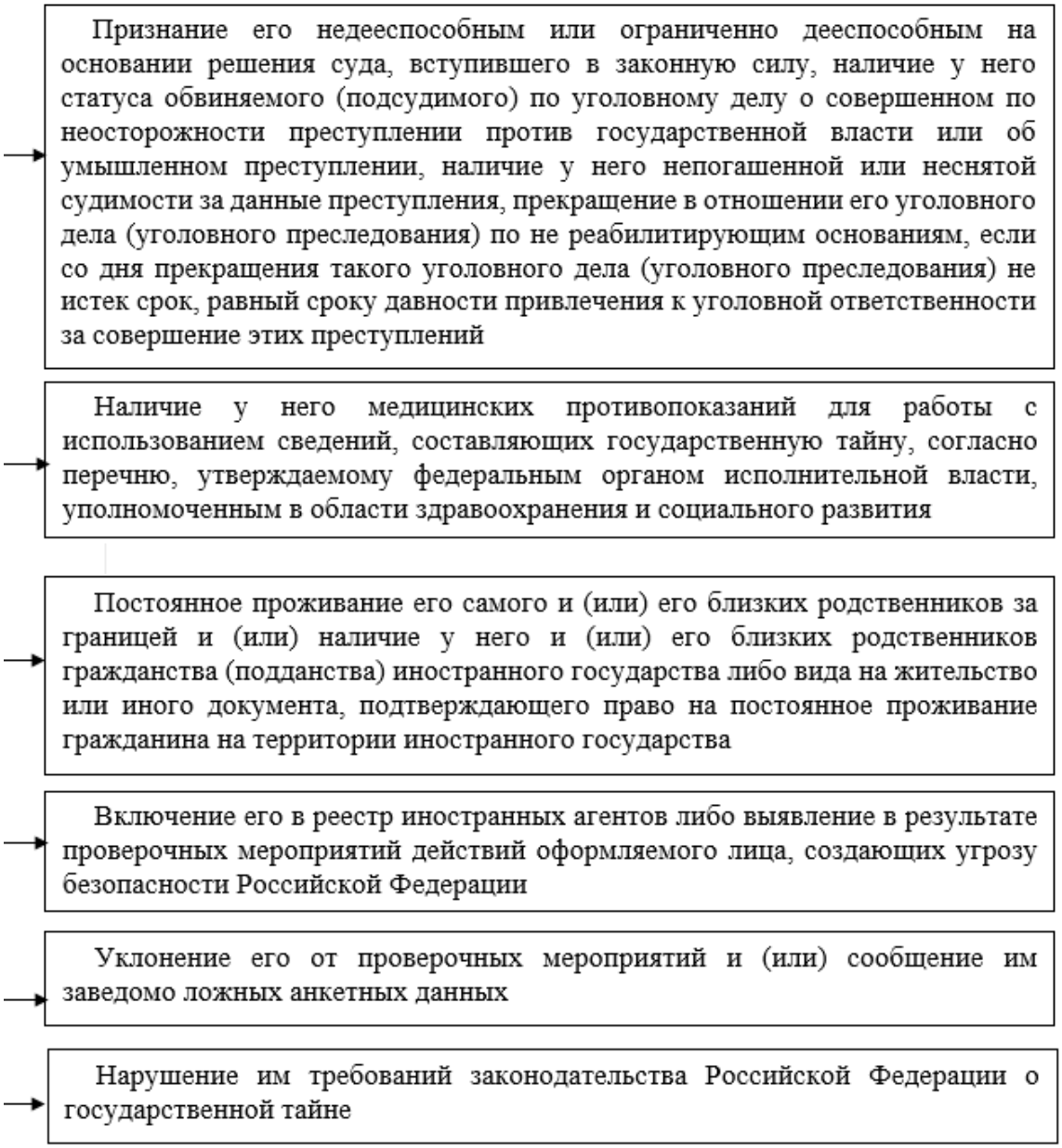
Таблица 4

Обязанности и социальные гарантии для должностных лиц и граждан, допущенных к государственной тайне

Обязанности должностных лиц и граждан, допущенных к государственной тайне	Социальные гарантии для должностных лиц и граждан, допущенных к государственной тайне
Не разглашать сведения, составляющие государственную тайну, а также выполнять иные требования законодательства РФ о государственной тайне	Процентные надбавки к должностному окладу (тарифной ставке) в зависимости от степени секретности сведений, к которым они имеют доступ
Информировать в установленном порядке об имеющихся у должностного лица или гражданина РФ, допущенного к государственной тайне, данных, свидетельствующих о наличии (возникновении) обстоятельств, которые являются основаниями для отказа в допуске к государственной тайне	Процентные надбавки к должностному окладу (тарифной ставке) за стаж работы в структурных подразделениях по защите государственной тайны
Информировать в установленном порядке о попытках получения от них сведений, составляющих государственную тайну	Преимущественное право при прочих равных условиях на оставление на работе при проведении органами государственной власти, органами местного самоуправления, органами публичной власти федеральных территорий, предприятиями, учреждениями и организациями организационных и (или) штатных мероприятий

Устанавливаются три формы допуска к государственной тайне должностных лиц и граждан, соответствующие трем степеням секретности сведений, составляющих государственную тайну: к сведениям особой важности, совершенно секретным сведениям или секретным сведениям. Наличие у должностных лиц и граждан права на доступ к сведениям более высокой степени секретности является основанием для доступа их к сведениям более низкой степени секретности.

Основания для отказа должностному лицу или гражданину в допуске к государственной тайне



Заключение трудового договора (контракта) до окончания проведения проверочных мероприятий, связанных с допуском к государственной тайне, не допускается.

В случае вынесения федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, и (или) его территориальным органом заключения о нецелесообразности допуска должностного лица или гражданина к государственной тайне такому должностному лицу или гражданину отказывается в допуске к государ-

ственной тайне. Лицо, в отношении которого принято решение об отказе в допуске к государственной тайне, имеет право обжаловать это решение вышестоящему должностному лицу, в вышестоящую организацию или в суд.

В соответствии со статьей 26 Закона Российской Федерации от 21.07.1993 № 5485-1 «О государственной тайне», должностные лица и граждане, виновные в нарушении законодательства Российской Федерации о государственной тайне, несут уголовную, административную, гражданско-правовую или дисциплинарную ответственность в соответствии с действующим законодательством (табл. 5).

Таблица 5

Меры уголовной и административной ответственности за нарушение законодательства о государственной тайне

Уголовная ответственность (Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ)	
Статья 275. Государственная измена	Государственная измена, то есть совершенные гражданином РФ шпионаж, выдача иностранному государству, международной либо иностранной организации или их представителям сведений, составляющих государственную тайну, доверенную лицу или ставшую известной ему по службе, работе, учебе или в иных случаях, предусмотренных законодательством РФ, переход на сторону противника либо оказание финансовой, материально-технической, консультационной или иной помощи иностранному государству, международной либо иностранной организации или их представителям в деятельности, направленной против безопасности РФ, – *наказывается лишением свободы на срок от двенадцати до двадцати лет со штрафом в размере до пятисот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до трех лет либо без такового и с ограничением свободы на срок до двух лет или пожизненным лишением свободы*
Статья 276. Шпионаж	Передача, собирание, похищение или хранение в целях передачи иностранному государству, международной либо иностранной организации или их представителям сведений, составляющих государственную тайну, а также передача или собирание по заданию иностранной разведки или лица, действующего в ее интересах, иных сведений для использования их против безопасности РФ либо передача, собирание, похищение или хранение в целях передачи противнику сведений, которые могут быть использованы против Вооруженных Сил

Продолжение табл. 5

Уголовная ответственность (Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ)	
Статья 276. Шпионаж	РФ, других войск, воинских формирований и органов РФ, совершенные в условиях вооруженного конфликта, военных действий или иных действий с применением вооружения и военной техники с участием РФ, то есть шпионаж, если эти деяния совершены иностранным гражданином или лицом без гражданства, – *наказываются лишением свободы на срок от десяти до двадцати лет*
Статья 283. Разглашение государственной тайны	1. Разглашение сведений, составляющих государственную тайну, лицом, которому она была доверена или стала известна по службе, работе, учебе или в иных случаях, предусмотренных законодательством РФ, если эти сведения стали достоянием других лиц, при отсутствии признаков преступлений, предусмотренных ст. 275 и 276 УК РФ, *–наказывается арестом на срок от четырех до шести месяцев либо лишением свободы на срок до четырех лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового.* 2. То же деяние, повлекшее по неосторожности тяжкие последствия, – *наказывается лишением свободы на срок от трех до семи лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет*
Статья 284. Утрата документов, содержащих государственную тайну	Нарушение лицом, имеющим допуск к государственной тайне, установленных правил обращения с содержащими государственную тайну документами, а равно с предметами, сведения о которых составляют государственную тайну, если это повлекло по неосторожности их утрату и наступление тяжких последствий, – *наказывается ограничением свободы на срок до трех лет, либо арестом на срок от четырех до шести месяцев, либо лишением свободы на срок до трех лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового*

Продолжение табл. 5

Административная ответственность Кодекс Российской Федерации об административных правонарушениях от 30.12.2001 № 195-ФЗ)	
Статья 13.12. Нарушение правил защиты информации	П. 3. Нарушение условий, предусмотренных лицензией на проведение работ, связанных с использованием и защитой информации, составляющей государственную тайну, созданием средств, предназначенных для защиты информации, составляющей государственную тайну, осуществлением мероприятий и (или) оказанием услуг по защите информации, составляющей государственную тайну, – *влечет наложение административного штрафа на должностных лиц в размере от двух тысяч до трех тысяч рублей; на юридических лиц – от двадцати тысяч до двадцати пяти тысяч рублей* П. 4. Использование несертифицированных средств, предназначенных для защиты информации, составляющей государственную тайну, – *влечет наложение административного штрафа на должностных лиц в размере от трех тысяч до четырех тысяч рублей; на юридических лиц – от двадцати тысяч до тридцати тысяч рублей с конфискацией несертифицированных средств, предназначенных для защиты информации, составляющей государственную тайну, или без таковой*. П. 7. Нарушение требований о защите информации, составляющей государственную тайну, установленных федеральными законами и принятыми в соответствии с ними иными нормативными правовыми актами РФ, если такие действия (бездействие) не содержат уголовно наказуемого деяния, – *влечет наложение административного штрафа на граждан в размере от одной тысячи до двух тысяч рублей; на должностных лиц – от трех тысяч до четырех тысяч рублей; на юридических лиц – от пятнадцати тысяч до двадцати тысяч рублей*
Статья 13.13. Незаконная деятельность в области защиты информации	П. 2. Занятие видами деятельности, связанной с использованием и защитой информации, составляющей государственную тайну, созданием средств, предназначенных для защиты информации, составляющей государственную тайну, осуществлением мероприятий и (или) оказанием услуг по защите информации, составляющей государственную тайну, без лицензии, – *влечет наложение административного штрафа на должностных лиц в размере от четырех тысяч до пяти тысяч рублей; на юридических лиц – от тридцати тысяч до сорока тысяч рублей с конфискацией созданных без лицензии средств защиты информации, составляющей государственную тайну, или без таковой*

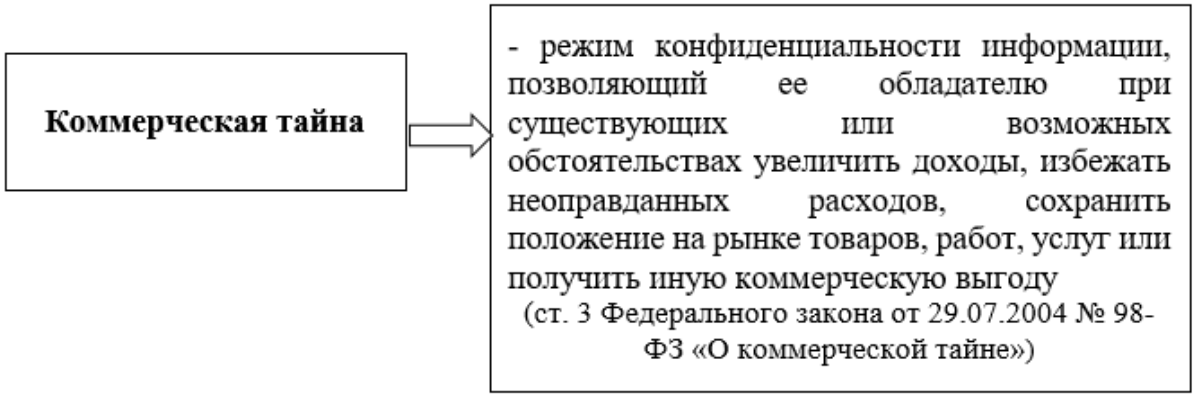
Окончание табл. 5

Административная ответственность Кодекс Российской Федерации об административных правонарушениях от 30.12.2001 № 195-ФЗ)	
Статья 13.14. Разглашение информации с ограниченным доступом	Разглашение информации, доступ к которой ограничен федеральным законом (за исключением случаев, если разглашение такой информации влечет уголовную ответственность), лицом, получившим доступ к такой информации в связи с исполнением служебных или профессиональных обязанностей, *– влечет наложение административного штрафа на граждан в размере от пяти тысяч до десяти тысяч рублей; на должностных лиц – от сорока тысяч до пятидесяти тысяч рублей или дисквалификацию на срок до трех лет; на юридических лиц – от ста тысяч до двухсот тысяч рублей*
Статья 14.49. Нарушение обязательных требований в отношении оборонной продукции (выполняемых работ, оказываемых услуг)	Нарушение изготовителем (лицом, выполняющим функции иностранного изготовителя), поставщиком (подрядчиком, исполнителем) обязательных требований в отношении оборонной продукции (выполняемых работ, оказываемых услуг), поставляемой по государственному оборонному заказу, продукции (выполняемых работ, оказываемых услуг), используемой в целях защиты сведений, составляющих государственную тайну или относимых к охраняемой в соответствии с законодательством РФ иной информации ограниченного доступа, продукции (выполняемых работ, оказываемых услуг), сведения о которой составляют государственную тайну, продукции (выполняемых работ, оказываемых услуг) и объектов, связанных с обеспечением ядерной и радиационной безопасности в области использования атомной энергии, процессов проектирования (включая изыскания), производства, строительства, монтажа, наладки, эксплуатации, хранения, перевозки, реализации, утилизации, захоронения, связанных с обязательными требованиями в отношении указанной продукции и объектов, установленными в соответствии с законодательством РФ о техническом регулировании и законодательством РФ о стандартизации, в том числе государственными заказчиками, федеральными органами исполнительной власти, уполномоченными в области обеспечения безопасности, обороны, внешней разведки, противодействия техническим разведкам и технической защиты информации, государственного управления использованием атомной энергии, государственного регулирования безопасности при использовании атомной энергии, и (или) государственными контрактами (договорами), *– влечет наложение административного штрафа на должностных лиц в размере от сорока тысяч до пятидесяти тысяч рублей; на юридических лиц – от семисот тысяч до одного миллиона рублей*

Соответствующие органы государственной власти и их должностные лица основываются на подготовленных в установленном порядке экспертных заключениях об отнесении незаконно распространенных сведений к сведениям, составляющим государственную тайну.

Защита прав и законных интересов граждан, органов государственной власти, предприятий, учреждений и организаций в сфере действия Закона Российской Федерации от 21.07.1993 №5485-1 «О государственной тайне» осуществляется в судебном или ином порядке, предусмотренном данным законом.

Коммерческая тайна



Информация, составляющая коммерческую тайну, – это 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;

Право на отнесение информации к информации, составляющей коммерческую тайну, и на определение перечня и состава такой информации принадлежит обладателю такой информации с учетом положений Федерального закона от 29.07.2004 № 98-ФЗ «О коммерческой тайне».

Информация, составляющая коммерческую тайну, полученная от ее обладателя на основании договора или другом законном основании, считается полученной законным способом.

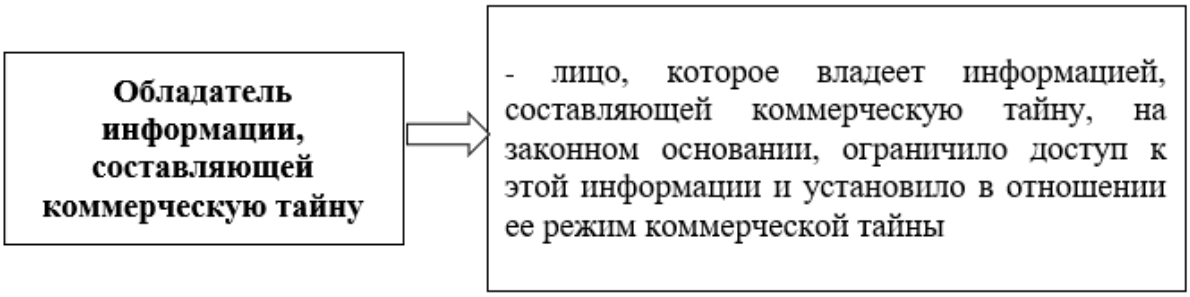
В соответствии со ст. 5 Федерального закона от 29.07.2004 № 98-ФЗ «О коммерческой тайне», режим коммерческой тайны не может быть установлен лицами, осуществляющими предпринимательскую деятельность, в отношении сведений, перечисленных ниже.

Сведения, в отношении которых не может быть установлен режим коммерческой тайны

- Сведения, содержащиеся в учредительных документах юридического лица, за исключением учредительных документов личного фонда или международного личного фонда, документах, подтверждающих факт внесения записей о юридических лицах и об индивидуальных предпринимателях в соответствующие государственные реестры
- Сведения, содержащиеся в документах, дающих право на осуществление предпринимательской деятельности
- Сведения о составе имущества государственного или муниципального унитарного предприятия, государственного учреждения и об использовании ими средств соответствующих бюджетов
- Сведения о состоянии противопожарной безопасности, санитарно-эпидемиологической и радиационной обстановке, безопасности пищевых продуктов
- Сведения о численности, о составе работников, о системе оплаты труда, об условиях труда, в том числе об охране труда, о показателях производственного травматизма и профессиональной заболеваемости, и о наличии свободных рабочих мест
- Сведения о задолженности работодателей по выплате заработной платы и социальным выплатам
- Сведения о нарушениях законодательства РФ и фактах привлечения к ответственности за совершение этих нарушений
- Сведения об условиях конкурсов или аукционов по приватизации объектов государственной или муниципальной собственности
- Сведения о размерах и структуре доходов некоммерческих организаций, за исключением личного фонда, в том числе международного личного фонда, о размерах и составе их имущества, об их расходах, о численности и об оплате труда их работников, об использовании безвозмездного труда граждан в деятельности некоммерческой организации, за исключением личного фонда, в том числе международного личного фонда

Обладатель информации, составляющей коммерческую тайну, по мотивированному требованию органа государственной власти, иного

государственного органа, органа местного самоуправления предоставляет им на безвозмездной основе информацию, составляющую коммерческую тайну.



Мотивированное требование должно быть подписано уполномоченным должностным лицом, содержать указание цели и правового основания затребования информации, составляющей коммерческую тайну, и срок предоставления этой информации, если иное не установлено федеральными законами.

Обладатель информации, составляющей коммерческую тайну, а также органы государственной власти, иные государственные органы, органы местного самоуправления, получившие такую информацию, обязаны предоставить эту информацию по запросу судов, органов предварительного следствия, органов дознания по делам, находящимся в их производстве, в порядке и на основаниях, которые предусмотрены законодательством Российской Федерации.

Федеральные органы исполнительной власти, получившие в рамках установленных полномочий информацию, составляющую коммерческую тайну, от обладателя такой информации, предоставляют такую информацию по запросу федеральных органов исполнительной власти в рамках межведомственного информационного взаимодействия с соблюдением требований и (или) ограничений, установленных Федеральным законом «О коммерческой тайне», в случаях, предусмотренных федеральными законами, с одновременным направлением обладателю такой информации любым доступным способом, в том числе посредством электронного документа, подписанного усиленной квалифицированной электронной подписью и направленного на адрес электронной почты обладателя такой информации, уведомления о ее предоставлении с указанием объема предоставленной информации.

На документах, составляющую коммерческую тайну, должен быть нанесен гриф «Коммерческая тайна» с указанием ее обладателя (для

юридических лиц – полное наименование и место нахождения, для индивидуальных предпринимателей – фамилия, имя, отчество гражданина, являющегося индивидуальным предпринимателем, и место жительства).

Права обладателя информации, составляющей коммерческую тайну

- Право устанавливать, изменять, отменять в письменной форме режим коммерческой тайны в соответствии с Федеральным законом «О коммерческой тайне» и гражданско-правовым договором
- Право использовать информацию, составляющую коммерческую тайну, для собственных нужд в порядке, не противоречащем законодательству Российской Федерации
- Право разрешать или запрещать доступ к информации, составляющей коммерческую тайну, определять порядок и условия доступа к этой информации
- Право требовать от юридических лиц, физических лиц, получивших доступ к информации, составляющей коммерческую тайну, органов государственной власти, иных государственных органов, органов местного самоуправления, которым предоставлена информация, составляющая коммерческую тайну, соблюдения обязанностей по охране ее конфиденциальности
- Право требовать от лиц, получивших доступ к информации, составляющей коммерческую тайну, в результате действий, совершенных случайно или по ошибке, охраны конфиденциальности этой информации
- Право защищать в установленном законом порядке свои права в случае разглашения, незаконного получения или незаконного использования

Права обладателя информации, составляющей коммерческую тайну, возникают с момента установления им в отношении этой информации режима коммерческой тайны.

Меры по охране конфиденциальности информации, принимаемые ее обладателем, установлены ст. 10 Федерального закона от 29.07.2004 № 98-ФЗ «О коммерческой тайне».

Меры по охране конфиденциальности информации, принимаемые ее обладателем

- Определение перечня информации, составляющей коммерческую тайну
- Ограничение доступа к информации, составляющей коммерческую тайну, путем установления порядка обращения с этой информацией и контроля за соблюдением такого порядка
- Учет лиц, получивших доступ к информации, составляющей коммерческую тайну, и (или) лиц, которым такая информация была предоставлена или передана
- Регулирование отношений по использованию информации, составляющей коммерческую тайну, работниками на основании трудовых договоров и контрагентами на основании гражданско-правовых договоров
- Нанесение на материальные носители, содержащие информацию, составляющую коммерческую тайну, или включение в состав реквизитов документов, содержащих такую информацию, грифа «Коммерческая тайна» с указанием обладателя такой информации (для юридических лиц - полное наименование и место нахождения, для индивидуальных предпринимателей - фамилия, имя, отчество гражданина, являющегося индивидуальным предпринимателем, и место жительства)совершенных случайно или по ошибке, охраны конфиденциальности этой информации

Режим коммерческой тайны считается установленным после принятия обладателем информации, составляющей коммерческую тайну, мер, указанных выше.

Наряду с мерами, указанными выше, обладатель информации, составляющей коммерческую тайну, вправе применять при необходимости средства и методы технической защиты конфиденциальности этой информации, другие, не противоречащие законодательству Российской Федерации, меры.

Разумно достаточные меры по охране конфиденциальности информации

⇩ ⇩

Исключается доступ к информации, составляющей коммерческую тайну, любых лиц без согласия ее обладателя	Обеспечивается возможность использования информации, составляющей коммерческую тайну, работниками и передачи ее контрагенетам без нарушения режима коммерческой тайны

Режим коммерческой тайны не может быть использован в целях, противоречащих требованиям защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства.

В соответствии со ст. 11 Федерального закона от 29.07.2004 № 98-ФЗ «О коммерческой тайне», в целях охраны конфиденциальности информации, составляющей коммерческую тайну, работодатель и работники имеют определенные обязанности (табл. 6)

Доступ работника к информации, составляющей коммерческую тайну, осуществляется с его согласия, если это не предусмотрено его трудовыми обязанностями.

Работодатель вправе потребовать возмещения убытков, причиненных ему разглашением информации, составляющей коммерческую тайну, от лица, получившего доступ к этой информации в связи с исполнением трудовых обязанностей, но прекратившего трудовые отношения с работодателем, если эта информация разглашена в течение срока действия режима коммерческой тайны.

Таблица 6

Обязанности работодателя и работников в целях охраны конфиденциальности информации, составляющей коммерческую тайну

Обязанности работодателя	Обязанности работника
Ознакомить под расписку работника, доступ которого к информации, обладателями которой являются работодатель и его контрагенты, необходим для исполнения данным работником своих трудовых обязанностей, с перечнем информации, составляющей коммерческую тайну	Выполнять установленный работодателем режим коммерческой тайны

Окончание табл. 6

Обязанности работодателя	Обязанности работника
Ознакомить под расписку работника с установленным работодателем режимом коммерческой тайны и с мерами ответственности за его нарушение	Не разглашать информацию, обладателями которой являются работодатель и его контрагенты, и без их согласия не использовать эту информацию в личных целях в течение всего срока действия режима коммерческой тайны, в том числе после прекращения действия трудового договора
Создать работнику необходимые условия для соблюдения им установленного работодателем режима коммерческой тайны	Возместить причиненные работодателю убытки, если работник виновен в разглашении информации, составляющей коммерческую тайну и ставшей ему известной в связи с исполнением им трудовых обязанностей
–	Передать работодателю при прекращении или расторжении трудового договора материальные носители информации, имеющиеся в пользовании работника и содержащие информацию, составляющую коммерческую тайну

Причиненные работником или прекратившим трудовые отношения с работодателем лицом убытки не возмещаются, если разглашение информации, составляющей коммерческую тайну, произошло вследствие несоблюдения работодателем мер по обеспечению режима коммерческой тайны, действий третьих лиц или непреодолимой силы.

Трудовым договором с руководителем организации должны предусматриваться его обязанности по обеспечению охраны конфиденциальности, составляющей коммерческую тайну информации, обладателем которой являются организация и ее контрагенты, и ответственность за обеспечение охраны конфиденциальности этой информации.

Руководитель организации возмещает организации убытки, причиненные его виновными действиями в связи с нарушением законодательства Российской Федерации о коммерческой тайне. При этом убытки определяются в соответствии с гражданским законодательством (ст. 15 Гражданского кодекс Российской Федерации (части первой) от 30.11.1994 № 51-ФЗ).

Работник имеет право обжаловать в судебном порядке незаконное установление режима коммерческой тайны в отношении информации, к которой он получил доступ в связи с исполнением трудовых обязанностей.

Работник, который в связи с исполнением трудовых обязанностей получил доступ к информации, составляющей коммерческую тайну, обладателями которой являются работодатель и его контрагенты, в случае умышленного или неосторожного разглашения этой информации при отсутствии в действиях такого работника состава преступления несет дисциплинарную ответственность в соответствии с законодательством Российской Федерации.

Органы государственной власти, иные государственные органы, органы местного самоуправления, получившие доступ к информации, составляющей коммерческую тайну, несут перед обладателем информации, составляющей коммерческую тайну, гражданско-правовую ответственность за разглашение или незаконное использование этой информации их должностными лицами, государственными или муниципальными служащими указанных органов, которым она стала известна в связи с выполнением ими должностных (служебных) обязанностей.

Нарушение Федерального закона «О коммерческой тайне» влечет за собой дисциплинарную, гражданско-правовую, административную или уголовную ответственность в соответствии с законодательством Российской Федерации (табл. 7).

Таблица 7

Меры уголовной и административной ответственности за нарушение законодательства о коммерческой тайне

Уголовная ответственность (Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ)	
Статья 183. Незаконные Получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну	1. Собирание сведений, составляющих коммерческую, налоговую или банковскую тайну, путем похищения документов, обмана, шантажа, принуждения, подкупа или угроз, а равно иным незаконным способом, – *наказывается штрафом в размере до пятисот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до одного года, либо исправительными работами на срок до одного года, либо принудительными работами на срок до двух лет, либо лишением свободы на тот же срок.*

Продолжение табл. 7

Уголовная ответственность (Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ)	
Статья 183. Незаконные Получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну	2. Незаконные разглашение или использование сведений, составляющих коммерческую, налоговую или банковскую тайну, без согласия их владельца лицом, которому она была доверена или стала известна по службе или работе, – *наказываются штрафом в размере до одного миллиона рублей или в размере заработной платы или иного дохода осужденного за период до двух лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет, либо исправительными работами на срок до двух лет, либо принудительными работами на срок до четырех лет, либо лишением свободы на тот же срок.* 3. Те же деяния, совершенные группой лиц по предварительному сговору или организованной группой, а равно причинившие крупный ущерб или совершенные из корыстной заинтересованности, – *наказываются штрафом в размере до одного миллиона пятисот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до трех лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет либо принудительными работами на срок до пяти лет, либо лишением свободы на тот же срок.* 4. Деяния, предусмотренные частями второй или третьей настоящей статьи, повлекшие тяжкие последствия, – *наказываются принудительными работами на срок до пяти лет либо лишением свободы на срок до семи лет*
Административная ответственность (Кодекс Российской Федерации об административных правонарушениях от 30.12.2001 № 195-ФЗ)	
Статья 13.14. Разглашение информации с ограниченным доступом	Разглашение информации, доступ к которой ограничен федеральным законом (за исключением случаев, если разглашение такой информации влечет уголовную ответственность), лицом, получившим доступ к такой информации в связи с исполнением служебных или профессиональных обязанностей, – *влечет наложение административного штрафа на граждан в размере от пяти тысяч до десяти тысяч рублей; на должностных лиц – от сорока тысяч до пятидесяти тысяч рублей или дисквалификацию на срок до трех лет; на юридических лиц – от ста тысяч до двухсот тысяч рублей*

Продолжение табл. 7

Административная ответственность (Кодекс Российской Федерации об административных правонарушениях от 30.12.2001 № 195-ФЗ)	
Статья 13.14.1. Незаконное получение информации с ограниченным доступом	Получение информации любым незаконным способом, доступ к которой ограничен федеральным законом, за исключением случаев, предусмотренных ст. 5.53, ч 1 и 2 ст. 13.11, ст. 14.29, ч 5 ст. 15.19, ч 2 ст. 17.13 КоАП РФ, если эти действия не содержат признаков уголовно наказуемого деяния, – *влечет наложение административного штрафа на граждан в размере от пяти тысяч до десяти тысяч рублей; на должностных лиц – от сорока тысяч до пятидесяти тысяч рублей или дисквалификацию на срок до трех лет; на юридических лиц – от ста тысяч до двухсот тысяч рублей*
Дисциплинарная ответственность (Трудовой кодекс Российской Федерации от 30.12.2001 № 197-ФЗ)	
Статья 81. Расторжение трудового договора по инициативе работодателя	Трудовой договор может быть расторгнут работодателем в случаях: ... ... в) разглашения охраняемой законом тайны (государственной, коммерческой, служебной и иной), ставшей известной работнику в связи с исполнением им трудовых обязанностей, в том числе разглашения персональных данных другого работника
Статья 192. Дисциплинарные взыскания	За совершение дисциплинарного проступка, то есть неисполнение или ненадлежащее исполнение работником по его вине возложенных на него трудовых обязанностей, работодатель имеет право применить следующие дисциплинарные взыскания: 1) замечание; 2) выговор; 3) увольнение по соответствующим основаниям

Окончание табл. 7

Гражданско-правовая ответственность Гражданский кодекс Российской Федерации (часть первая) от 30.11.1994 № 51-ФЗ; Гражданский кодекс Российской Федерации (часть четвертая) от 18.12.2006 № 230-ФЗ	
Статья 15. Возмещение убытков	1. Лицо, право которого нарушено, может требовать полного возмещения причиненных ему убытков, если законом или договором не предусмотрено возмещение убытков в меньшем размере. 2. Под убытками понимаются расходы, которые лицо, чье право нарушено, произвело или должно будет произвести для восстановления нарушенного права, утрата или повреждение его имущества (реальный ущерб), а также неполученные доходы, которые это лицо получило бы при обычных условиях гражданского оборота, если бы его право не было нарушено (упущенная выгода). Если лицо, нарушившее право, получило вследствие этого доходы, лицо, право которого нарушено, вправе требовать возмещения наряду с другими убытками упущенной выгоды в размере не меньшем, чем такие доходы
Статья 1472. Ответственность за нарушение исключительного права на секрет производства	1. Нарушитель исключительного права на секрет производства, в том числе лицо, которое неправомерно получило сведения, составляющие секрет производства, и разгласило или использовало эти сведения, а также лицо, обязанное сохранять конфиденциальность секрета производства в соответствии с п. 2 ст. 1468, п. 3 ст. 1469 или п. 2 ст. 1470 ГКРФ, обязано возместить убытки, причиненные нарушением исключительного права на секрет производства, если иная ответственность не предусмотрена законом или договором с этим лицом. 2. Лицо, которое использовало секрет производства и не знало и не должно было знать о том, что его использование незаконно, в том числе в связи с тем, что оно получило доступ к секрету производства случайно или по ошибке, не несет ответственность в соответствии с п. 1 данной статьи

Персональные данные

Персональные данные → - любая информация, относящаяся к прямо или косвенно определенному, или определяемому физическому лицу (субъекту персональных данных)
(ст. 3 Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных»)

Принципы обработки персональных данных

- Обработка персональных данных должна осуществляться на законной и справедливой основе
- Обработка персональных данных должна ограничиваться достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных
- Не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой
- Обработке подлежат только персональные данные, которые отвечают целям их обработки
- Содержание и объем обрабатываемых персональных данных должны соответствовать заявленным целям обработки.
- При обработке персональных данных должны быть обеспечены точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных
- Хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом или договором
- Обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом

Обработка персональных данных допускается в следующих случаях:

– обработка персональных данных осуществляется с согласия субъекта персональных данных на обработку его персональных данных;

– обработка персональных данных необходима для достижения целей, предусмотренных международным договором Российской Федерации или законом, для осуществления и выполнения возложенных законодательством Российской Федерации на оператора функций, полномочий и обязанностей;

– обработка персональных данных осуществляется в связи с участием лица в конституционном, гражданском, административном, уголовном судопроизводстве, судопроизводстве в арбитражных судах;

– обработка персональных данных необходима для исполнения судебного акта, акта другого органа или должностного лица, подлежащих исполнению в соответствии с законодательством Российской Федерации об исполнительном производстве;

– обработка персональных данных необходима для исполнения полномочий федеральных органов исполнительной власти, органов государственных внебюджетных фондов, исполнительных органов государственной власти субъектов Российской Федерации, органов местного самоуправления и функций организаций, участвующих в предоставлении соответственно государственных и муниципальных услуг, предусмотренных Федеральным законом от 27.07.2010 № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг», включая регистрацию субъекта персональных данных на едином портале государственных и муниципальных услуг и (или) региональных порталах государственных и муниципальных услуг;

– обработка персональных данных необходима для исполнения договора, стороной которого либо выгодоприобретателем или поручителем является субъект персональных данных, а также для заключения договора по инициативе субъекта персональных данных или договора, по которому субъект персональных данных будет являться выгодоприобретателем или поручителем. Заключаемый с субъектом персональных данных договор не может содержать положения, ограничивающие права и свободы субъекта персональных данных, устанавливающие случаи обработки персональных данных несовершеннолетних, если иное не предусмотрено законодательством Российской Федерации,

а также положения, допускающие в качестве условия заключения договора бездействие субъекта персональных данных;

– обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных, если получение согласия субъекта персональных данных невозможно;

– обработка персональных данных необходима для осуществления прав и законных интересов оператора или третьих лиц, в том числе в случаях, предусмотренных Федеральным законом от 03.07.2016 № 230-ФЗ «О защите прав и законных интересов физических лиц при осуществлении деятельности по возврату просроченной задолженности и о внесении изменений в Федеральный закон «О микрофинансовой деятельности и микрофинансовых организациях», либо для достижения общественно значимых целей при условии, что при этом не нарушаются права и свободы субъекта персональных данных;

– обработка персональных данных необходима для осуществления профессиональной деятельности журналиста и (или) законной деятельности средства массовой информации либо научной, литературной или иной творческой деятельности при условии, что при этом не нарушаются права и законные интересы субъекта персональных данных;

– обработка персональных данных осуществляется в статистических или иных исследовательских целях, за исключением целей, указанных в ст. 15 Федерального закона «О персональных данных», при условии обязательного обезличивания персональных данных;

– обработка персональных данных, полученных в результате обезличивания персональных данных, осуществляется в целях повышения эффективности государственного или муниципального управления;

– осуществляется обработка персональных данных, подлежащих опубликованию или обязательному раскрытию в соответствии с федеральным законом.

Оператор вправе поручить обработку персональных данных другому лицу с согласия субъекта персональных данных, если иное не предусмотрено федеральным законом, на основании заключаемого с этим лицом договора, в том числе государственного или муниципального контракта, либо путем принятия государственным органом или муниципальным органом соответствующего акта.

Лицо, осуществляющее обработку персональных данных по поручению оператора, обязано соблюдать принципы и правила обработки

персональных данных, предусмотренные Федеральным законом «О персональных данных», соблюдать конфиденциальность персональных данных, принимать необходимые меры, направленные на обеспечение выполнения обязанностей, предусмотренных данным законом.

Лицо, осуществляющее обработку персональных данных по поручению оператора, не обязано получать согласие субъекта персональных данных на обработку его персональных данных.

В случае, если оператор поручает обработку персональных данных другому лицу, ответственность перед субъектом персональных данных за действия указанного лица несет оператор. Лицо, осуществляющее обработку персональных данных по поручению оператора, несет ответственность перед оператором.

В случае, если оператор поручает обработку персональных данных иностранному физическому лицу или иностранному юридическому лицу, ответственность перед субъектом персональных данных за действия указанных лиц несет оператор и лицо, осуществляющее обработку персональных данных по поручению оператора.

Операторы и иные лица, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.

В соответствии со ст. 8 Федерального закона «О персональных данных», в целях информационного обеспечения могут создаваться общедоступные источники персональных данных (в том числе справочники, адресные книги).

В общедоступные источники персональных данных с письменного согласия субъекта персональных данных могут включаться его фамилия, имя, отчество, год и место рождения, адрес, абонентский номер, сведения о профессии и иные персональные данные, сообщаемые 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.

Операторы и иные лица, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.

Субъект персональных данных принимает решение о предоставлении его персональных данных и дает согласие на их обработку свободно, своей волей и в своем интересе.

Согласие на обработку персональных данных может быть дано субъектом персональных данных или его представителем в любой позволяющей подтвердить факт его получения форме, если иное не установлено федеральным законом.

Согласие на обработку персональных данных может быть отозвано субъектом персональных данных.

В случаях, предусмотренных федеральным законом, обработка персональных данных осуществляется только с согласия в письменной форме субъекта персональных данных.

В соответствии со ст. 11 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность (биометрические персональные данные) и которые используются оператором для установления личности субъекта персональных данных, могут обрабатываться только при наличии согласия в письменной форме субъекта персональных данных, за исключением случаев, установленных законом.

Государственные органы, муниципальные органы создают в пределах своих полномочий, установленных в соответствии с федеральными законами, государственные или муниципальные информационные системы персональных данных.

Права и свободы человека и гражданина не могут быть ограничены по мотивам, связанным с использованием различных способов обработки персональных данных или обозначения принадлежности персональных данных, содержащихся в государственных или муниципальных информационных системах персональных данных, конкретному субъекту персональных данных.

Не допускается использование оскорбляющих чувства граждан или унижающих человеческое достоинство способов обозначения принадлежности персональных данных, содержащихся в государственных или муниципальных информационных системах персональных данных, конкретному субъекту персональных данных.

Оператор при обработке персональных данных обязан принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения,

блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

Меры обеспечения безопасности персональных данных

- Определение угроз безопасности персональных данных при их обработке в информационных системах персональных данных
- Применение организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных
- Применение прошедших в установленном порядке процедуру оценки соответствия средств защиты информации
- Применение для уничтожения персональных данных, прошедших в установленном порядке процедуру оценки соответствия средств защиты информации, в составе которых реализована функция уничтожения информации
- Оценка эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных
- Учет машинных носителей персональных данных
- Обнаружение фактов несанкционированного доступа к персональным данным и принятие мер, в том числе мер по обнаружению, предупреждению и ликвидации последствий компьютерных атак
- Восстановление персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним
- Установление правил доступа к персональным данным, обрабатываемым в информационной системе, а также обеспечение регистрации и учета всех действий, совершаемых с персональными данными
- Контроль за принимаемыми мерами по обеспечению безопасности персональных данных и уровнем защищенности информационных систем персональных данных

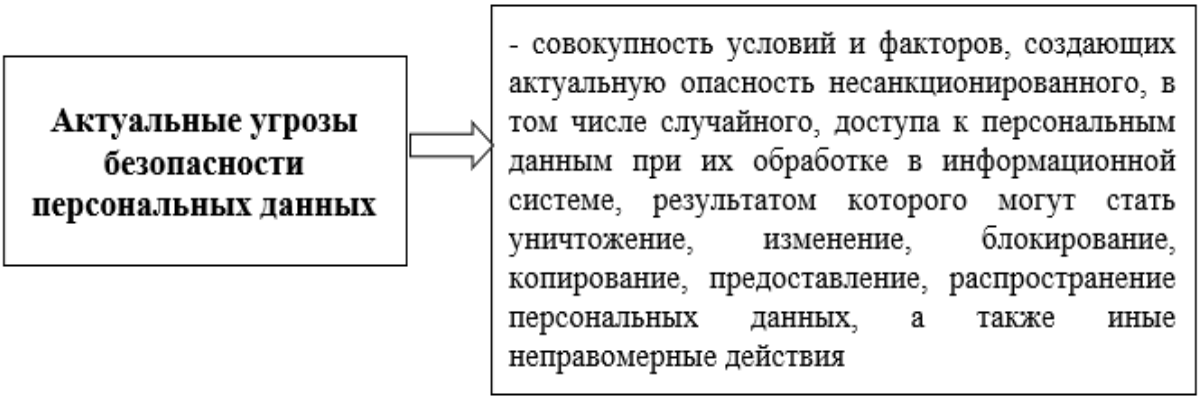
Правительство РФ с учетом возможного вреда субъекту персональных данных, объема и содержания обрабатываемых персональных

данных, вида деятельности, при осуществлении которого обрабатываются персональные данные, актуальности угроз безопасности персональных данных устанавливает:

1) уровни защищенности персональных данных при их обработке в информационных системах персональных данных в зависимости от угроз безопасности этим данным (Постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»);

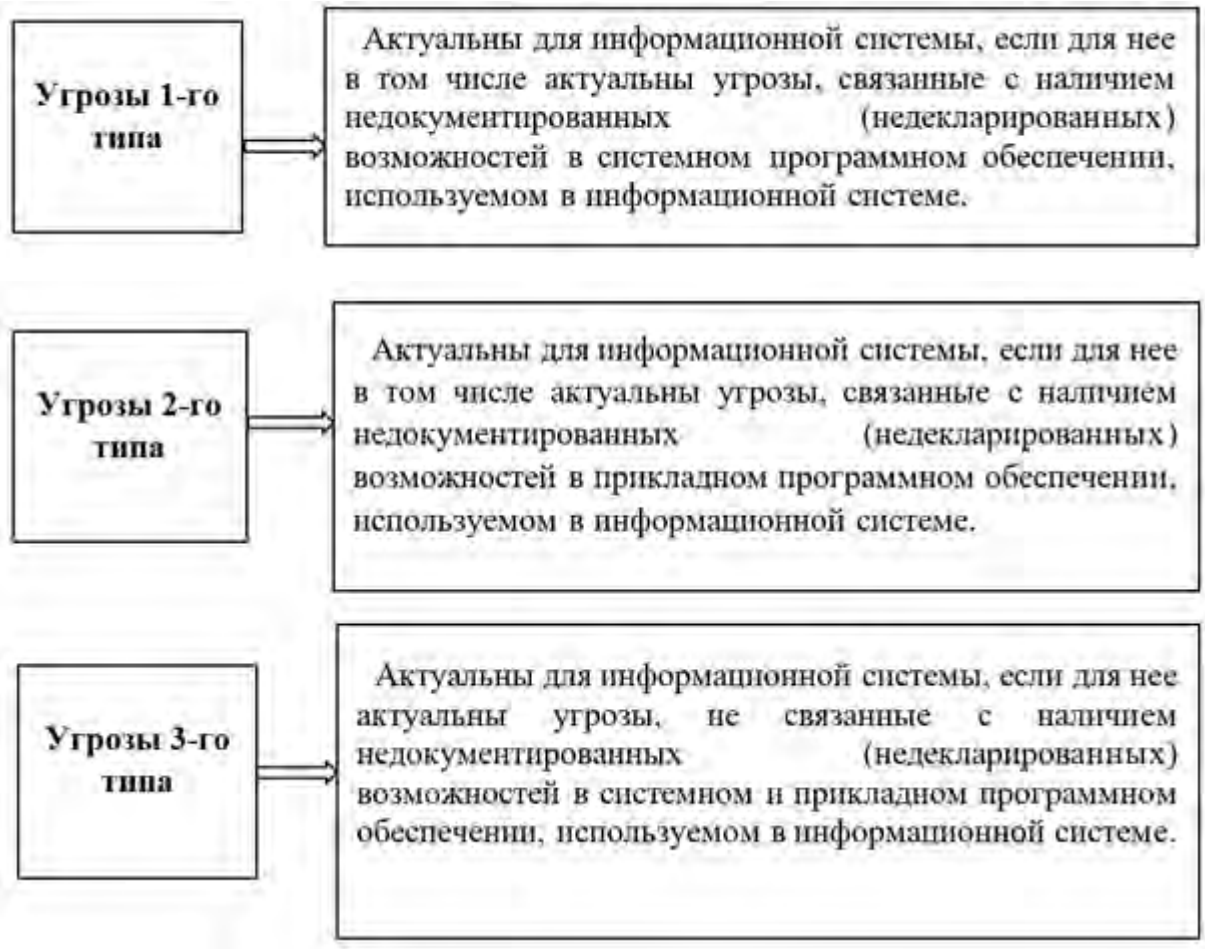
2) требования к защите персональных данных при их обработке в информационных системах персональных данных, исполнение которых обеспечивает установленные уровни защищенности персональных данных;

3) Требования к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных (Постановление Правительства РФ от 06.07.2008 № 512 «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных»).



Определение типа угроз безопасности персональных данных, актуальных для информационной системы, производится оператором с учетом оценки возможного вреда, проведенной во исполнение п. 5 ч. 1 ст. 18.1 Федерального закона «О персональных данных», и в соответствии с нормативными правовыми актами, принятыми во исполнение части 5 статьи 19 Федерального закона «О персональных данных».

Уровни актуальных угроз безопасности



В соответствии с Постановлением Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», при обработке персональных данных в информационных системах устанавливаются 4-го уровня защищенности персональных данных (табл. 8).

Таблица 8

Обеспечение различных уровней защищенности персональных данных

Необходимость обеспечения 1-го уровня защищенности персональных данных при их обработке в информационной системе устанавливается при наличии хотя бы одного из следующих условий:
– для информационной системы актуальны угрозы 1-го типа, и информационная система обрабатывает либо специальные категории персональных данных, либо биометрические персональные данные, либо иные категории персональных данных;

Продолжение таб. 8

– для информационной системы актуальны угрозы 2-го типа, и информационная система обрабатывает специальные категории персональных данных более чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора
Необходимость обеспечения 2-го уровня защищенности персональных данных при их обработке в информационной системе устанавливается при наличии хотя бы одного из следующих условий:
– для информационной системы актуальны угрозы 1-го типа, и информационная система обрабатывает общедоступные персональные данные; – для информационной системы актуальны угрозы 2-го типа, и информационная система обрабатывает специальные категории персональных данных сотрудников оператора или специальные категории персональных данных менее чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора; – для информационной системы актуальны угрозы 2-го типа, и информационная система обрабатывает биометрические персональные данные; – для информационной системы актуальны угрозы 2-го типа, и информационная система обрабатывает общедоступные персональные данные более чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора; – для информационной системы актуальны угрозы 2-го типа, и информационная система обрабатывает иные категории персональных данных более чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора; – для информационной системы актуальны угрозы 3-го типа, и информационная система обрабатывает специальные категории персональных данных более чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора
Необходимость обеспечения 3-го уровня защищенности персональных данных при их обработке в информационной системе устанавливается при наличии хотя бы одного из следующих условий:
– для информационной системы актуальны угрозы 2-го типа, и информационная система обрабатывает общедоступные персональные данные сотрудников оператора или общедоступные персональные данные менее чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора; – для информационной системы актуальны угрозы 2-го типа, и информационная система обрабатывает иные категории персональных данных сотрудников оператора или иные категории персональных данных менее чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора;

Окончание табл. 8

– для информационной системы актуальны угрозы 3-го типа, и информационная система обрабатывает специальные категории персональных данных сотрудников оператора или специальные категории персональных данных менее чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора; – для информационной системы актуальны угрозы 3-го типа, и информационная система обрабатывает биометрические персональные данные; – для информационной системы актуальны угрозы 3-го типа, и информационная система обрабатывает иные категории персональных данных более чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора
Необходимость обеспечения 4-го уровня защищенности персональных данных при их обработке в информационной системе устанавливается при наличии хотя бы одного из следующих условий:
– для информационной системы актуальны угрозы 3-го типа, и информационная система обрабатывает общедоступные персональные данные; – для информационной системы актуальны угрозы 3-го типа, и информационная система обрабатывает иные категории персональных данных сотрудников оператора или иные категории персональных данных менее чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора

Контроль за выполнением настоящих требований организуется и проводится оператором (уполномоченным лицом) самостоятельно и (или) с привлечением на договорной основе юридических лиц и индивидуальных предпринимателей, имеющих лицензию на осуществление деятельности по технической защите конфиденциальной информации.

Указанный контроль проводится не реже 1 раза в 3 года в сроки, определяемые оператором (уполномоченным лицом).

Федеральные органы исполнительной власти, осуществляющие функции по выработке государственной политики и нормативно-правовому регулированию в установленной сфере деятельности, органы государственной власти субъектов Российской Федерации, Банк России, органы государственных внебюджетных фондов, иные государственные органы в пределах своих полномочий принимают нормативные правовые акты, в которых определяют угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности, с учетом содержания персональных данных, характера и способов их обработки.

Уполномоченным органом по защите прав субъектов персональных данных является федеральный орган исполнительной власти, осуществляющий самостоятельно функции по контролю и надзору за соответствием обработки персональных данных требованиям законодательства Российской Федерации в области персональных данных (Постановление Правительства РФ от 16.03.2009 № 228 «О Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций»).

Уполномоченный орган по защите прав субъектов персональных данных рассматривает обращения субъекта персональных данных о соответствии содержания персональных данных и способов их обработки целям их обработки и принимает соответствующее решение.

В отношении персональных данных, ставших известными уполномоченному органу по защите прав субъектов персональных данных в ходе осуществления им своей деятельности, должна обеспечиваться конфиденциальность персональных данных.

Решения уполномоченного органа по защите прав субъектов персональных данных могут быть обжалованы в судебном порядке.

Информация о компьютерных инцидентах, повлекших неправомерную или случайную передачу (предоставление, распространение, доступ) персональных данных, в порядке, установленном совместно федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, и уполномоченным органом по защите прав субъектов персональных данных, передается в федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности.

В соответствии со ст. 23.1 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», федеральный государственный контроль (надзор) за обработкой персональных данных осуществляется федеральным органом исполнительной власти, осуществляющим функции по контролю (надзору) за соответствием обработки персональных данных требованиям законодательства Российской Федерации в области персональных данных.

Предметом федерального государственного контроля (надзора) за обработкой персональных данных является соблюдение операторами обязательных требований в области персональных данных, установленных настоящим Федеральным законом и принимаемыми в соответствии с ним иными нормативными правовыми актами Российской Федерации.

Федеральный государственный контроль (надзор) за обработкой персональных данных осуществляется в соответствии с Федеральным законом от 31.07.2020 № 248-ФЗ «О государственном контроле (надзоре) и муниципальном контроле в Российской Федерации» (за исключением контрольных (надзорных) мероприятий, проводимых без взаимодействия с контролируемым лицом).

Сведения о причинении вреда (ущерба) или об угрозе причинения вреда (ущерба) охраняемым законом ценностям, выявленные в ходе проведения мероприятий без взаимодействия с контролируемым лицом, являются основанием для принятия решения о проведении контрольного (надзорного) мероприятия в соответствии со ст. 60 Федерального закона от 31 июля 2020 № 248-ФЗ «О государственном контроле (надзоре) и муниципальном контроле в Российской Федерации».

Положение о федеральном государственном контроле (надзоре) за обработкой персональных данных, в том числе порядок организации и осуществления контрольных (надзорных) мероприятий, проводимых без взаимодействия с контролируемым лицом, утверждается Правительством Российской Федерации (Постановление Правительства РФ от 29.06.2021 № 1046 «О федеральном государственном контроле (надзоре) за обработкой персональных данных»).

Меры ответственности за нарушение законодательства представлены в табл. 9.

Таблица 9

Меры ответственности за нарушение законодательства о персональных данных

Уголовная ответственность (Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ)	
Статья 137. Нарушение неприкосновенности частной жизни	1. Незаконное собирание или распространение сведений о частной жизни лица, составляющих его личную или семейную тайну, без его согласия либо распространение этих сведений в публичном выступлении, публично демонстрирующемся произведении или средствах массовой информации, – **наказываются штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев, либо обязательными работами на срок до трехсот шестидесяти часов, либо исправительными работами на срок до одного года, либо принудительными работами на срок до двух лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех**

Продолжение табл. 9

Уголовная ответственность (Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ)	
	лет или без такового, либо арестом на срок до четырех месяцев, либо лишением свободы на срок до двух лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет. 2. Те же деяния, совершенные лицом с использованием своего служебного положения, – **наказываются штрафом в размере от ста тысяч до трехсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от одного года до двух лет, либо лишением права занимать определенные должности или заниматься определенной деятельностью на срок от двух до пяти лет, либо принудительными работами на срок до четырех лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до пяти лет или без такового, либо арестом на срок до шести месяцев, либо лишением свободы на срок до четырех лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до пяти лет** 3. Незаконное распространение в публичном выступлении, публично демонстрирующемся произведении, средствах массовой информации или информационно-телекоммуникационных сетях информации, указывающей на личность несовершеннолетнего потерпевшего, не достигшего шестнадцатилетнего возраста, по уголовному делу, либо информации, содержащей описание полученных им в связи с преступлением физических или нравственных страданий, повлекшее причинение вреда здоровью несовершеннолетнего, или психическое расстройство несовершеннолетнего, или иные тяжкие последствия, – **наказывается штрафом в размере от ста пятидесяти тысяч до трехсот пятидесяти тысяч рублей или в размере заработной платы или иного дохода осужденного за период от восемнадцати месяцев до трех лет, либо лишением права занимать определенные должности или заниматься определенной деятельностью на срок от трех до пяти лет, либо принудительными работами на срок до пяти лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до шести лет или без такового, либо арестом на срок до шести месяцев, либо лишением свободы на срок до пяти лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до шести лет**

Продолжение табл. 9

Уголовная ответственность (Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ)	
Статья 140. Отказ в предоставлении гражданину информации	Неправомерный отказ должностного лица в предоставлении собранных в установленном порядке документов и материалов, непосредственно затрагивающих права и свободы гражданина, либо предоставление гражданину неполной или заведомо ложной информации, если эти деяния причинили вред правам и законным интересам граждан, – **наказываются штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев либо лишением права занимать определенные должности или заниматься определенной деятельностью на срок от двух до пяти лет**
Статья 272. Неправомерный доступ к компьютерной информации	1. Неправомерный доступ к охраняемой законом компьютерной информации, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование компьютерной информации, – **наказывается штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев, либо исправительными работами на срок до одного года, либо ограничением свободы на срок до двух лет, либо принудительными работами на срок до двух лет, либо лишением свободы на тот же срок** 2. То же деяние, причинившее крупный ущерб или совершенное из корыстной заинтересованности, – **наказывается штрафом в размере от ста тысяч до трехсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от одного года до двух лет, либо исправительными работами на срок от одного года до двух лет, либо ограничением свободы на срок до четырех лет, либо принудительными работами на срок до четырех лет, либо лишением свободы на тот же срок**. 3. Деяния, предусмотренные частями первой или второй настоящей статьи, совершенные группой лиц по предварительному сговору или организованной группой либо лицом с использованием своего служебного положения, – **наказываются штрафом в размере до пятисот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до трех лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет, либо ограничением свободы на срок до четырех лет, либо принудительными работами на срок до пяти лет, либо лишением свободы на тот же срок**. 4. Деяния, предусмотренные частями первой, второй или третьей настоящей статьи, если они повлекли тяжкие последствия или создали угрозу их наступления, – **наказываются лишением свободы на срок до семи лет**

Продолжение табл. 9

Административная ответственность (Кодекс Российской Федерации об административных правонарушениях от 30.12.2001 № 195-ФЗ)	
Статья 5.39. Отказ в предоставлении информации	Неправомерный отказ в предоставлении гражданину, в том числе адвокату в связи с поступившим от него адвокатским запросом, и (или) организации информации, предоставление которой предусмотрено федеральными законами, несвоевременное ее предоставление либо предоставление заведомо недостоверной информации – **влечет наложение административного штрафа на должностных лиц в размере от пяти тысяч до десяти тысяч рублей**
Статья 13.11. Нарушение законодательства Российской Федерации в области персональных данных	Обработка персональных данных в случаях, не предусмотренных законодательством Российской Федерации в области персональных данных, либо обработка персональных данных, несовместимая с целями сбора персональных данных, за исключением случаев, предусмотренных частью 2 настоящей статьи и статьей 17.13 КоАП РФ, если эти действия не содержат уголовно наказуемого деяния, – **влечет наложение административного штрафа на граждан в размере от двух тысяч до шести тысяч рублей; на должностных лиц – от десяти тысяч до двадцати тысяч рублей; на юридических лиц – от шестидесяти тысяч до ста тысяч рублей.** 2. Обработка персональных данных без согласия в письменной форме субъекта персональных данных на обработку его персональных данных в случаях, когда такое согласие должно быть получено в соответствии с законодательством Российской Федерации в области персональных данных, за исключением случаев, предусмотренных ст. 17.13 КоАП РФ, если эти действия не содержат уголовно наказуемого деяния, либо обработка персональных данных с нарушением установленных законодательством Российской Федерации в области персональных данных требований к составу сведений, включаемых в согласие в письменной форме субъекта персональных данных на обработку его персональных данных, – **влечет наложение административного штрафа на граждан в размере от десяти тысяч до пятнадцати тысяч рублей; на должностных лиц – от ста тысяч до трехсот тысяч рублей; на юридических лиц – от трехсот тысяч до семисот тысяч рублей.** 3. Невыполнение оператором предусмотренной законодательством Российской Федерации в области персональных данных обязанности по опубликованию или обеспечению иным образом неограниченного доступа к документу, определяющему политику оператора в отношении обработки персональных данных, или сведениям о реализуемых требованиях

Продолжение табл. 9

Административная ответственность (Кодекс Российской Федерации об административных правонарушениях от 30.12.2001 № 195-ФЗ)	
	к защите персональных данных – **влечет наложение административного штрафа на граждан в размере от одной тысячи пятисот до трех тысяч рублей; на должностных лиц – от шести тысяч до двенадцати тысяч рублей; на индивидуальных предпринимателей – от десяти тысяч до двадцати тысяч рублей; на юридических лиц – от тридцати тысяч до шестидесяти тысяч рублей.** 4. Невыполнение оператором предусмотренной законодательством Российской Федерации в области персональных данных обязанности по предоставлению субъекту персональных данных информации, касающейся обработки его персональных данных, – **влечет наложение административного штрафа на граждан в размере от двух тысяч до четырех тысяч рублей; на должностных лиц – от восьми тысяч до двенадцати тысяч рублей; на индивидуальных предпринимателей – от двадцати тысяч до тридцати тысяч рублей; на юридических лиц – от сорока тысяч до восьмидесяти тысяч рублей.** 5. Невыполнение оператором в сроки, установленные законодательством Российской Федерации в области персональных данных, требования субъекта персональных данных или его представителя либо уполномоченного органа по защите прав субъектов персональных данных об уточнении персональных данных, их блокировании или уничтожении в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, – **влечет наложение административного штрафа на граждан в размере от двух тысяч до четырех тысяч рублей; на должностных лиц – от восьми тысяч до двадцати тысяч рублей; на индивидуальных предпринимателей – от двадцати тысяч до сорока тысяч рублей; на юридических лиц – от пятидесяти тысяч до девяноста тысяч рублей.** 6. Невыполнение оператором при обработке персональных данных без использования средств автоматизации обязанности по соблюдению условий, обеспечивающих в соответствии с законодательством Российской Федерации в области персональных данных сохранность персональных данных при хранении материальных носителей персональных данных и исключающих несанкционированный к ним доступ, если это повлекло неправомерный или случайный доступ к персональным данным, их уничтожение, изменение, блокирование, копирование, предоставление, распространение либо иные неправомерные действия в отношении персональных данных, при отсутствии признаков уголовно наказуемого деяния,

Продолжение табл. 9

Административная ответственность (Кодекс Российской Федерации об административных правонарушениях от 30.12.2001 № 195-ФЗ)	
	– **влечет наложение административного штрафа на граждан в размере от одной тысячи пятисот до четырех тысяч рублей; на должностных лиц – от восьми тысяч до двадцати тысяч рублей; на индивидуальных предпринимателей – от двадцати тысяч до сорока тысяч рублей; на юридических лиц – от пятидесяти тысяч до ста тысяч рублей.** 7. Невыполнение оператором, являющимся государственным или муниципальным органом, предусмотренной законодательством Российской Федерации в области персональных данных обязанности по обезличиванию персональных данных, либо несоблюдение установленных требований или методов по обезличиванию персональных данных, – **влечет наложение административного штрафа на должностных лиц в размере от шести тысяч до двенадцати тысяч рублей.** 8. Невыполнение оператором при сборе персональных данных, в том числе посредством информационно-телекоммуникационной сети «Интернет», предусмотренной законодательством Российской Федерации в области персональных данных обязанности по обеспечению записи, систематизации, накопления, хранения, уточнения (обновления, изменения) или извлечения персональных данных граждан Российской Федерации с использованием баз данных, находящихся на территории Российской Федерации, – **влечет наложение административного штрафа на граждан в размере от тридцати тысяч до пятидесяти тысяч рублей; на должностных лиц – от ста тысяч до двухсот тысяч рублей; на юридических лиц – от одного миллиона до шести миллионов рублей**
Статья 13.12. Нарушение правил защиты информации	1. Нарушение условий, предусмотренных лицензией на осуществление деятельности в области защиты информации (за исключением информации, составляющей государственную тайну), – **влечет наложение административного штрафа на граждан в размере от одной тысячи до одной тысячи пятисот рублей; на должностных лиц – от одной тысячи пятисот до двух тысяч пятисот рублей; на юридических лиц – от пятнадцати тысяч до двадцати тысяч рублей.** 2. Использование несертифицированных информационных систем, баз и банков данных, а также несертифицированных средств защиты информации, если они подлежат обязательной сертификации (за исключением средств защиты информации, составляющей государственную тайну), – **влечет наложение административного штрафа на граждан в размере от одной тысячи пятисот до двух тысяч пятисот рублей**

Продолжение табл. 9

Административная ответственность (Кодекс Российской Федерации об административных правонарушениях от 30.12.2001 № 195-ФЗ)	
	с конфискацией несертифицированных средств защиты информации или без таковой; на должностных лиц – от двух тысяч пятисот до трех тысяч рублей; на юридических лиц – от двадцати тысяч до двадцати пяти тысяч рублей с конфискацией несертифицированных средств защиты информации или без таковой. 3. Нарушение условий, предусмотренных лицензией на проведение работ, связанных с использованием и защитой информации, составляющей государственную тайну, созданием средств, предназначенных для защиты информации, составляющей государственную тайну, осуществлением мероприятий и (или) оказанием услуг по защите информации, составляющей государственную тайну, – **влечет наложение административного штрафа на должностных лиц в размере от двух тысяч до трех тысяч рублей; на юридических лиц – от двадцати тысяч до двадцати пяти тысяч рублей.** 4. Использование несертифицированных средств, предназначенных для защиты информации, составляющей государственную тайну, – **влечет наложение административного штрафа на должностных лиц в размере от трех тысяч до четырех тысяч рублей; на юридических лиц – от двадцати тысяч до тридцати тысяч рублей с конфискацией несертифицированных средств, предназначенных для защиты информации, составляющей государственную тайну, или без таковой.** 5. Грубое нарушение условий, предусмотренных лицензией на осуществление деятельности в области защиты информации (за исключением информации, составляющей государственную тайну), – **влечет наложение административного штрафа на лиц, осуществляющих предпринимательскую деятельность без образования юридического лица, в размере от двух тысяч до трех тысяч рублей или административное приостановление деятельности на срок до девяноста суток; на должностных лиц – от двух тысяч до трех тысяч рублей; на юридических лиц – от двадцати тысяч до двадцати пяти тысяч рублей или административное приостановление деятельности на срок до девяноста суток.** 6. Нарушение требований о защите информации (за исключением информации, составляющей государственную тайну), установленных федеральными законами и принятыми в соответствии с ними иными нормативными правовыми актами Российской Федерации, за исключением случаев, предусмотренных ч 1, 2 и 5 настоящей статьи, – **влечет наложение административного штрафа на граждан в размере от пятисот до одной тысячи рублей; на должностных лиц – от одной тысячи до двух тысяч рублей; на юридических лиц – от десяти тысяч до пятнадцати тысяч рублей.**

Продолжение табл. 9

Административная ответственность (Кодекс Российской Федерации об административных правонарушениях от 30.12.2001 № 195-ФЗ)	
	7. Нарушение требований о защите информации, составляющей государственную тайну, установленных федеральными законами и принятыми в соответствии с ними иными нормативными правовыми актами Российской Федерации, за исключением случаев, предусмотренных ч. 3 и 4 настоящей статьи, если такие действия (бездействие) не содержат уголовно наказуемого деяния, – **влечет наложение административного штрафа на граждан в размере от одной тысячи до двух тысяч рублей; на должностных лиц – от трех тысяч до четырех тысяч рублей; на юридических лиц – от пятнадцати тысяч до двадцати тысяч рублей**
Статья 13.13. Незаконная деятельность в области защиты информации	1. Занятие видами деятельности в области защиты информации (за исключением информации, составляющей государственную тайну) без получения в установленном порядке специального разрешения (лицензии), если такое разрешение (такая лицензия) в соответствии с федеральным законом обязательно (обязательна), – **влечет наложение административного штрафа на граждан в размере от пятисот до одной тысячи рублей с конфискацией средств защиты информации или без таковой; на должностных лиц – от двух тысяч до трех тысяч рублей с конфискацией средств защиты информации или без таковой; на юридических лиц – от десяти тысяч до двадцати тысяч рублей с конфискацией средств защиты информации или без таковой.** 2. Занятие видами деятельности, связанной с использованием и защитой информации, составляющей государственную тайну, созданием средств, предназначенных для защиты информации, составляющей государственную тайну, осуществлением мероприятий и (или) оказанием услуг по защите информации, составляющей государственную тайну, без лицензии, – **влечет наложение административного штрафа на должностных лиц в размере от четырех тысяч до пяти тысяч рублей; на юридических лиц – от тридцати тысяч до сорока тысяч рублей с конфискацией созданных без лицензии средств защиты информации, составляющей государственную тайну, или без таковой**

Продолжение табл. 9

Административная ответственность (Кодекс Российской Федерации об административных правонарушениях от 30.12.2001 № 195-ФЗ)	
Статья 13.14. Разглашение информации с ограниченным доступом	Разглашение информации, доступ к которой ограничен федеральным законом (за исключением случаев, если разглашение такой информации влечет уголовную ответственность), лицом, получившим доступ к такой информации в связи с исполнением служебных или профессиональных обязанностей, за исключением случаев, предусмотренных ч. 1 ст. 14.33 и ст. 17.13 КоАП РФ, – **влечет наложение административного штрафа на граждан в размере от пяти тысяч до десяти тысяч рублей; на должностных лиц – от сорока тысяч до пятидесяти тысяч рублей или дисквалификацию на срок до трех лет; на юридических лиц – от ста тысяч до двухсот тысяч рублей**
Статья 19.7. Непредставление сведений (информации)	Непредставление или несвоевременное представление в государственный орган (должностному лицу), орган (должностному лицу), осуществляющий (осуществляющему) государственный контроль (надзор), государственный финансовый контроль, организацию, уполномоченную в соответствии с федеральными законами на осуществление государственного надзора (должностному лицу), орган (должностному лицу), осуществляющий (осуществляющему) муниципальный контроль, муниципальный финансовый контроль, сведений (информации), представление которых предусмотрено законом и необходимо для осуществления этим органом (должностным лицом) его законной деятельности, либо представление в государственный орган (должностному лицу), орган (должностному лицу), осуществляющий (осуществляющему) государственный контроль (надзор), государственный финансовый контроль, организацию, уполномоченную в соответствии с федеральными законами на осуществление государственного надзора (должностному лицу), орган (должностному лицу), осуществляющий (осуществляющему) муниципальный контроль, муниципальный финансовый контроль, таких сведений (информации) в неполном объеме или в искаженном виде, – **влечет предупреждение или наложение административного штрафа на граждан в размере от ста до трехсот рублей; на должностных лиц – от трехсот до пятисот рублей; на юридических лиц – от трех тысяч до пяти тысяч рублей**

Окончание табл. 9

Дисциплинарная ответственность (Трудовой кодекс Российской Федерации от 30.12.2001 № 197-ФЗ)	
Статья 81. Расторжение трудового договора по инициативе работодателя	Трудовой договор может быть расторгнут работодателем в случаях: ... ... в) разглашения охраняемой законом тайны (государственной, коммерческой, служебной и иной), ставшей известной работнику в связи с исполнением им трудовых обязанностей, в том числе разглашения персональных данных другого работника
Статья 90. Ответственность за нарушение норм, регулирующих обработку и защиту персональных данных работника	Лица, виновные в нарушении положений законодательства Российской Федерации в области персональных данных при обработке персональных данных работника, привлекаются к дисциплинарной и материальной ответственности в порядке, установленном Трудовым кодексом РФ и иными федеральными законами, а также привлекаются к гражданско-правовой, административной и уголовной ответственности в порядке, установленном федеральными законами
Статья 192. Дисциплинарные взыскания	За совершение дисциплинарного проступка, то есть неисполнение или ненадлежащее исполнение работником по его вине возложенных на него трудовых обязанностей, работодатель имеет право применить следующие дисциплинарные взыскания: 1) замечание; 2) выговор; 3) увольнение по соответствующим основаниям

Моральный вред, причиненный субъекту персональных данных вследствие нарушения его прав, нарушения правил обработки персональных данных, установленных Федеральным законом «О персональных данных», а также требований к защите персональных данных (Постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»), подлежит возмещению в соответствии с § 4 Гражданского кодекса Российской Федерации (части второй) от 26.01.1996 № 14-ФЗ.

Возмещение морального вреда осуществляется независимо от возмещения имущественного вреда и понесенных субъектом персональных данных убытков.

ОБЕСПЕЧЕНИЕ ДОСТУПА К ИНФОРМАЦИИ О ДЕЯТЕЛЬНОСТИ ГОСУДАРСТВЕННЫХ ОРГАНОВ И ОРГАНОВ МЕСТНОГО УПРАВЛЕНИЯ

Информация о деятельности государственных органов и органов местного самоуправления → - информация (в том числе документированная), созданная в пределах своих полномочий государственными органами, их территориальными органами, органами местного самоуправления или организациями, подведомственными государственным органам, органам местного самоуправления, либо поступившая в указанные органы и организации (ст. 1 Федерального закона от 09.02.2009 № 8-ФЗ «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления»)

К информации о деятельности государственных органов относятся также законы и иные нормативные правовые акты, а к информации о деятельности органов местного самоуправления – муниципальные правовые акты, устанавливающие структуру, полномочия, порядок формирования и деятельности указанных органов.

Основные принципы обеспечения доступа к информации о деятельности государственных органов и органов местного самоуправления

- Открытость и доступность информации о деятельности государственных органов и органов местного самоуправления, за исключением случаев, предусмотренных федеральным законом
- Достоверность информации о деятельности государственных органов и органов местного самоуправления и своевременность ее предоставления
- Свобода поиска, получения, передачи и распространения информации о деятельности государственных органов и органов местного самоуправления любым законным способом
- Соблюдение прав граждан на неприкосновенность частной жизни, личную и семейную тайну, защиту их чести и деловой репутации, права организаций на защиту их деловой репутации при предоставлении информации о деятельности государственных органов и органов местного самоуправления

Доступ к информации о деятельности государственных органов и органов местного самоуправления ограничивается в случаях, если указанная информация отнесена в установленном федеральным законом порядке к сведениям, составляющим государственную или иную охраняемую законом тайну.

Способы обеспечения доступа к информации о деятельности государственных органов и органов местного самоуправления

- Обнародование (опубликование) государственными органами и органами местного самоуправления информации о своей деятельности в средствах массовой информации
- Размещение государственными органами, органами местного самоуправления и подведомственными организациями в сети «Интернет» информации
- Размещение государственными органами и органами местного самоуправления информации о своей деятельности в помещениях, занимаемых указанными органами, и в иных отведенных для этих целей местах
- Ознакомление пользователей информацией с информацией о деятельности государственных органов и органов местного самоуправления в помещениях, занимаемых указанными органами, а также через библиотечные и архивные фонды
- Предоставление пользователям информацией по их запросу информации о деятельности государственных органов и органов местного самоуправления
- Присутствие граждан (физических лиц), в том числе представителей организаций (юридических лиц), общественных объединений, государственных органов и органов местного самоуправления, на заседаниях коллегиальных государственных органов и коллегиальных органов местного самоуправления, а также на заседаниях коллегиальных органов государственных органов и коллегиальных органов местного самоуправления
- Другие способы, предусмотренные законами и (или) иными нормативными правовыми актами, а в отношении доступа к информации о деятельности органов местного самоуправления - также муниципальными правовыми актами.

Перечень сведений, относящихся к информации ограниченного доступа, а также порядок отнесения указанных сведений к информации ограниченного доступа устанавливается федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

Информация о деятельности государственных органов и органов местного самоуправления может предоставляться в устной форме и в виде документированной информации, в том числе в виде электронного документа.

Общедоступная информация о деятельности государственных органов и органов местного самоуправления предоставляется государственными органами и органами местного самоуправления неограниченному кругу лиц посредством ее размещения на официальных сайтах в форме открытых данных.

Информация о деятельности государственных органов и органов местного самоуправления в устной форме предоставляется пользователям информацией во время приема.

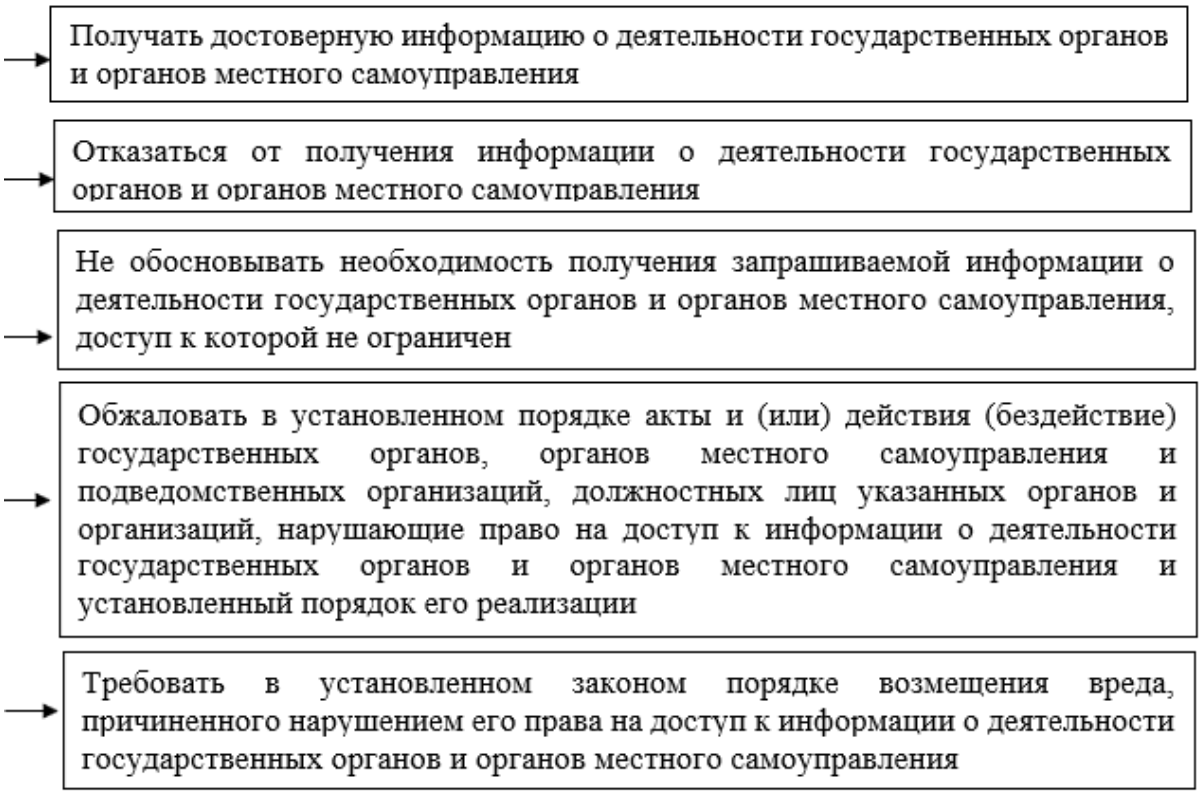
Указанная информация предоставляется также по телефонам справочных служб государственного органа, органа местного самоуправления либо по телефонам должностных лиц, уполномоченных государственным органом, органом местного самоуправления на ее предоставление.

Информация о деятельности государственных органов и органов местного самоуправления может быть передана по сетям связи общего пользования.

Правительство РФ определяет случаи, при которых доступ с использованием сети «Интернет» к информации, содержащейся в государственных и муниципальных информационных системах, предоставляется исключительно пользователям информации, прошедшим авторизацию в единой системе идентификации и аутентификации (Постановление Правительства РФ от 10.07.2013 № 584 «Об использовании федеральной государственной информационной системы «Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме»).

Доступ к информации о деятельности государственных органов и органов местного самоуправления обеспечивается в пределах своих полномочий государственными органами, органами местного самоуправления и подведомственными организациями.

Права пользователя информации о деятельности государственных органов и органов местного самоуправления



Права и обязанности указанных подразделений и должностных лиц устанавливаются регламентами государственных органов и (или) иными нормативными правовыми актами, регламентами органов местного самоуправления и (или) иными муниципальными правовыми актами, регулирующими деятельность соответствующих государственных органов, органов местного самоуправления.

Организация доступа к информации о деятельности государственных органов и органов местного самоуправления осуществляется с учетом требований Федерального закона «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления» в порядке, установленном государственными органами, органами местного самоуправления в пределах своих полномочий, а в отношении доступа к информации о деятельности судов в Российской Федерации – также с учетом требований Федерального закона от 22.12.2008 № 262-ФЗ «Об обеспечении доступа к информации о деятельности судов в Российской Федерации».

В соответствии со ст. 11 Федерального закона от 09.02.2009 № 8-ФЗ «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления» устанавливаются основные требования при обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления.

Основные требования к обеспечению доступа к информации о деятельности государственных органов и органов местного самоуправления

- Достоверность предоставляемой информации о деятельности государственных органов и органов местного самоуправления
- Соблюдение сроков и порядка предоставления информации о деятельности государственных органов и органов местного самоуправления
- Изъятие из предоставляемой информации о деятельности государственных органов и органов местного самоуправления сведений, относящихся к информации ограниченного доступа
- Учет расходов, связанных с обеспечением доступа к информации о деятельности государственных органов и органов местного самоуправления, при планировании бюджетного финансирования указанных органов
- Создание государственными органами, органами местного самоуправления и подведомственными организациями в пределах своих полномочий организационно-технических и других условий, необходимых для реализации права на доступ к информации о деятельности государственных органов и органов местного самоуправления, а также создание государственных и муниципальных информационных систем для обслуживания пользователей информацией

Информация о деятельности государственных органов и органов местного самоуправления, предоставляемая на бесплатной основе

- Передаваемая в устной форме
- Размещаемая государственным органом, органом местного самоуправления в сети «Интернет», а также в отведенных для размещения информации о деятельности государственных органов и органов местного самоуправления местах
- Затрагивающая права и установленные законодательством Российской Федерации обязанности заинтересованного пользователя информацией
- Иная установленная законом информация о деятельности государственных органов и органов местного самоуправления, а также иная установленная муниципальными правовыми актами информация о деятельности органов местного самоуправления

Плата за предоставление информации о деятельности государственных органов и органов местного самоуправления

⇩ Плата за предоставление информации о деятельности государственных органов и органов местного самоуправления взимается в случае ее предоставления по запросу, если объем запрашиваемой и полученной информации превышает определенный Правительством РФ объем информации, предоставляемой на бесплатной основе.

⇩ Оплата расходов на изготовление копий запрашиваемых документов и (или) материалов, а также расходы, связанные с их пересылкой по почте.

Решения и действия (бездействие) государственных органов и органов местного самоуправления, их должностных лиц, нарушающие право на доступ к информации о деятельности государственных органов и органов местного самоуправления, могут быть обжалованы в вышестоящий орган или вышестоящему должностному лицу либо в суд.

Если в результате неправомерного отказа в доступе к информации о деятельности государственных органов и органов местного самоуправления, либо несвоевременного ее предоставления, либо предоставления заведомо недостоверной или не соответствующей содержанию запроса информации пользователю информацией были причинены убытки, такие убытки подлежат возмещению в соответствии с гражданским законодательством Российской Федерации.

Контроль за обеспечением доступа к информации о деятельности государственных органов и органов местного самоуправления осуществляют руководители государственных органов и органов местного самоуправления. Порядок осуществления контроля за обеспечением доступа к информации о деятельности государственных органов и органов местного самоуправления устанавливается соответственно нормативными правовыми актами государственных органов, муниципальными правовыми актами.

Надзор за исполнением государственными органами, органами местного самоуправления, их должностными лицами настоящего Федерального закона осуществляют органы прокуратуры РФ в порядке, установленном Федеральным законом от 17.01.1992 № 2202-1 «О прокуратуре Российской Федерации».

Должностные лица государственных органов, органов местного самоуправления и подведомственных организаций, государственные и муниципальные служащие, работники подведомственных организаций, виновные в нарушении права на доступ к информации о деятельности государственных органов, органов местного самоуправления и подведомственных организаций, несут дисциплинарную, административную, гражданскую и уголовную ответственность в соответствии с законодательством Российской Федерации.

ПРАВОВОЕ РЕГУЛИРОВАНИЕ ОТНОШЕНИЙ, СВЯЗАННЫХ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-КОММУНИКАЦИОННОЙ СЕТИ «ИНТЕРНЕТ»

Обязанности организатора распространения информации в сети «Интернет»

Технически воплощенный в виде системы взаимосвязи машин, составляющей глобальную компьютерную сеть, использующую стандартизированный набор протоколов передачи данных, Интернет стал популярным и широко распространенным инструментом, использование которого разнообразно: обмен сообщениями, поиск информации, социальные сети, совместная работа и т. д.

Первоначально Интернет представлял собой военную сеть США (называемую ARPANET).

Цель состояла в том, чтобы создать сеть, устойчивую к атакам: если точка в сети будет уничтожена, информация должна иметь возможность продолжать поступать. Таким образом, Интернет с самого начала задумывался как паутина.

Если одна точка в сети уничтожена, другие точки в сети могут продолжать обмениваться данными друг с другом, поскольку информация автоматически перемещается по другому пути.

Эта система действует и сегодня: когда вы отправляете или получаете информацию через Интернет, ваши пакеты данных проходят через десятки разных компьютеров и могут даже проходить по разным путям.

Соединяя между собой все сети на планете (военные, университеты, правительства, компании, провайдеры...), мы получаем гигантскую сеть, охватывающую большую часть планеты.

Принцип Интернета заключается в том, что, как только вы подключаетесь к нему, вы становитесь наравне с другими: каждый подключенный компьютер имеет уникальный адрес (IP-адрес) и может отправлять и получать информацию с любого другого компьютера.

Сеть Интернет не делает различий. Расстояния не имеют значения: вы платите не больше, если отправляете что-то своему соседу по лестничной клетке, чем кому-то в Европу. Интернет существует только для

передачи ваших данных на выбранный вами компьютер. Он не предоставляет никаких других услуг.

Конечно, было создано множество приложений, чтобы сделать Интернет более удобным. Единственное неравенство – это доступная вам пропускная способность.

Самым известным приложением в Интернете является HTTP: это веб-страницы, которые вы видите в своем браузере.

Протокол HTTP (используемый вашим браузером) использует Интернет для передачи HTML-страниц, изображений (jpeg, gif ...), музыки, видео и т. д.

Существует также множество других протоколов, которые можно использовать для выполнения множества других задач:

– протокол DNS позволяет найти IP-адрес на основе имени компьютера (что-то вроде каталога);

– протокол FTP используется для передачи файлов с одного компьютера на другой;

– протокол IRC позволяет создавать «чаты» в реальном времени;

– протокол ICQ позволяет узнать, находится ли кто-то в сети, и вступить с ним в диалог;

– протокол NTP позволяет компьютерам подключаться к Интернету с точностью до 500 миллисекунд;

– протоколы P2P позволяют обмениваться файлами в больших масштабах;

– протокол NNTP обеспечивает доступ к дискуссионным форумам по тысячам различных тем;

– протокол SSH обеспечивает безопасный доступ к удаленным компьютерам;

– протокол SMTP позволяет отправлять электронные письма, а протокол POP3 – получать их;

– другие протоколы позволяют проводить телефонные или визуальные конференции;

– другие протоколы.

Никогда изобретатели Интернета не могли представить себе все приложения, существующие сегодня в Интернете.

Организатором распространения информации в сети «Интернет» является лицо, осуществляющее обеспечение функционирования информационных систем и (или) программ для электронных вычислительных машин, которые предназначены и (или) используются для

приема, передачи, доставки и (или) обработки электронных сообщений пользователей сети «Интернет».

Организатор распространения информации в сети «Интернет» обязан в установленном Правительством РФ порядке (Постановление Правительства РФ от 12.11.2020 № 1824 «Об утверждении Правил уведомления организаторами распространения информации в информационно-телекоммуникационной сети “Интернет” Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций о начале осуществления деятельности по обеспечению функционирования информационных систем и (или) программ для электронных вычислительных машин, которые предназначены и (или) используются для приема, передачи, доставки и (или) обработки электронных сообщений пользователей информационно-телекоммуникационной сети “Интернет”, а также ведения реестра указанных организаторов») уведомить федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, о начале осуществления деятельности.

Организатор распространения информации в сети «Интернет» обязан предоставлять указанную информацию уполномоченным государственным органам, осуществляющим оперативно-розыскную деятельность или обеспечение безопасности Российской Федерации в случаях, установленных федеральными законами.

Организатор распространения информации в сети «Интернет» обязан обеспечивать реализацию установленных федеральным органом исполнительной власти в области связи по согласованию с уполномоченными государственными органами, осуществляющими оперативно-розыскную деятельность или обеспечение безопасности Российской Федерации, требований к оборудованию и программно-техническим средствам, используемым указанным организатором в эксплуатируемых им информационных системах, для проведения этими органами в случаях, установленных федеральными законами, мероприятий в целях реализации возложенных на них задач, а также принимать меры по недопущению раскрытия организационных и тактических приемов проведения данных мероприятий.

Порядок взаимодействия организаторов распространения информации в сети «Интернет» с уполномоченными государственными органами, осуществляющими оперативно-розыскную деятельность или обеспечение безопасности Российской Федерации, устанавливается

Правительством Российской Федерации (Постановление Правительства РФ от 31.07.2014 № 743 «Об утверждении Правил взаимодействия организаторов распространения информации в информационно-телекоммуникационной сети “Интернет” с уполномоченными государственными органами, осуществляющими оперативно-розыскную деятельность или обеспечение безопасности Российской Федерации»).

Обязанности организатора распространения информации в сети «Интернет» в Российской Федерации

(Постановление Правительства РФ от 26.02.2022 № 256 «Об утверждении Правил хранения организатором распространения информации в информационно-телекоммуникационной сети «Интернет» текстовых сообщений пользователей информационно-телекоммуникационной сети «Интернет», голосовой информации, изображений, звуков, видео-, иных электронных сообщений пользователей информационно-телекоммуникационной сети «Интернет»)

⇩

Обязан хранить информацию о фактах приема, передачи, доставки и (или) обработки голосовой информации, письменного текста, изображений, звуков, видео- или иных электронных сообщений пользователей сети «Интернет» и информацию об этих пользователях в течение одного года с момента окончания осуществления таких действий

⇩

Обязан хранить текстовые сообщения пользователей сети «Интернет», голосовую информацию, изображения, звуки, видео-, иные электронные сообщения пользователей сети «Интернет» до шести месяцев с момента окончания их приема, передачи, доставки и (или) обработки

Организатор распространения информации в сети «Интернет» обязан при использовании для приема, передачи, доставки и (или) обработки электронных сообщений пользователей сети «Интернет» дополнительного кодирования электронных сообщений и (или) при предоставлении пользователям сети «Интернет» возможности дополнительного кодирования электронных сообщений представлять в федеральный орган исполнительной власти в области обеспечения безопасности информацию, необходимую для декодирования принимаемых, передаваемых, доставляемых и (или) обрабатываемых электронных сообщений.

Организатор сервиса обмена мгновенными сообщениями, являющийся российским юридическим лицом или гражданином Российской Федерации, вправе осуществлять идентификацию пользователей сервиса обмена мгновенными сообщениями самостоятельно путем определения абонентского номера подвижной радиотелефонной связи пользователя сервиса обмена мгновенными сообщениями.

Правительством Российской Федерации могут устанавливаться требования к порядку определения абонентского номера подвижной радиотелефонной связи пользователя сервиса обмена мгновенными сообщениями организатором сервиса обмена мгновенными сообщениями, являющимся российским юридическим лицом или гражданином Российской Федерации.

Организатор сервиса обмена мгновенными сообщениями, являющийся российским юридическим лицом или гражданином Российской Федерации, обязан хранить сведения об идентификации абонентского номера подвижной радиотелефонной связи пользователя сервиса обмена мгновенными сообщениями только на территории Российской Федерации.

Предоставление третьим лицам идентификационных сведений об абонентском номере может осуществляться только с согласия пользователя сервиса обмена мгновенными сообщениями, за исключением случаев, предусмотренных настоящим Федеральным законом и другими федеральными законами. Обязанность предоставить доказательство получения согласия пользователя сервиса обмена мгновенными сообщениями на предоставление третьим лицам идентификационных сведений об абонентском номере данного пользователя сервиса обмена мгновенными сообщениями возлагается на организатора сервиса обмена мгновенными сообщениями.

Особенности регулирования деятельности провайдера хостинга

Провайдер хостинга обязан в установленном Правительством Российской Федерации порядке (Постановление Правительства РФ от 28.11.2023 № 2009 «Об утверждении Правил направления провайдером хостинга уведомления о начале осуществления деятельности по предоставлению вычислительной мощности для размещения информации в информационной системе, постоянно подключенной к информационно-телекоммуникационной сети “Интернет”») направить

уведомление в федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, о начале осуществления деятельности по предоставлению вычислительной мощности для размещения информации в информационной системе, постоянно подключенной к сети «Интернет».

Провайдер хостинга обязан обеспечивать реализацию установленных федеральным органом исполнительной власти в области связи по согласованию с федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, требований о защите информации при предоставлении вычислительной мощности для размещения информации в информационной системе, постоянно подключенной к сети «Интернет» (Приказ Минцифры России от 01.11.2023 № 936 «Об утверждении требований о защите информации при предоставлении вычислительной мощности для размещения информации в информационной системе, постоянно подключенной к информационно-телекоммуникационной сети “Интернет”»).

Провайдер хостинга обязан обеспечивать реализацию установленных федеральным органом исполнительной власти в области связи по согласованию с уполномоченными государственными органами, осуществляющими оперативно-розыскную деятельность или обеспечение безопасности Российской Федерации, требований к вычислительной мощности, используемой провайдером хостинга, для проведения этими органами в случаях, установленных федеральными законами, мероприятий в целях реализации возложенных на них задач, а также принимать меры по недопущению раскрытия организационных и тактических приемов проведения данных мероприятий.

Порядок взаимодействия провайдеров хостинга с уполномоченными государственными органами, осуществляющими оперативно-розыскную деятельность или обеспечение безопасности Российской Федерации, устанавливается Правительством Российской Федерации (Постановление Правительства РФ от 22.11.2023 № 1952 «Об утверждении Правил взаимодействия провайдеров хостинга с уполномоченными государственными органами, осуществляющими оперативно-розыскную деятельность или обеспечение безопасности Российской Федерации»).

Провайдер хостинга вправе осуществлять деятельность по предоставлению вычислительной мощности для размещения информации в информационной системе, постоянно подключенной к сети «Интер-

нет», лицам, обратившимся к провайдеру хостинга, только после прохождения указанными лицами идентификации и (или) аутентификации в порядке, устанавливаемом Правительством Российской Федерации.

Федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, ведет реестр провайдеров хостинга.

Сведения о провайдере хостинга включаются в реестр провайдеров хостинга на основании уведомления.

Правила формирования и ведения реестра провайдеров хостинга, состав сведений, включаемых в реестр провайдеров хостинга, порядок включения таких сведений в реестр провайдеров хостинга и исключения их из реестра провайдеров хостинга, порядок предоставления сведений, содержащихся в реестре провайдеров хостинга, устанавливаются Правительством Российской Федерации (Постановление Правительства РФ от 28.11.2023 № 2008 «Об утверждении Правил формирования и ведения реестра провайдеров хостинга»).

Федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, в соответствии с критериями, определенными Правительством Российской Федерации (Постановление Правительства РФ от 23.11.2023 № 1970 «Об определении критериев, в соответствии с которыми Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций может привлечь к формированию и ведению реестра провайдеров хостинга оператора такого реестра – организацию, зарегистрированную на территории Российской Федерации»), может привлечь к формированию и ведению реестра провайдеров хостинга оператора такого реестра – организацию, зарегистрированную на территории Российской Федерации.

В случае выявления федеральным органом исполнительной власти, осуществляющим функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, нарушения требований и (или) получения указанной информации от федерального органа исполнительной власти в области связи, федерального органа исполнительной власти, уполномоченного в области обеспечения безопасности, федерального органа исполнительной власти, уполномоченного в области противодействия техническим разведкам и технической защиты информации, федераль-

ный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, направляет провайдеру хостинга требование принять меры по устранению выявленных нарушений, в котором указываются сроки устранения выявленных нарушений и представления информации о принятых мерах, составляющие не более чем десять рабочих дней.

Провайдер хостинга в сроки, указанные в требовании федерального органа исполнительной власти, осуществляющего функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, принимает меры по устранению выявленных нарушений, а также представляет информацию о принятых мерах в указанный орган.

Неустранение провайдером хостинга выявленных нарушений, указанных в требовании федерального органа исполнительной власти, осуществляющего функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, либо непредставление провайдером хостинга в указанный орган информации о принятых мерах является основанием для исключения сведений о провайдере хостинга из реестра провайдеров хостинга.

Не допускается осуществление деятельности по предоставлению вычислительной мощности для размещения информации в информационной системе, постоянно подключенной к сети «Интернет», провайдерами хостинга, сведения о которых не включены в реестр провайдеров хостинга.

Особенности предоставления информации с применением рекомендательных технологий

Владелец сайта и (или) страницы сайта в сети «Интернет», и (или) информационной системы, и (или) программы для электронных вычислительных машин, на которых применяются информационные технологии предоставления информации на основе сбора, систематизации и анализа сведений, относящихся к предпочтениям пользователей сети «Интернет», находящихся на территории Российской Федерации, обязан соблюдать требования законодательства Российской Федерации, в частности:

– не допускать применение информационных технологий предоставления информации на основе сбора, систематизации и анализа сведений, относящихся к предпочтениям пользователей сети «Интернет», находящихся на территории Российской Федерации, которые нарушают права и законные интересы граждан и организаций, а также не допускать применение рекомендательных технологий в целях предоставления информации с нарушением законодательства Российской Федерации;

– не допускать предоставление информации с применением рекомендательных технологий без информирования пользователей сети «Интернет» о применении на данном сайте и (или) странице сайта в сети «Интернет» и (или) в информационной системе, и (или) в программе для электронных вычислительных машин рекомендательных технологий. Требования к содержанию информации о применении рекомендательных технологий и размещению такой информации на информационном ресурсе устанавливаются федеральным органом исполнительной власти, осуществляющим функции контроля и надзора в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи (Приказ Роскомнадзора от 06.10.2023 № 149 «Об утверждении требований к содержанию информации о применении информационных технологий предоставления информации на основе сбора, систематизации и анализа сведений, относящихся к предпочтениям пользователей сети «Интернет», находящихся на территории Российской Федерации, и размещению такой информации на информационном ресурсе»);

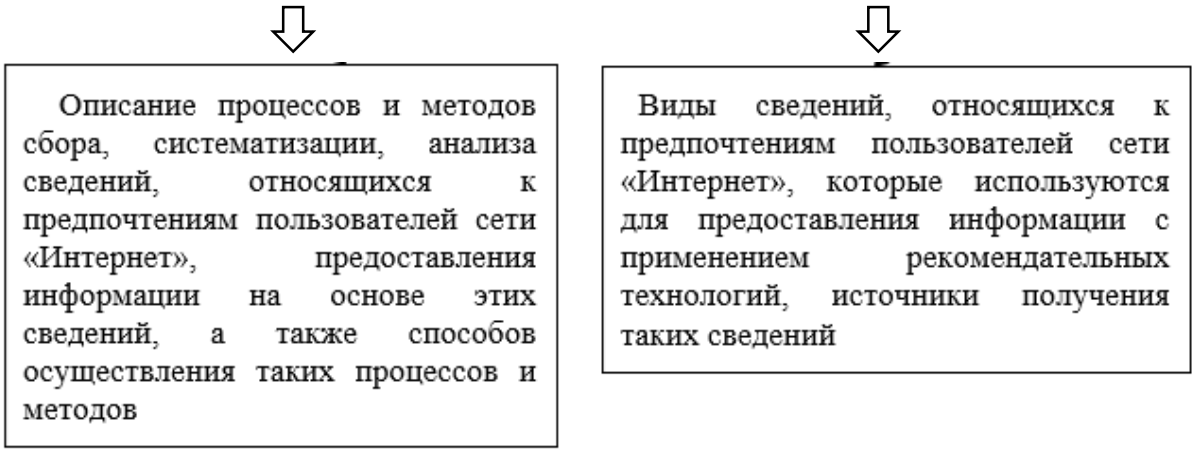
– разместить на информационном ресурсе, на котором применяются рекомендательные технологии, документ, устанавливающий правила применения рекомендательных технологий;

– разместить на информационном ресурсе, на котором применяются рекомендательные технологии, адрес электронной почты для направления ему юридически значимых сообщений, свои фамилию и инициалы (для физического лица) или наименование (для юридического лица).

Правила применения рекомендательных технологий должны быть размещены на информационном ресурсе, на котором применяются рекомендательные технологии, на русском языке.

Владелец информационного ресурса, на котором применяются рекомендательные технологии, должен обеспечить беспрепятственный и безвозмездный доступ пользователей сети «Интернет» к правилам применения рекомендательных технологий.

Содержание Правил применения рекомендательных технологий



В случае обнаружения в сети «Интернет» информационного ресурса, на котором рекомендательные технологии применяются с признаками нарушения требований, федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, вправе запрашивать у владельца информационного ресурса, на котором применяются рекомендательные технологии, информацию, связанную с применением рекомендательных технологий, а также доступ к программно-техническим средствам рекомендательных технологий для проведения оценки соответствия применения рекомендательных технологий требованиям настоящей статьи.

Указанное лицо обязано предоставлять запрашиваемую информацию и доступ к программно-техническим средствам не позднее десяти дней со дня получения запроса федерального органа исполнительной власти, осуществляющего функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи.

В случае установления факта неисполнения владельцем информационного ресурса, на котором применяются рекомендательные технологии, обязанностей, предусмотренных настоящей статьей, федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, направляет указанному лицу уведомление, содержащее требование принять меры по устранению выявленного нарушения.

Владелец информационного ресурса, на котором применяются рекомендательные технологии, обязан принять меры по устранению указанного в уведомлении нарушения не позднее десяти дней со дня получения уведомления или в иной, установленный в уведомлении срок.

В случае непринятия владельцем информационного ресурса, на котором применяются рекомендательные технологии, мер, указанных выше, федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, незамедлительно направляет указанному лицу требование о прекращении предоставления информации с применением рекомендательных технологий.

В случае неисполнения владельцем информационного ресурса, на котором применяются рекомендательные технологии, требования о прекращении предоставления информации с применением рекомендательных технологий федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, незамедлительно направляет по системе взаимодействия операторам связи требование о принятии мер по ограничению доступа к информационному ресурсу, на котором применяются рекомендательные технологии.

Данное требование должно содержать доменное имя сайта в сети «Интернет», сетевой адрес, указатели страниц сайта в сети «Интернет», позволяющие идентифицировать такой информационный ресурс.

После получения по системе взаимодействия требования федерального органа исполнительной власти, осуществляющего функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, о принятии мер по ограничению доступа оператор связи, оказывающий услуги по предоставлению доступа к информационно-телекоммуникационной сети «Интернет», обязан незамедлительно ограничить доступ к информационному ресурсу.

В случае, если владелец информационного ресурса, на котором применяются рекомендательные технологии, принял меры, указанные выше, он направляет уведомление об этом в федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору

в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи. Такое уведомление может быть направлено также в электронном виде.

Порядок взаимодействия федерального органа исполнительной власти, осуществляющего функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, с владельцами информационных ресурсов, на которых применяются рекомендательные технологии, устанавливается указанным федеральным органом исполнительной власти (Приказ Роскомнадзора от 06.10.2023 № 150 «Об утверждении порядка взаимодействия Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций с владельцами сайтов и (или) страниц сайтов в сети «Интернет», и (или) информационных систем, и (или) программ для электронных вычислительных машин, на которых применяются информационные технологии предоставления информации на основе сбора, систематизации и анализа сведений, относящихся к предпочтениям пользователей сети «Интернет», находящихся на территории Российской Федерации»).

Нарушение владельцем информационного ресурса, на котором применяются рекомендательные технологии, требований, указанных выше, влечет за собой уголовную, административную и иную ответственность в соответствии с законодательством Российской Федерации.

Особенности распространения информации в социальных сетях

Одним из преобладающих современных приложений Интернета являются социальные сети.

Их демократизация, в частности, является частью движения Web 2.0 и Сети людей: инструменты обмена и публикации в Интернете позволяют и все больше способствуют обмену между людьми.

Социальная сеть сегодня используется территориальными органами власти для продвижения и оживления территории, стимулирования гражданского диалога, оживления сообществ, повышения ценности организации и «гипер-локальности». Например, во многих субъектах РФ и муниципальных образованиях создано веб-телевидение и интернет-пространство для диалога между органами государственной власти и местного самоуправления и населением – такое

развертывание стало возможным благодаря технологиям и практикам социальной сети.

Первоначально предназначенные для широкой публики и позволяющие устанавливать связи между людьми, разделяющими общие интересы или связи (например, Facebook), социальные сети совсем недавно появились в организациях. В таком случае мы говорим о профессиональных социальных сетях или социальных сетях организации, позволяющих, в частности, укреплять связи и обмен мнениями между сотрудниками, а также чувство принадлежности к одному сообществу, капитализации и обмену знаниями внутри организаций.

Владелец сайта и (или) страницы сайта в сети «Интернет», и (или) информационной системы, и (или) программы для электронных вычислительных машин, которые предназначены и (или) используются их пользователями для предоставления и (или) распространения посредством созданных ими персональных страниц информации на государственном языке Российской Федерации, государственных языках республик в составе Российской Федерации или иных языках народов Российской Федерации, на которых может распространяться реклама, направленная на привлечение внимания потребителей, находящихся на территории Российской Федерации, и доступ к которым в течение суток составляет более пятисот тысяч пользователей сети «Интернет», находящихся на территории Российской Федерации, обязан соблюдать следующие требования законодательства Российской Федерации:

1. Не допускать использование сайта и (или) страницы сайта в сети «Интернет», и (или) информационной системы, и (или) программы для электронных вычислительных машин, которые предназначены и (или) используются их пользователями для предоставления и (или) распространения посредством созданных ими персональных страниц информации на государственном языке Российской Федерации, государственных языках республик в составе Российской Федерации и иных языках народов Российской Федерации, на которых может распространяться реклама, направленная на привлечение внимания потребителей, находящихся на территории Российской Федерации, и доступ к которым в течение суток составляет более пятисот тысяч пользователей сети «Интернет», находящихся на территории Российской Федерации, в целях совершения уголовно наказуемых деяний, разглашения сведений, составляющих государственную или иную специально охраняемую законом тайну, распространения материалов, содержащих публичные призывы к осуществлению террористической

деятельности или публично оправдывающих терроризм, других экстремистских материалов, а также материалов, пропагандирующих порнографию, насилие и жестокость, и материалов, содержащих нецензурную брань.

2. Не допускать распространение информации с целью опорочить гражданина или отдельные категории граждан по признакам пола, возраста, расовой или национальной принадлежности, языка, отношения к религии, профессии, места жительства и работы, а также в связи с их политическими убеждениями.

3. Соблюдать запреты и ограничения, предусмотренные законодательством РФ о референдуме и законодательством Российской Федерации о выборах.

4. Соблюдать права и законные интересы граждан и организаций, в том числе честь, достоинство и деловую репутацию граждан, деловую репутацию организаций.

5. Осуществлять мониторинг социальной сети в целях выявления:

– материалов с порнографическими изображениями несовершеннолетних и (или) объявлений о привлечении несовершеннолетних в качестве исполнителей для участия в зрелищных мероприятиях порнографического характера;

– информации о способах, методах разработки, изготовления и использования наркотических средств, психотропных веществ и их прекурсоров, новых потенциально опасных психоактивных веществ, местах их приобретения, способах и местах культивирования наркосодержащих растений;

– информации о способах совершения самоубийства, а также призывов к совершению самоубийства;

– информации, нарушающей требования Федерального закона от 29.12.2006 №244-ФЗ «О государственном регулировании деятельности по организации и проведению азартных игр и о внесении изменений в некоторые законодательные акты Российской Федерации» и Федерального закона от 11.11.2003 № 138-ФЗ «О лотереях» о запрете деятельности по организации и проведению азартных игр и лотерей с использованием сети “Интернет”» и иных средств связи;

– информации, содержащей предложения о розничной продаже дистанционным способом алкогольной продукции, и (или) спиртосодержащей пищевой продукции, и (или) этилового спирта, и (или) спиртосодержащей непищевой продукции, розничная продажа которой ограничена или запрещена законодательством о государственном регулировании производства и оборота этилового спирта, алкогольной

и спиртосодержащей продукции и об ограничении потребления (распития) алкогольной продукции;

– информации, направленной на склонение или иное вовлечение несовершеннолетних в совершение противоправных действий, представляющих угрозу для их жизни и (или) здоровья либо для жизни и (или) здоровья иных лиц;

– информации, выражающей в неприличной форме, которая оскорбляет человеческое достоинство и общественную нравственность, явное неуважение к обществу, государству, официальным государственным символам Российской Федерации, Конституции РФ или органам, осуществляющим государственную власть в Российской Федерации;

– информации, содержащей призывы к массовым беспорядкам, осуществлению экстремистской деятельности, участию в массовых (публичных) мероприятиях, проводимых с нарушением установленного порядка, недостоверной общественно значимой информации, распространяемой под видом достоверных сообщений, которая создает угрозу причинения вреда жизни и (или) здоровью граждан, имуществу, угрозу массового нарушения общественного порядка и (или) общественной безопасности либо угрозу создания помех функционированию или прекращения функционирования объектов жизнеобеспечения, транспортной или социальной инфраструктуры, кредитных организаций, объектов энергетики, промышленности или связи, информационных материалов иностранной или международной организации, деятельность которой признана нежелательной на территории Российской Федерации в соответствии с Федеральным законом от 28.12.2012 № 272-ФЗ «О мерах воздействия на лиц, причастных к нарушениям основополагающих прав и свобод человека, прав и свобод граждан Российской Федерации», сведений, позволяющих получить доступ к указанным информации или материалам;

– информации, пропагандирующей нетрадиционные сексуальные отношения и (или) предпочтения, педофилию, смену пола;

– информации, оскорбляющей человеческое достоинство и общественную нравственность, выражающей явное неуважение к обществу, содержащей изображение действий с признаками противоправных, в том числе насильственных, и распространяемой из хулиганских, корыстных или иных низменных побуждений.

6. Разместить в социальной сети адрес электронной почты для направления ему юридически значимых сообщений, свои фамилию

и инициалы (для физического лица) или наименование (для юридического лица), а также электронную форму для направления обращений о распространяемой с нарушением закона информации, требования к которой устанавливаются федеральным органом исполнительной власти, осуществляющим функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи.

7. Ежегодно размещать отчет о результатах рассмотрения обращений, а также о результатах мониторинга. Требования к форме, составу и размещению данного отчета устанавливаются федеральным органом исполнительной власти, осуществляющим функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи.

8. Разместить в социальной сети документ, устанавливающий правила использования социальной сети.

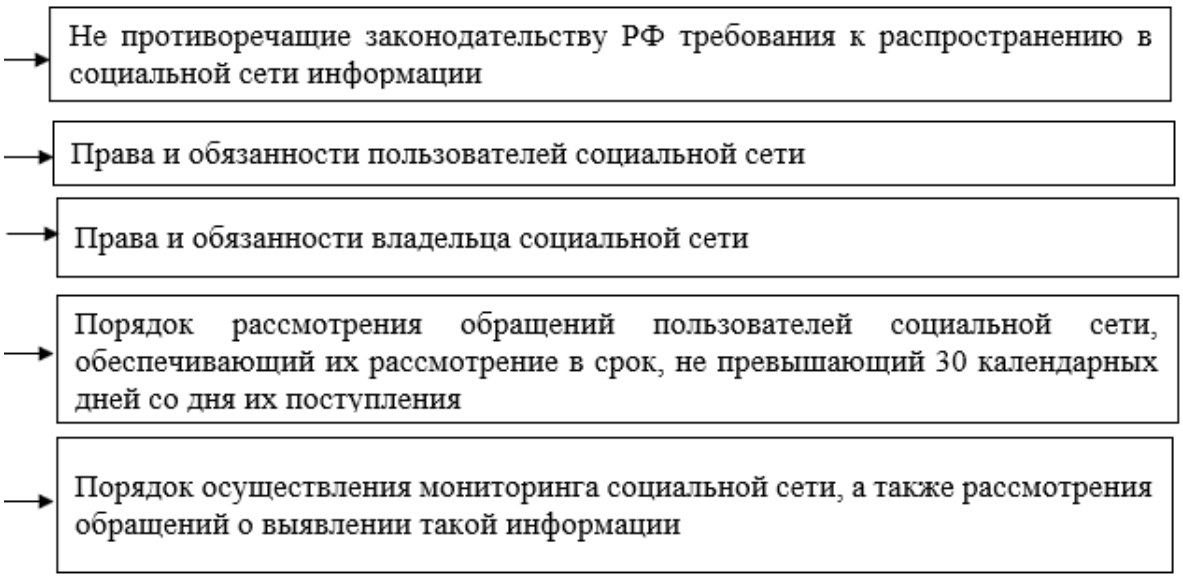
9. В случае внесения изменений в правила использования социальной сети в течение трех дней со дня внесения таких изменений информировать об этом пользователей социальной сети путем направления каждому из них уведомления об этом с описанием внесенных изменений.

10. Установить одну из предлагаемых федеральным органом исполнительной власти, осуществляющим функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, предназначенных для определения количества пользователей информационным ресурсом в сети «Интернет» программ для электронных вычислительных машин.

11. Уведомлять пользователя социальной сети о принятых мерах по ограничению доступа к его информации, а также об основаниях такого ограничения.

12. Предоставлять по запросу федерального органа исполнительной власти, осуществляющего функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, и (или) федерального органа исполнительной власти, уполномоченного в области обеспечения безопасности, сведения о пользователе социальной сети. Состав сведений и порядок их предоставления устанавливаются Правительством РФ.

Содержание Правил использования социальной сети



Правила использования социальной сети должны быть размещены в социальной сети на русском языке. Владелец социальной сети должен обеспечить беспрепятственный и безвозмездный доступ пользователей к правилам использования социальной сети.

Федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, ведет реестр социальных сетей.

В случае обнаружения в сети «Интернет» информационного ресурса, который предназначен и (или) используется его пользователями для предоставления и (или) распространения посредством созданных ими персональных страниц информации на государственном языке Российской Федерации, государственных языках республик в составе Российской Федерации, других языках народов Российской Федерации, на котором может распространяться реклама, направленная на привлечение внимания потребителей, находящихся на территории Российской Федерации, и доступ к которому в течение суток составляет более пятисот тысяч пользователей сети «Интернет», находящихся на территории Российской Федерации, включая рассмотрение соответствующих обращений органов государственной власти, органов местного самоуправления, граждан или организаций, федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи:

– признает информационный ресурс в сети «Интернет» социальной сетью и включает его в реестр социальных сетей;

– определяет провайдера хостинга или иное обеспечивающее размещение социальной сети в сети «Интернет» лицо;

– направляет провайдеру хостинга уведомление в электронном виде на русском и английском языках о необходимости предоставления данных, позволяющих идентифицировать владельца социальной сети;

– фиксирует дату и время направления уведомления провайдеру хостинга.

13. В течение трех рабочих дней с момента получения уведомления, провайдер хостинга обязан предоставить данные, позволяющие идентифицировать владельца социальной сети.

После получения данных, федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, направляет владельцу социальной сети уведомление о включении его информационного ресурса в реестр социальных сетей с указанием требований законодательства Российской Федерации, применимых к данным информационным ресурсам.

В течение двух месяцев со дня включения информационного ресурса в реестр социальных сетей владелец социальной сети обязан обеспечить приведение правил использования социальной сети в соответствие с требованиями настоящего Федерального закона и ознакомление с указанными правилами пользователей своей социальной сети.

В случае, если доступ к социальной сети на протяжении трех месяцев составляет в течение суток менее пятисот тысяч пользователей сети «Интернет», расположенных на территории Российской Федерации, данная социальная сеть по заявлению ее владельца исключается из реестра социальных сетей, о чем владельцу социальной сети направляется соответствующее уведомление.

Данная социальная сеть может быть исключена из реестра социальных сетей при отсутствии заявления ее владельца, если доступ к данной социальной сети на протяжении шести месяцев составляет в течение суток менее пятисот тысяч пользователей сети «Интернет», расположенных на территории Российской Федерации.

Порядок взаимодействия федерального органа исполнительной власти, осуществляющего функции по контролю и надзору в сфере

средств массовой информации, массовых коммуникаций, информационных технологий и связи, с владельцами социальных сетей устанавливается указанным федеральным органом исполнительной власти.

Федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, вправе направить владельцу социальной сети предписание об осуществлении мониторинга социальной сети в целях выявления информации, схожей до степени смешения с информацией, меры по удалению которой владелец данной или иной социальной сети обязан принимать на основании ранее направленного требования или уведомления указанного федерального органа в соответствии с настоящим Федеральным законом.

ПРАВОВОЕ РЕГУЛИРОВАНИЕ ЭЛЕКТРОННОЙ ПОДПИСИ

Во все более оцифрованном мире электронная подпись стала незаменимым инструментом для оформления документов.

Электронная подпись – это система, позволяющая ставить свою подпись на цифровых документах в режиме онлайн.

Электронная подпись служит для обеспечения целостности и подлинности электронного документа с помощью соответствующих сертификатов.

Использование электронных подписей получило огромное распространение во всех сегментах нашей экономики. Причинами служат упрощение, а также автоматизация процессов подписания любого типа документов, при этом не игнорируя аспект конфиденциальности или юридическую силу собранных подписей.

Благодаря значительному успеху, которого они достигли, электронные подписи теперь доступны с помощью множества программ. Будь то электронное выставление счетов, электронное архивирование или необходимость электронной подписи цифровых документов, это программное обеспечение предлагает множество решений. Некоторые даже предлагают расширенные возможности, такие как шифрование документов, для повышения безопасности. Личность подписывающего лица тщательно проверяется, что гарантирует юридическую ценность подписанных документов. Это программное обеспечение, использующее электронные сертификаты и доверенные центры сертификации, обеспечивают эффективную цифровую подпись. Некоторые зашли так далеко, что предлагают возможность подписывать рукописные документы в электронном виде.

Подключение к Интернету стало основным условием для этого программного обеспечения, что позволяет удаленно использовать электронную подпись. Некоторые также используют цифровые сейфы для безопасного хранения подписанных документов, что повышает их конфиденциальность.

Электронная подпись → - информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию (ст. 2 Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи»)

Виды электронных подписей, используемых органами исполнительной власти и органами местного самоуправления, порядок их использования, а также требования об обеспечении совместимости средств электронных подписей при организации электронного взаимодействия указанных органов между собой устанавливает Правительство Российской Федерации (Постановление Правительства РФ от 09.02.2012 № 111 «Об электронной подписи, используемой органами исполнительной власти и органами местного самоуправления при организации электронного взаимодействия между собой, о порядке ее использования, а также об установлении требований к обеспечению совместимости средств электронной подписи».

Принципы использования электронной подписи

- Право участников электронного взаимодействия использовать электронную подпись любого вида по своему усмотрению, если требование об использовании конкретного вида электронной подписи в соответствии с целями ее использования не предусмотрено федеральными законами или принимаемыми в соответствии с ними нормативными правовыми актами либо соглашением между участниками электронного взаимодействия
- Возможность использования участниками электронного взаимодействия по своему усмотрению любой информационной технологии и (или) технических средств, позволяющих выполнить требования федерального закона применительно к использованию конкретных видов электронных подписей
- Недопустимость признания электронной подписи и (или) подписанного ею электронного документа не имеющими юридической силы только на основании того, что такая электронная подпись создана не собственноручно, а с использованием средств электронной подписи для автоматического создания и (или) автоматической проверки электронных подписей в информационной системе

В соответствии со ст. 5 Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи», видами электронных подписей, отношения в области использования которых регулируются данным законом, являются простая электронная подпись и усиленная электронная подпись.

Различаются усиленная неквалифицированная электронная подпись и усиленная квалифицированная электронная подпись.

Признаки неквалифицированной электронной подписи

- Получена в результате криптографического преобразования информации с использованием ключа электронной подписи
- Позволяет определить лицо, подписавшее электронный документ
- Позволяет обнаружить факт внесения изменений в электронный документ после момента его подписания
- Создается с использованием средств электронной подписи

Признаки квалифицированной электронной подписи

- Получена в результате криптографического преобразования информации с использованием ключа электронной подписи
- Позволяет определить лицо, подписавшее электронный документ
- Позволяет обнаружить факт внесения изменений в электронный документ после момента его подписания
- Создается с использованием средств электронной подписи
- Ключ проверки электронной подписи указан в квалифицированном сертификате
- Для создания и проверки электронной подписи используются средства электронной подписи, имеющие подтверждение соответствия требованиям, установленным в соответствии с законом сертификате

При использовании неквалифицированной электронной подписи сертификат ключа проверки электронной подписи может не создаваться, если соответствие электронной подписи признакам неквалифицированной электронной подписи, установленным законом, может быть обеспечено без использования сертификата ключа проверки электронной подписи.

Условия признания электронных документов, подписанных электронной подписью, равнозначными документам на бумажном носителе, подписанным собственноручной подписью

⇩	⇩
Информация в электронной форме, подписанная квалифицированной электронной подписью, признается электронным документом, равнозначным документу на бумажном носителе, подписанному собственноручной подписью, и может применяться в любых правоотношениях в соответствии с законодательством РФ, кроме случая, если федеральными законами или принимаемыми в соответствии с ними нормативными правовыми актами установлено требование о необходимости составления документа исключительно на бумажном носителе	Информация в электронной форме, подписанная простой электронной подписью или неквалифицированной электронной подписью, признается электронным документом, равнозначным документу на бумажном носителе, подписанному собственноручной подписью, в случаях, установленных федеральными законами, принимаемыми в соответствии с ними нормативными правовыми актами, нормативными актами Центрального банка РФ или соглашением между участниками электронного взаимодействия, в том числе правилами платежных систем

Нормативные правовые акты и соглашения между участниками электронного взаимодействия, устанавливающие случаи признания электронных документов, подписанных неквалифицированной электронной подписью, равнозначными документам на бумажных носителях, подписанным собственноручной подписью, должны предусматривать порядок проверки электронной подписи.

Преимущества электронной подписи:

1. Сокращение времени обработки: быстрее, чем при подписании от руки, за счет сокращения времени, необходимого для завершения транзакций. Очевидная экономия времени и производительности для ваших команд.
2. Снижение затрат: без бумаги, чернил и почтовых расходов вы значительно сэкономите в долгосрочной перспективе.

3. Доступность: с помощью простого подключения к Интернету подписывающие стороны могут подписывать документы где угодно и когда угодно.

4. Повышенная безопасность: электронная подпись имеет расширенные возможности безопасности, такие как шифрование данных и многофакторная аутентификация, гарантирующие целостность и подписанные документы.

5. Решения для отслеживания: решения для электронной подписи предоставляют подробные контрольные журналы для каждого этапа процесса подписания, обеспечивая повышенную прозрачность и отслеживаемость.

Недостатки электронной подписи:

1. Зависимость от технологий: перебои в подключении или сбои сервера могут помешать доступу к документам или нарушить процесс подписания.

2. Соблюдение законодательства: хотя большинство стран признают юридическую силу электронных подписей, для некоторых документов могут потребоваться рукописные подписи по нормативным причинам.

3. Принятие: некоторые организации по-прежнему неохотно внедряют новые технологии и предпочитают традиционные методы рукописной подписи.

4. Безопасность данных: ни одна система не является надежной, и, хотя решения для электронной подписи, как правило, безопасны, всегда существует потенциальный риск утечки данных или нарушения безопасности.

Нормативные правовые акты и соглашения между участниками электронного взаимодействия, устанавливающие случаи признания электронных документов, подписанных простой электронной подписью, равнозначными документам на бумажных носителях, подписанным собственноручной подписью, должны соответствовать требованиям ст. 9 Федерального закона «Об электронной подписи».

Если в соответствии с федеральными законами, принимаемыми в соответствии с ними нормативными правовыми актами или обычаем делового оборота документ должен быть заверен печатью, электронный документ, подписанный усиленной электронной подписью и признаваемый равнозначным документу на бумажном носителе, подписанному собственноручной подписью, признается равнозначным документу на бумажном носителе, подписанному собственноручной подписью и заверенному печатью.

Федеральными законами, принимаемыми в соответствии с ними нормативными правовыми актами или соглашением между участниками электронного взаимодействия, могут быть предусмотрены дополнительные требования к электронному документу в целях признания его равнозначным документу на бумажном носителе, заверенному печатью.

Одной электронной подписью могут быть подписаны несколько связанных между собой электронных документов (пакет электронных документов). При подписании электронной подписью пакета электронных документов каждый из электронных документов, входящих в этот пакет, считается подписанным электронной подписью того вида, которой подписан пакет электронных документов.

Исключение составляют случаи, когда в состав пакета электронных документов лицом, подписавшим пакет, включены электронные документы, созданные иными лицами (органами, организациями) и подписанные ими тем видом электронной подписи, который установлен законодательством Российской Федерации для подписания таких документов.

В этих случаях электронный документ, входящий в пакет, считается подписанным лицом, первоначально создавшим такой электронный документ, тем видом электронной подписи, которым этот документ был подписан при создании, вне зависимости от того, каким видом электронной подписи подписан пакет электронных документов.

Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи» закреплены полномочия федеральных органов исполнительной власти в сфере использования электронной подписи (табл. 10).

Уполномоченный федеральный орган в сфере использования электронной подписи определяется Правительством Российской Федерации. В настоящее время это Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации (далее – Минцифры России).

Таблица 10

Полномочия федеральных органов исполнительной власти в сфере использования электронной подписи

Министерство цифрового развития, связи и массовых коммуникаций РФ	Федеральная служба безопасности
Осуществляет аккредитацию удостоверяющих центров, проводит проверки соблюдения аккредитованными удостоверяющими центрами требований, установленных законодательством	По согласованию с уполномоченным федеральным органом устанавливает требования к форме квалифицированного сертификата и правила подтверждения владения ключом электронной подписи
Осуществляет функции головного удостоверяющего центра в отношении аккредитованных удостоверяющих центров	Устанавливает требования к средствам электронной подписи, средствам удостоверяющего центра и средствам доверенной третьей стороны, включая требования к используемым доверенной третьей стороной средствам электронной подписи
Осуществляет аккредитацию доверенных третых сторон, проводит проверки соблюдения доверенными третьими сторонами требований, установленных законодательством	Устанавливает требования к средствам электронной подписи и средствам удостоверяющего центра, применяемым для реализации функций, предусмотренных ч. 2.2 ст. 15 Федерального закона «Об электронной подписи»
–	Осуществляет подтверждение соответствия средств электронной подписи и средств удостоверяющего центра требованиям, установленным в соответствии с законом, и публикует перечень таких средств
–	Осуществляет подтверждение соответствия средств доверенной третьей стороны требованиям, установленным в соответствии с законом, и публикует перечень таких средств

В соответствии со ст. 9 Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи», электронный документ считается подписанным простой электронной подписью при выполнении в том числе одного из следующих условий:

– простая электронная подпись содержится в самом электронном документе;

– ключ простой электронной подписи применяется в соответствии с правилами, установленными оператором информационной системы, с использованием которой осуществляются создание и (или) отправка электронного документа, и в созданном и (или) отправленном электронном документе содержится информация, указывающая на лицо, от имени которого был создан и (или) отправлен электронный документ.

Нормативные правовые акты и (или) соглашения между участниками электронного взаимодействия, устанавливающие случаи признания электронных документов, подписанных простой электронной подписью, равнозначными документам на бумажных носителях, подписанным собственноручной подписью, должны предусматривать, в частности:

– правила определения лица, подписывающего электронный документ, по его простой электронной подписи;

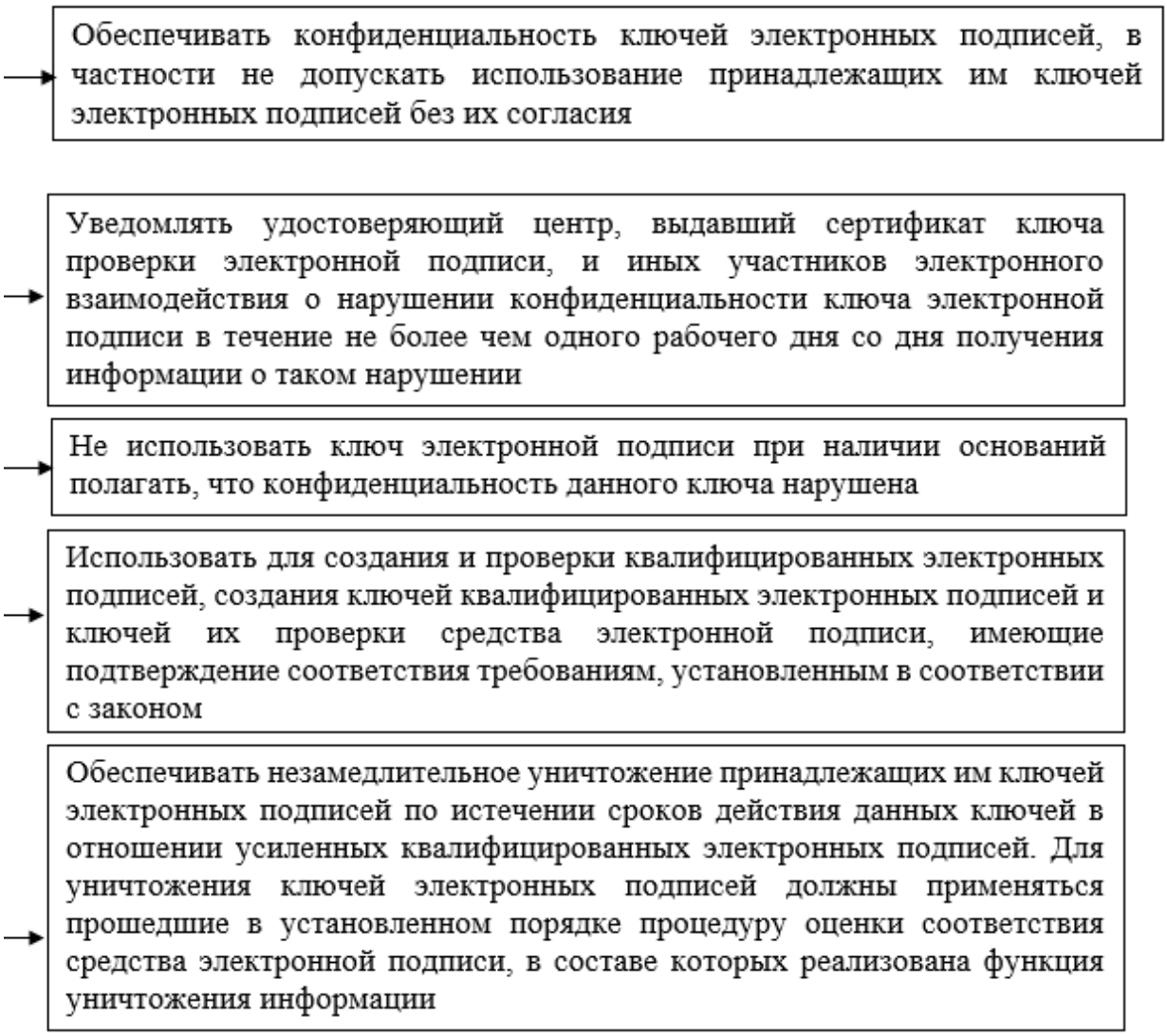
– обязанность лица, создающего и (или) использующего ключ простой электронной подписи, соблюдать его конфиденциальность.

К отношениям, связанным с использованием простой электронной подписи, в том числе с созданием и использованием ключа простой электронной подписи, не применяются правила, установленные ст. 10–18 Федерального закона «Об электронной подписи».

Использование простой электронной подписи для подписания электронных документов, содержащих сведения, составляющие государственную тайну, или в информационной системе, содержащей сведения, составляющие государственную тайну, не допускается.

Участники электронного взаимодействия не вправе устанавливать иные, за исключением предусмотренных настоящим Федеральным законом, ограничения признания усиленной квалифицированной электронной подписи.

Обязанности участников электронного взаимодействия при использовании усиленных электронных подписей

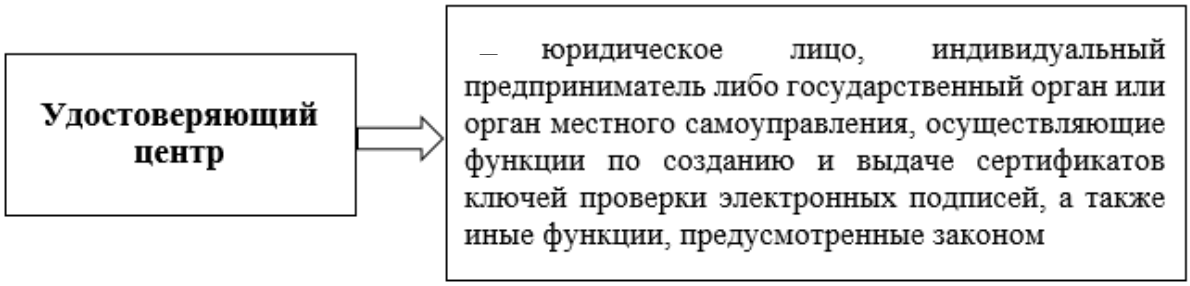


Нарушение запрета на ограничение или отказ от признания электронных документов, подписанных квалифицированной электронной подписью, соответствующей предъявляемым к ней требованиям, равнозначными документам на бумажном носителе, подписанным собственноручной подписью, а также нарушение запрета операторами государственных и муниципальных информационных систем, информационных систем, использование которых предусмотрено нормативными правовыми актами, или информационных систем общего пользования на предъявление требований о наличии в квалифицированном сертификате информации, не являющейся обязательной в соответствии с Федеральным законом «Об электронной подписи» и принимаемыми в соответствии с ним нормативными правовыми актами,

по любым причинам, кроме предусмотренных Федеральным законом «Об электронной подписи», не допускается.

Средства электронной подписи, предназначенные для создания электронных подписей в электронных документах, содержащих сведения, составляющие государственную тайну, или предназначенные для использования в информационной системе, содержащей сведения, составляющие государственную тайну, подлежат подтверждению соответствия обязательным требованиям по защите сведений соответствующей степени секретности в соответствии с законодательством Российской Федерации.

Средства электронной подписи, предназначенные для создания электронных подписей в электронных документах, содержащих информацию ограниченного доступа (в том числе персональные данные), не должны нарушать конфиденциальность такой информации.



Удостоверяющий центр:

– создает сертификаты ключей проверки электронных подписей и выдает такие сертификаты заявителям при условии идентификации заявителя;

– осуществляет в соответствии с правилами подтверждения владения ключом электронной подписи подтверждение владения заявителем ключом электронной подписи, соответствующим ключу проверки электронной подписи, указанному им для получения сертификата ключа проверки электронной подписи (Приказ ФСБ России от 20.04.2021 № 154 «Об утверждении Правил подтверждения владения ключом электронной подписи»);

– создает сертификаты ключей проверки электронной подписи и выдает такие сертификаты заявителям в отношении усиленной неквалифицированной электронной подписи;

– устанавливает сроки действия сертификатов ключей проверки электронных подписей;

– аннулирует выданные этим удостоверяющим центром сертификаты ключей проверки электронных подписей;

– выдает по обращению заявителя средства электронной подписи, содержащие ключ электронной подписи и ключ проверки электронной подписи (в том числе созданные удостоверяющим центром) или обеспечивающие возможность создания ключа электронной подписи и ключа проверки электронной подписи заявителем;

– ведет реестр выданных и аннулированных этим удостоверяющим центром сертификатов ключей проверки электронных подписей, в том числе включающий в себя информацию, содержащуюся в выданных этим удостоверяющим центром сертификатах ключей проверки электронных подписей, и информацию о датах прекращения действия или аннулирования сертификатов ключей проверки электронных подписей и об основаниях таких прекращения или аннулирования;

– устанавливает порядок ведения реестра сертификатов, не являющихся квалифицированными, и порядок доступа к нему, а также обеспечивает доступ лиц к информации, содержащейся в реестре сертификатов, в том числе с использованием информационно-телекоммуникационной сети «Интернет»;

– создает по обращениям заявителей ключи электронных подписей и ключи проверки электронных подписей;

– проверяет уникальность ключей проверки электронных подписей в реестре сертификатов;

– осуществляет по обращениям участников электронного взаимодействия проверку электронных подписей;

– осуществляет иную связанную с использованием электронной подписи деятельность.

Удостоверяющий центр обязан:

– информировать заявителей об условиях и о порядке использования электронных подписей и средств электронной подписи, о рисках, связанных с использованием электронных подписей, и о мерах, необходимых для обеспечения безопасности электронных подписей и их проверки;

– обеспечивать актуальность информации, содержащейся в реестре сертификатов, и ее защиту от неправомерного доступа, уничтожения, модификации, блокирования, иных неправомерных действий;

– предоставлять безвозмездно любому лицу по его обращению в соответствии с установленным порядком доступа к реестру сертификатов информацию, содержащуюся в реестре сертификатов, в том

числе информацию об аннулировании сертификата ключа проверки электронной подписи;

– обеспечивать конфиденциальность созданных удостоверяющим центром ключей электронных подписей;

– отказать заявителю в создании сертификата ключа проверки электронной подписи в случае, если не было подтверждено, что заявитель владеет ключом электронной подписи, который соответствует ключу проверки электронной подписи, указанному заявителем для получения сертификата ключа проверки электронной подписи;

– отказать заявителю в создании сертификата ключа проверки электронной подписи в случае отрицательного результата проверки в реестре сертификатов уникальности ключа проверки электронной подписи, указанного заявителем для получения сертификата ключа проверки электронной подписи;

– незамедлительно информировать владельца квалифицированного сертификата о выявленных случаях приостановления (прекращения) технической возможности использования ключа электронной подписи, не предусмотренных соглашением сторон, или возникновения у аккредитованного удостоверяющего центра обоснованных сомнений в получении поручения от уполномоченного соглашением сторон лица об использовании ключа электронной подписи.

Удостоверяющему центру запрещается указывать в создаваемом им сертификате ключа проверки электронной подписи ключ проверки электронной подписи, который содержится в сертификате ключа проверки электронной подписи, выданном этому удостоверяющему центру любым другим удостоверяющим центром.

Удостоверяющий центр в соответствии с законодательством Российской Федерации несет ответственность за вред, причиненный третьим лицам в результате:

– неисполнения или ненадлежащего исполнения обязательств, вытекающих из договора оказания услуг удостоверяющим центром;

– неисполнения или ненадлежащего исполнения обязанностей, предусмотренных Федеральным законом «Об электронной подписи».

Информация, внесенная в реестр сертификатов, подлежит хранению в течение всего срока деятельности удостоверяющего центра, если более короткий срок не установлен нормативными правовыми актами.

В случае прекращения деятельности удостоверяющего центра без перехода его функций другим лицам он должен уведомить об этом

в письменной форме владельцев сертификатов ключей проверки электронных подписей, которые выданы этим удостоверяющим центром и срок действия которых не истек, не менее чем за один месяц до даты прекращения деятельности этого удостоверяющего центра.

В указанном случае после завершения деятельности удостоверяющего центра информация, внесенная в реестр сертификатов, должна быть уничтожена.

В случае прекращения деятельности удостоверяющего центра с переходом его функций другим лицам он должен уведомить об этом в письменной форме владельцев сертификатов ключей проверки электронных подписей, которые выданы этим удостоверяющим центром, и срок действия которых не истек, не менее чем за месяц до даты передачи своих функций.

В указанном случае после завершения деятельности удостоверяющего центра информация, внесенная в реестр сертификатов, должна быть передана лицу, к которому перешли функции удостоверяющего центра, прекратившего свою деятельность.

Порядок реализации функций удостоверяющего центра, осуществления его прав и исполнения обязанностей, определенных настоящей статьей, устанавливается удостоверяющим центром самостоятельно, если иное не установлено Федеральным законом «Об электронной подписи» и иными федеральными законами или принимаемыми в соответствии с ними нормативными правовыми актами либо соглашением между участниками электронного взаимодействия.

Договор об оказании услуг удостоверяющим центром, осуществляющим свою деятельность в отношении неограниченного круга лиц с использованием информационной системы общего пользования, является публичным договором.

Аккредитация удостоверяющего центра осуществляется на добровольной основе. Аккредитация удостоверяющего центра осуществляется на срок три года, если более короткий срок не указан в заявлении удостоверяющего центра.

Федеральный государственный контроль (надзор) в сфере электронной подписи осуществляется федеральным органом исполнительной власти, уполномоченным Правительством РФ.

Предметом федерального государственного контроля (надзора) в сфере электронной подписи является соблюдение аккредитованными удостоверяющими центрами, доверенными третьими сторонами обяза-

тельных требований, установленных Федеральным законом «Об электронной подписи» и принимаемыми в соответствии с ним иными нормативными правовыми актами Российской Федерации.

Организация и осуществление федерального государственного контроля (надзора) в сфере электронной подписи регулируются Федеральным законом от 31.07.2020 № 248-ФЗ «О государственном контроле (надзоре) и муниципальном контроле в Российской Федерации».

Положение о федеральном государственном контроле (надзоре) в сфере электронной подписи утверждается Правительством Российской Федерации (Постановление Правительства РФ от 29.06.2021 № 1044 «Об утверждении Положения о федеральном государственном контроле (надзоре) в сфере электронной подписи»).

При осуществлении федерального государственного контроля (надзора) в сфере электронной подписи плановые контрольные (надзорные) мероприятия не проводятся.

ЭЛЕКТРОННЫЙ ДОКУМЕНТООБОРОТ

Электронное управление документами является следствием дематериализации документов, которая внедряется в новую государственную и корпоративную практику.

Полки освобождены от тяжелых, забытых, пыльных архивов, которые не позволяют правильно использовать содержащуюся в них информацию. Электронный документооборот позволяет оптимально хранить, архивировать и использовать документальные ресурсы. Это компьютеризированный процесс, целью которого является организация и управление электронной информацией и документами.

Внедрение системы электронного документооборота как для частных, так и для государственных структур независимо от их размера направлено на устранение структурных и нормативных препятствий в российской экономике.

Объемы информации и документов в учреждениях и организациях быстро становятся неуправляемыми и могут снизить их производительность. Вот почему важно централизовать и унифицировать их.

Электронный документооборот позволяет:

– упростить работу и внутреннее общение;

– контролировать затраты и сроки на предоставление документов;

– безупречно управлять взаимоотношениями с клиентами (без потери договорных или финансовых документов);

– повысить ценность информации, обогащаемой по мере продвижения несколькими сотрудниками или сторонними субъектами;

– соответствовать требованиям бухгалтерского учета и законодательству в области архивирования.

Преимущества электронного управления документами:

1. Преимущество № 1: долгосрочное решение. Бумага портится, теряется, забывается на дне ящика. В цифровом формате он защищен. Существуют даже сверхзащищенные системы резервного копирования, обеспечивающие дублирование на нескольких серверах.

2. Преимущество № 2: эффективный инструмент исследования. С помощью метаданных можно присвоить документу несколько характеристик, чтобы поисковая система могла найти его по нескольким путям (например, счет-фактуру можно найти, введя имя клиента или название продукта).

3. Преимущество № 3: структурирующая классификация. Документы хранятся в виртуальной библиотеке и доступны каждому через древовидную структуру. Последнее помогает пользователям ориентироваться в том, как организованы папки, подпапки и файлы.

4. Преимущество № 4: снижение затрат, экономия времени. Больше не нужно все распечатывать и складывать в картонные коробки, которые занимают много места, управление осуществляется в цифровом формате. Экономия времени достигается на всех уровнях: при поиске документов, в их классификации, распространении и автоматизации определенных задач (индексация и т.д.).

5. Преимущество № 5: совместная работа и прослеживаемость. Отредактированные файлы обновляются в режиме реального времени, все работают с одними и теми же документами одновременно из нескольких мест. К более ранним версиям можно получить доступ через историю с указанием даты и имени сотрудника, внесшего изменения, с отметкой времени. Это называется управлением версиями, и это позволяет избежать дублирования.

6. Преимущество № 6: обеспечение информационного капитала. Можно управлять правами доступа для защиты своей информации. Существуют также встроенные цифровые хранилища для индексации, поиска и архивирования конфиденциальных файлов, имеющих доказательную ценность, в высокозащищенной среде. В дополнение к этому, этот инструмент не используется в один и тот же момент жизненного цикла документа.

Недостатки электронного управления документами:

– разнообразие данных. В настоящее время и во все большей степени данные поступают из нескольких источников (веб-приложения, электронные сообщения, электронные формы, вики, блоги или мультимедийная реклама (мультимедиа), включая изображения, видео и звук). Это усложняет задачи, связанные с электронным документооборотом, с точки зрения архивирования и индексации. Вот почему решения для электронного управления документами постепенно превращаются в системы управления веб-контентом;

– человеческие и финансовые вложения. Вначале необходимо вложить минимальные средства во внутреннюю организацию, возможно, в аудит, обучение или поддержку, а также в полную дематериализацию существующих бумажных документов. Внедрение электронного документооборота требует полной перестройки организационной структуры и ее привычек, чтобы она была действительно эффективной и максимально быстрой.

В настоящее время в Российской Федерации отсутствует полноценная нормативная, организационная и технологическая основа для юридически значимого электронного документооборота, а также единые подходы к созданию, обороту, хранению и использованию электронных документов участниками документооборота. В настоящее время проникновение электронных документов в хозяйственную деятельность составляет единицы процентов от общего числа всех документов.

За счет внедрения Федеральной налоговой службой РФ формата универсального передаточного документа, который объединяет формат счета-фактуры с форматами первичных учетных документов, в электронную форму переводятся первичные учетные документы.

Причины слабой тенденции миграции бумажного документооборота в электронную форму

- Высокая вариативность форм и видов хозяйственной деятельности, требующая индивидуализации документов для соответствия потребностям участников хозяйственной деятельности
- Большое количество регуляторов со стороны государства, что приводит к отсутствию межведомственной унификации в требованиях к форматам электронных документов безопасности
- Недостаточный уровень доверия участников хозяйственной деятельности к соблюдению режима конфиденциальности электронных документов
- Отсутствие единых подходов к реализации порядка обмена электронными документами
- Отсутствие требований по обязательности электронных документов и стимулов для участников хозяйственной деятельности переходить на электронные документы
- Отсутствие координации между регуляторами в части очередности внедрения электронных документов в оборот, учитывающую полноту документарного оформления фактов хозяйственной жизни в электронной форме
- Недостаточная гармонизация сроков вступления в силу отдельных подзаконных актов, которые должны учитывать изменения прочих федеральных законов

Требования к составлению и оформлению ряда документов, которые необходимы хозяйствующим субъектам для ведения деятельности, а также к порядку их направления и хранения, в настоящий момент регулируются различными нормативно-правовыми актами и федеральными органами исполнительной власти (табл. 11).

Таблица 11

Нормативно-правовые акты,
регулирующие составление и оформление документов

Документы/ отношения	Нормативно-правовые акты
Договорные отношения	Гражданский кодекс Российской Федерации (часть вторая) от 26.01.1996 № 14-ФЗ
Первичные учетные документы	Федеральный закон от 06.12.2011 № 402-ФЗ «О бухгалтерском учете»
Счета-фактуры	Налоговый кодекс Российской Федерации (часть вторая) от 05.08.2000 № 117-ФЗ
Документы, связанные с трудовыми отношениями	Трудовой кодекс Российской Федерации от 30.12.2001 № 197-ФЗ
Архивное хранение документов	Федеральный закон от 22.10.2004 № 125-ФЗ «Об архивном деле в Российской Федерации»
Правила работы с документами, содержащими персональные данные	Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»
Правоотношения по осуществлению закупок для обеспечения государственных и муниципальных нужд	Федеральный закон от 05.04.2013 № 44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд»

Одним из направлений оптимизации работы с документами в хозяйственной деятельности является цифровизация документооборота финансово-хозяйственной деятельности, а именно перевод документов, их оборота и хранения в электронной форме.

Для государства внедрение электронного документооборота влечет следующие положительные эффекты:

– повышение эффективности налогового администрирования и администрирования страховых взносов, увеличение объемов поступления налоговых сборов и страховых взносов;

– сокращение сроков проведения мероприятий налогового контроля;

– сокращение количества документов, представляемых в государственные органы на бумажном носителе, и стимулирование перехода плательщиков на электронный документооборот;

– своевременное выявление и анализ рисков с целью предупреждения нарушений законодательства Российской Федерации о налогах и сборах и оперативного урегулирования спорных вопросов правильности исчисления (удержания), полноты и своевременности уплаты (перечисления) налогов, сборов, страховых взносов;

– повышение эффективности государственного управления за счет снижения административного бремени путем получения и обработки больших данных электронных документов;

– установление правил равной конкуренции за счет прозрачности ведения хозяйственных операций для всех участников хозяйственной деятельности;

– повышение конкурентоспособности национального бизнеса;

– повышение эффективности информационного обмена между налоговыми органами стран, входящих в Евразийский экономический союз;

– естественное стимулирование развития наукоемких технологий;

– сокращение сроков проведения мероприятий налогового контроля и контроля полноты и своевременности уплаты страховых взносов;

– сокращение сроков на подготовку, оформление и обработку документов, возникающих при ведении хозяйственной деятельности.

Цифровизация документов и их оборот стимулирует возникновение новых цифровых сервисов для бизнеса и появление новых компаний в этой области, что позволяет прогнозировать ускоренное развитие цифровой экономики страны.

Помимо этого, цифровая трансформация процесса обмена документами в долгосрочном периоде сокращает транзакционные издержки взаимодействия экономических агентов и позволяет осуществлять государственное управление, основанное на цифровых данных.

За счет сокращения непроизводственных расходов, высвобождения рабочей силы и упрощения условий работы бизнеса, государство может добиться ускорения роста внутреннего валового продукта.

Взаимодействие участников электронного документооборота при обмене электронными документами, формируемыми при планировании, осуществлении закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд, закупок отдельных видов юридических лиц, а также при исполнении государственных и муниципальных контрактов и договоров, осуществляется в соответствии с положениями законодательства Российской Федерации о контрактной системе в сфере закупок и законодательством о закупках отдельных видов юридических лиц (табл. 12).

Таблица 12

Участники электронного документооборота

Участник	Характеристика
Отправитель	Хозяйствующий субъект пли физическое лицо, которое инициирует начало документооборота путем отправки электронных документов получателю
Получатель	Хозяйствующий субъект пли физическое лицо, которое получает электронный документ от отправителя
Оператор электронного документооборота (далее – ОЭД)	Российская организация, соответствующая требованиям, утвержденным федеральным органом исполнительной власти, уполномоченным по контролю и надзору в области налогов и сборов
Оператор электронного документооборота отправителя	Оператор электронного документооборота, заключивший договор по обмену электронными документами с отправителем
Оператор электронного документооборота получателя	Оператор электронного документооборота, заключивший договор по обмену электронным документами с получателем

Обмен электронными документами между участниками электронного документооборота может осуществляться через оператора электронного документооборота или иным согласованным отправителем и получателем способом, а в случае обмена электронными

документами, формируемыми в рамках закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд, закупок отдельных видов юридических лиц, осуществляется в порядке, предусмотренном законодательством Российской Федерации о контрактной системе в сфере закупок и законодательством о закупках отдельных видов юридических лиц.

Порядок обмена электронными документами между участниками электронного документооборота без участия оператора электронного документооборота может осуществляться в соответствии с соглашением, если иное не определено законодательством или иным нормативным правовым актом, а в случае обмена электронными документами, формируемыми в рамках закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд, закупок отдельных видов юридических лиц, в порядке, предусмотренном законодательством Российской Федерации о контрактной системе в сфере закупок и законодательством о закупках отдельных видов юридических лиц.

Операторы электронного документооборота, соответствующие требованиям, утвержденным федеральным органом государственной власти, уполномоченным по контролю и надзору в области налогов и сборов, а также иными нормативными правовыми актами, руководствуются размещенной на сайте федерального органа исполнительной власти, уполномоченного по контролю и надзору в области налогов и сборов, технологией обмена юридически значимыми электронными документами между операторами электронного документооборота.

В случае, если ОЭД заключены договоры как с отправителем, так и с получателем, при осуществлении электронного документооборота указанным ОЭД принципы взаимодействия с данным ОЭД определяются информационной системой ОЭД.

Электронные документы, которыми обмениваются участники электронного документооборота в соответствии с настоящими методическими рекомендациями, могут быть подписаны любым согласованным отправителем и получателем видом электронной подписи, предусмотренным Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи», за исключением отдельных типов документов, к которым нормативными правовыми актами установлены специальные требования.

Обмен электронными документами между участниками электронного документооборота может осуществляться в зашифрованном виде

или незашифрованном виде за исключением случаев, когда законодательством или нормативными правовыми актами урегулировано применение шифрования.

Шифрование не допускается при наличии в договоре между оператором электронного документооборота и участником электронного документооборота условий о проведении оператором электронного документооборота проверки электронных документов.

Очередность направления и подписания многосторонних электронных документов определяется по согласованию участников электронного документооборота, за исключением случаев, когда законодательством или нормативными правовыми актами определена такая очередность.

При обмене многосторонними документами допускается использование только одного канала взаимодействия: с применением оператора электронного документооборота или согласованным участниками способом без участия оператора электронного документооборота. При этом финальная версия электронного документа, подписанная всеми участниками, должна быть получена каждой стороной.

В соответствии со ст. 11.1 Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», органы государственной власти, органы местного самоуправления, а также организации, осуществляющие в соответствии с федеральными законами отдельные публичные полномочия, в пределах своих полномочий обязаны предоставлять по выбору граждан (физических лиц) и организаций информацию в форме электронных документов, подписанных усиленной квалифицированной электронной подписью, и (или) документов на бумажном носителе, за исключением случаев, если иной порядок предоставления такой информации установлен федеральными законами или иными нормативными правовыми актами Российской Федерации, регулирующими правоотношения в установленной сфере деятельности.

Информация, необходимая для осуществления полномочий органов государственной власти и органов местного самоуправления, организаций, осуществляющих в соответствии с федеральными законами отдельные публичные полномочия, может быть представлена гражданами (физическими лицами) и организациями в органы государственной власти, органы местного самоуправления, в организации, осуществляющие в соответствии с федеральными законами отдельные публичные полномочия, в форме электронных документов, подписанных электронной подписью, если иное не установлено федеральными

законами, регулирующими правоотношения в установленной сфере деятельности.

Требования к осуществлению взаимодействия в электронной форме граждан (физических лиц) и организаций с органами государственной власти, органами местного самоуправления, с организациями, осуществляющими в соответствии с федеральными законами отдельные публичные полномочия, и порядок такого взаимодействия устанавливаются Правительством Российской Федерации (Постановление Правительства РФ от 09.06.2016 № 516 «Об утверждении Правил осуществления взаимодействия в электронной форме граждан (физических лиц) и организаций с органами государственной власти, органами местного самоуправления, с организациями, осуществляющими в соответствии с федеральными законами отдельные публичные полномочия») в соответствии с Федеральным законом от 6.04.2011 № 63-ФЗ «Об электронной подписи».

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Информационная безопасность – это набор методов и процессов, которые защищают информацию от несанкционированного использования, доступа, изменения, нарушения или уничтожения.

Данные или контент, которые должны быть защищены, могут быть цифровой информацией, такой как данные, хранящиеся в облаке, или физической информацией, такой как печатные файлы и контракты.

Информационная безопасность подразумевает, прежде всего, защиту данных от несанкционированного использования или доступа, а также обеспечение соответствия информации действующим нормативным актам.

Некоторые без особого различия упоминают термины «информационная безопасность» и «кибербезопасность». Однако эти два термина, хотя и близки по смыслу, имеют некоторые различия. Информационная безопасность на самом деле является компонентом кибербезопасности, который, со своей стороны, относится к более широкому процессу или методу защиты компьютерных ресурсов от внешних атак, помимо информации.

Таким образом, кибербезопасность, которую мы также можем встретить под термином «компьютерная безопасность», является гораздо более широкой областью, чем информационная безопасность.

Все, что связано с мерами или политиками защиты программ, серверов и сетей от несанкционированного доступа, злоупотреблений или других угроз, относится к сфере кибербезопасности. Таким образом, она заботится не только о данных и информации, но и о системах и оборудовании компании.

Существует несколько категорий кибербезопасности:

– безопасность приложений – защищает устройства и программное обеспечение от угроз. Это может быть, например, разработка программного обеспечения с функциями безопасности, такими как шифрование, или разработка исправлений для устранения уязвимостей по мере их появления;

– информационная безопасность – защищает данные независимо от того, хранятся они или передаются;

– сетевая безопасность – предотвращает доступ злоумышленников, будь то вредоносные программы или хакеры, специально нацеленные на сеть, к компьютерной сети компании;

– операционная безопасность – включает в себя предоставление пользователям разрешений и паролей для предоставления им доступа к определенным типам контента или к самой компьютерной сети;

– аварийное восстановление – компонент кибербезопасности, который определяет действия, которые необходимо предпринять в случае атаки, сбоя в работе или потери данных.

Вот некоторые распространенные угрозы, от которых эффективная кибербезопасность может защитить:

– фишинговое мошенничество – ситуация, когда законное на первый взгляд электронное письмо или сообщение побуждает пользователей раскрыть личную информацию;

– вредоносное программное обеспечение – вирусы, трояны или другие компьютерные программы, которые повреждают устройство или предоставляют несанкционированный доступ к компьютерным программам или определенным данным;

– программы-вымогатели – программное обеспечение, установленное на устройстве, которое не позволяет пользователю получить доступ к файлам или программам до выплаты выкупа. Однако выплата выкупа не всегда приводит к удалению вредоносного ПО.

Существуют три основных принципа информационной безопасности: доступность, целостность и конфиденциальность. Цель политики информационной безопасности – соответствовать хотя бы одному из этих критериев. Вместе эти принципы образуют ДВС-триаду:

1) доступность. Данный принцип гарантирует, что авторизованные и правомочные пользователи могут получить доступ к вашему контенту. Доступность означает, что те, кому необходимо загрузить или открыть контент, могут это сделать. Доступ к авторизованному контенту также должен быть быстрым и немедленным. Это избавляет авторизованных пользователей от необходимости ждать, чтобы открыть файл, или от необходимости проходить длительный и утомительный процесс, чтобы получить доступ к нужному им контенту;

2) целостность. Этот принцип относится к состоянию данных или содержимого. Очень важно, чтобы неавторизованные пользователи не могли изменять контент, которым владеет ваша компания. Например, хакер не должен иметь возможности изменять количество или характер ингредиента в рецепте, который вы разработали. Представьте, что сладкий напиток, который вы производите для своих клиентов, таким образом превращается в опасный яд. Хакеры также не должны иметь возможности изменять контракты и повышать или снижать заработную плату ваших сотрудников.

Также важно, чтобы целостность данных вашей компании была защищена от ваших сотрудников, которые могут иметь не самые лучшие намерения. Ревнивый сотрудник не должен иметь возможности получить доступ к личному делу коллеги и изменять его часы, потраченные на проект, или добавлять комментарии или сфальсифицированные дисциплинарные взыскания в свой файл.

Инструменты, которые вы используете для обеспечения конфиденциальности вашего контента, такие как шифрование и защита паролем, также помогают гарантировать его целостность. Есть и другие шаги, которые вы можете предпринять, чтобы восстановить и исправить ситуацию со взломом вашей информации. Если кому-то удастся получить несанкционированный доступ к рецепту или электронной таблице и изменить в них определенную информацию, вы можете восстановить предыдущие версии своего содержимого, чтобы устранить повреждения и восстановить целостность ваших данных;

3) конфиденциальность. Одна из первых вещей, которые могут прийти в голову, когда мы думаем о защите контента компании, – это то, как обеспечить конфиденциальность ее данных и информации. Независимо от того, управляете ли вы контрактами со своими сотрудниками или информацией о клиентах, вы должны убедиться, что данные защищены от несанкционированного доступа пользователей или запросов.

Цель обеспечения конфиденциальности триады DIC-гарантировать конфиденциальность данных. Только лица, имеющие соответствующие полномочия, должны иметь доступ к файлам, которые их содержат.

Сфера применения ИТ-безопасности обширна и часто включает в себя сочетание технологий и решений в области безопасности, которые в совокупности устраняют уязвимости в цифровых устройствах, компьютерных сетях, серверах, базах данных и программных приложениях.

Наиболее часто приводимые примеры ИТ-безопасности включают навыки цифровой безопасности, такие как безопасность конечных точек, облака, сети и приложений. Но компьютерная безопасность также включает меры физической безопасности (замки, удостоверения личности, камеры видеонаблюдения), необходимые для защиты зданий и устройств, в которых хранятся данные и ИТ-активы.

Указом Президента РФ от 05.12.2016 № 646 утверждена Доктрина информационной безопасности Российской Федерации.

Доктрина представляет собой систему официальных взглядов на обеспечение национальной безопасности Российской Федерации в информационной сфере.

Информационные технологии приобрели глобальный трансграничный характер и стали неотъемлемой частью всех сфер деятельности личности, общества и государства. Их эффективное применение является фактором ускорения экономического развития государства и формирования информационного общества.

Информационная сфера играет важную роль в обеспечении реализации стратегических национальных приоритетов Российской Федерации.

Реализация национальных интересов в информационной сфере направлена на формирование безопасной среды оборота достоверной информации и устойчивой к различным видам воздействия информационной инфраструктуры в целях обеспечения конституционных прав и свобод человека и гражданина, стабильного социально-экономического развития страны, а также национальной безопасности Российской Федерации.

Расширение областей применения информационных технологий, являясь фактором развития экономики и совершенствования функционирования общественных и государственных институтов, одновременно порождает новые информационные угрозы.

Национальные интересы в информационной сфере

- Обеспечение и защита конституционных прав и свобод человека и гражданина в части, касающейся получения и использования информации, неприкосновенности частной жизни при использовании информационных технологий, обеспечение информационной поддержки демократических институтов, а также применение информационных технологий в интересах сохранения культурных, исторических и духовно-нравственных ценностей многонационального народа Российской Федерации
- Обеспечение устойчивого и бесперебойного функционирования информационной инфраструктуры, в первую очередь критической информационной инфраструктуры РФ и единой сети электросвязи РФ, в мирное время, в период непосредственной угрозы агрессии и в военное время
- Развитие в РФ отрасли информационных технологий и электронной промышленности, а также совершенствование деятельности производственных, научных и научно-технических организаций по разработке, производству и эксплуатации средств обеспечения информационной безопасности
- Доведение до российской и международной общественности достоверной информации о государственной политике РФ и ее официальной позиции по социально значимым событиям в стране и мире, применение информационных технологий в целях обеспечения национальной безопасности РФ в области культуры
- Содействие формированию системы международной информационной безопасности, направленной на противодействие угрозам использования информационных технологий в целях нарушения стратегической стабильности, на укрепление равноправного стратегического партнерства в области информационной безопасности, а также на защиту суверенитета РФ в информационном пространстве

Возможности трансграничного оборота информации все чаще используются для достижения геополитических, противоречащих международному праву военно-политических, а также террористических, экстремистских, криминальных и иных противоправных целей в ущерб международной безопасности и стратегической стабильности.

При этом практика внедрения информационных технологий без увязки с обеспечением информационной безопасности существенно повышает вероятность проявления информационных угроз.

Расширяются масштабы использования специальными службами отдельных государств средств оказания информационно-психологического воздействия, направленного на дестабилизацию внутриполитической и социальной ситуации в различных регионах мира и приводящего к подрыву суверенитета и нарушению территориальной целостности других государств.

В эту деятельность вовлекаются религиозные, этнические, правозащитные и иные организации, а также отдельные группы граждан, при этом широко используются возможности информационных технологий.

Отмечается тенденция к увеличению в зарубежных средствах массовой информации объема материалов, содержащих предвзятую оценку государственной политики Российской Федерации.

Наращивается информационное воздействие на население России, в первую очередь на молодежь, в целях размывания традиционных российских духовно-нравственных ценностей.

Различные террористические и экстремистские организации широко используют механизмы информационного воздействия на индивидуальное, групповое и общественное сознание в целях нагнетания межнациональной и социальной напряженности, разжигания этнической и религиозной ненависти либо вражды, пропаганды экстремистской идеологии, а также привлечения к террористической деятельности новых сторонников. Такими организациями в противоправных целях активно создаются средства деструктивного воздействия на объекты критической информационной инфраструктуры.

Возрастают масштабы компьютерной преступности, прежде всего в кредитно-финансовой сфере, увеличивается число преступлений, связанных с нарушением конституционных прав и свобод человека и гражданина, в том числе в части, касающейся неприкосновенности частной жизни, личной и семейной тайны, при обработке персональных данных с использованием информационных технологий. При этом методы, способы и средства совершения таких преступлений становятся все изощреннее (табл. 13).

Таблица 13

Состояние информационной безопасности
в различных областях

Область	Характеристика
Оборона	Увеличение масштабов применения отдельными государствами п организациями информационных технологий в военно-политических целях, в том числе для осуществления действий, противоречащих международному праву, направленных на подрыв суверенитета, политической и социальной стабильности, территориальной целостности РФ н ее союзников и представляющих угрозу международному миру, глобальной н региональной безопасности
Государственная и общественная безопасности	Постоянное повышение сложности, увеличение масштабов и рост компьютерных атак на объекты критической информационной инфраструктуры, усиление разведывательной деятельности иностранных государств в отношении РФ, а также нарастание угроз применения информационных технологий в целях нанесение ущерба суверенитету, территориальной целостности, политической и социальной стабильности РФ
Экономическая сфера	Недостаточный уровень развития конкурентоспособных информационных технологий и их использования для производства продукции и оказания услуг. Остается высоким уровень зависимости отечественной промышленности от зарубежных информационных технологий в части, касающейся электронной компонентной базы, программного обеспечения, вычислительной техники и средств связи, что обусловливает зависимость социально-экономического развития РФ от геополитических интересов зарубежных стран
Наука, технология и образование	Недостаточная эффективность научных исследований, направленных на создание перспективных информационных технологий, низкий уровень внедрения отечественных разработок и недостаточное кадровое обеспечение в области информационной безопасности, а также низкая осведомленность граждан в вопросах обеспечения личной информационной безопасности

Окончание табл. 13

Область	Характеристика
Стратегическая стабильность и равноправное стратегическое партнерство	Стремление отдельных государств использовать технологическое превосходство для доминирования в информационном пространстве

Существующее в настоящее время распределение между странами ресурсов, необходимых для обеспечения безопасного и устойчивого функционирования сети «Интернет», не позволяет реализовать совместное справедливое, основанное на принципах доверия управление ими.

Отсутствие международно-правовых норм, регулирующих межгосударственные отношения в информационном пространстве, а также механизмов и процедур их применения, учитывающих специфику информационных технологий, затрудняет формирование системы международной информационной безопасности, направленной на достижение стратегической стабильности и равноправного стратегического партнерства.

Система обеспечения информационной безопасности является частью системы обеспечения национальной безопасности Российской Федерации (табл. 14).

Таблица 14

Стратегические цели обеспечения информационной безопасности в различных областях

Область	Стратегические цели
Оборона страны	Защита жизненно важных интересов личности, общества и государства от внутренних и внешних угроз, связанных с применением информационных технологий в военно-политических целях, противоречащих международному праву, в том числе в целях осуществления враждебных действий и актов агрессии, направленных на подрыв суверенитета, нарушение территориальной целостности государств и представляющих угрозу международному миру

Окончание табл. 14

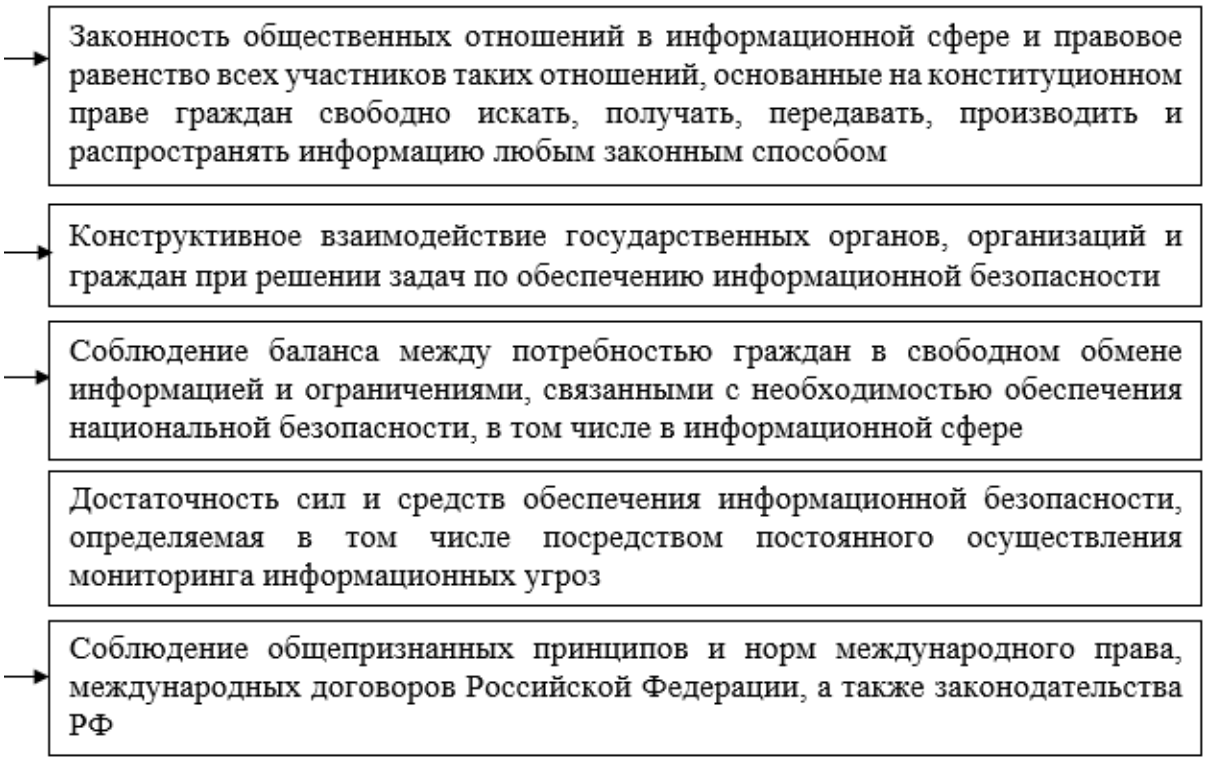
Область	Стратегические цели
Государственная и общественная безопасность	Защита суверенитета, поддержание политической и социальной стабильности, территориальной целостности РФ, обеспечение основных прав и свобод человека и гражданина, а также защита критической информационной инфраструктуры
Экономическая сфера	Сведение к минимально возможному уровню влияния негативных факторов, обусловленных недостаточным уровнем развития отечественной отрасли информационных технологий и электронной промышленности, разработка и производство конкурентоспособных средств обеспечения информационной безопасности
Наука, технология и образование	Поддержка инновационного и ускоренного развития системы обеспечения информационной безопасности, отрасли информационных технологий и электронной промышленности

Обеспечение информационной безопасности осуществляется на основе сочетания законодательной, правоприменительной, правоохранительной, судебной, контрольной и других форм деятельности государственных органов во взаимодействии с органами местного самоуправления, организациями и гражданами.

Система обеспечения информационной безопасности строится на основе разграничения полномочий органов законодательной, исполнительной и судебной власти в данной сфере с учетом предметов ведения федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации, а также органов местного самоуправления, определяемых законодательством Российской Федерации в области обеспечения безопасности.

Состав системы обеспечения информационной безопасности определяется Президентом Российской Федерации.

Принципы деятельности государственных органов по обеспечению информационной безопасности



Задачи государственных органов по обеспечению информационной безопасности представлены в табл. 15

Таблица 15

Задачи государственных органов в рамках деятельности по обеспечению, развитию и совершенствованию системы обеспечения информационной безопасности

Обеспечение информационной безопасности	Развитие и совершенствование обеспечения информационной безопасности
Обеспечение защиты прав и законных интересов граждан и организаций в информационной сфере	Укрепление вертикали управления и централизация сил обеспечения информационной безопасности на федеральном, региональном, муниципальном уровнях, а также на уровне объектов и операторов информационных систем

Окончание табл. 15

Обеспечение информационной безопасности	Развитие и совершенствование обеспечения информационной безопасности
Оценка состояния информационной безопасности, прогнозирование и обнаружение информационных угроз, определение направлений их предотвращения и ликвидации последствий их проявления	Совершенствование форм и методов взаимодействия сил обеспечения информационной безопасности в целях повышения их готовности к противодействию информационным угрозам
Планирование, осуществление и оценка эффективности комплекса мер по обеспечению информационной безопасности	Совершенствование информационно-аналитических и научно-технических аспектов функционирования системы обеспечения информационной безопасности
Организация деятельности и координация взаимодействия сил обеспечения информационной безопасности, совершенствование их правового, организационного, научно-технического, аналитического, кадрового н экономического обеспечения	Повышение эффективности взаимодействия государственных органов, органов местного самоуправления, организаций и граждан при решении задач по обеспечению информационной безопасности
Реализация мер государственной поддержки организаций, осуществляющих деятельность по разработке, производству и эксплуатации средств обеспечения информационной безопасности	–

Реализация Доктрины информационной безопасности России осуществляется на основе отраслевых документов стратегического планирования Российской Федерации.

В целях актуализации таких документов Советом Безопасности Российской Федерации определяется перечень приоритетных направлений обеспечения информационной безопасности на среднесрочную перспективу с учетом положений стратегического прогноза Российской Федерации.

Результаты мониторинга реализации Доктрины информационной безопасности России отражаются в ежегодном докладе Секретаря Совета Безопасности Российской Федерации Президенту Российской Федерации о состоянии национальной безопасности и мерах ее укрепления.

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ

Искусственный интеллект сегодня находится в центре всей нашей деятельности. И не зря! У него есть множество преимуществ. Он затрагивает все отрасли, от самых простых до самых сложных, таких как медицинские исследования или безопасность.

Действительно, все крупные ИТ-компании стремятся создавать программы для искусственного интеллекта, потому что интерес к нему огромен. Несмотря на некоторые препятствия и довольно высокие инвестиционные вложения, получаемая такими компаниями прибыль более чем высока.

В 1956 г. термин «искусственный интеллект» был впервые произнесен Марвином Мински на конференции «Дартмутский летний исследовательский проект по искусственному интеллекту». Многие считают эту конференцию настоящим рождением искусственного интеллекта в том виде, в каком он известен сегодня.

Ключевые моменты в истории искусственного интеллекта:

1943 г. – представлена идея модели, имитирующей клетки мозга;

1950 г. – Алан Тьюринг разрабатывает тест, чтобы выяснить, могут ли машины мыслить, как люди. Был создан первый компьютер на основе нейронных сетей;

1956 г. – впервые используется термин «искусственный интеллект»;

1959 г. – названа концепция «машинного обучения»;

1963 г. – в Стэнфорде создана первая исследовательская лаборатория по искусственному интеллекту;

1966 г. – создан первый чат-бот ELIZA;

1972–1980 гг. – интерес к ИИ падает, что приводит к периоду, известному как «зима ИИ»;

1980 г. – исследования в области ИИ возобновляются с разработкой успешного бизнес-приложения;

1997 г. – произошло важное событие в истории искусственного интеллекта. Система IBM Deep Blue одержала победу над чемпионом мира по шахматам Гари Каспаровым. Впервые машина победила человека;

2002 г. – ИИ начинает использоваться в бытовых пылесосах;

2005 г. – вооруженные силы США начинают использовать роботов;

2006 г. – крупные технологические компании начинают активно использовать ИИ;

2008 г. – Google добавляет распознавание речи в приложения для iPhone;

2011 г. – Watson от IBM побеждает в викторине, демонстрируя понимание языка;

2012 г. – проект Google демонстрирует значительные успехи в обучении ИИ на основе видео;

2014 г. – Google тестирует беспилотный автомобиль; Amazon запускает Alexa;

2016 г. – представлен робот по имени София;

2020 г. – ИИ помогает ускорить разработку вакцины от COVID-19.

Эти события показывают, как ИИ прошел путь от первых концепций до того, что играет важную роль в нашей повседневной жизни.

Искусственный интеллект облегчает деятельность и в повседневной жизни, и в использовании в бизнесе.

Искусственный интеллект – это набор методов, которые заключаются в наделении машины способностями, аналогичными человеческому мозгу. Устройства, запрограммированные на выполнение определенных задач, могут выполнить их точно так же как человек или даже намного лучше. Например, искусственный интеллект позволяет нам разблокировать наш смартфон, не двигая пальцем; может помочь в диагностике заболеваний или разработке новых лекарственных препаратов.

Искусственный интеллект может использоваться в различных типах машин, а не только в компьютере. Другими словами, это программное обеспечение, которое позволяет устройствам обрабатывать данные и принимать разумные решения.

Область применения искусственного интеллекта практически не ограничена, поскольку он постоянно развивается вместе с развитием информационных технологий.

Личные помощники Алиса, Алекса, Сири, Google Assistant, Кортана или Маруся прекрасно иллюстрируют, что искусственный интеллект может привнести в нашу повседневную жизнь много полезного: они организуют наш распорядок дня, заказывают еду, управляют умным домом, отправляют сообщения и т. д. Достаточно голосовой команды, чтобы искусственный интеллект взял на себя ответственность за то, чтобы все работало на нас.

Другой пример касается автозаполнения в смартфонах. Клавиатура, которая угадывает, что вы собираетесь написать, или автоматически исправляет ошибки, также работает на искусственном интеллекте. Кроме того, распознавание лиц для разблокировки экранов или идентификации лиц в социальных сетях – это тоже все благодаря искусственному интеллекту.

Как было упомянуто ранее, искусственный интеллект присутствует во многих отраслях. Хотя по своей сути речь идет о компьютерной программе, в своих приложениях она выходит далеко за рамки этой области.

Участие искусственного интеллекта в области здравоохранения превосходит все ожидания. Во-первых, с точки зрения удаленного мониторинга, он позволяет анализировать данные о состоянии здоровья пациентов. Это позволяет ускорить диагностику и поиск методов лечения, так как устройства с искусственным интеллектом могут обрабатывать большие объемы данных в рекордно короткие сроки. В сочетании с робототехникой искусственный интеллект помогает в медицинских учреждениях. Роботы-медсестры и роботы-хирурги предоставляют возможность оказывать высокоточную медицинскую помощь.

Еще одна ключевая область, которая использует преимущества искусственного интеллекта – это транспорт. Благодаря искусственному интеллекту автомобили с автоматическим управлением ездят без водителя. Используя «компьютерное зрение» и различные датчики, искусственный интеллект дает возможность транспортным средствам распознавать дорожные знаки и вообще обстановку на дороге. Существуют даже решения с искусственным интеллектом, которые позволяют улучшить управление автомобилем и снизить риск аварий. Искусственный интеллект может использоваться для контроля движения транспорта, предлагая решения для сокращения пробок на дорогах или загруженности общественного транспорта, в том числе и метро.

В области финансовых услуг вклад искусственного интеллекта заключается в сборе информации и улучшении отношений с клиентами. Система, построенная на искусственном интеллекте, например, позволяет определить предпочтения клиентов, следовательно, консультантам легче предлагать эффективные решения в соответствии с потребностями клиентов.

Возможно, одним из самых больших преимуществ использования искусственного интеллекта на предприятии, является автоматизация. Для повторяющихся операций (задач), требующих большого количества времени, это одно из лучших решений.

С помощью алгоритмов обучения искусственный интеллект может изучать и имитировать действия человека более быстро и эффективно. Кроме того, автоматизируя определенные процессы, компания может высвободить ресурсы в пользу более важных видов производственной деятельности. Например, управление запасами: вычислительные и аналитические возможности искусственного интеллекта позволяют ему автоматически обрабатывать документы и прогнозировать потребности в запасах.

Кроме того, эта технология хорошо известна своим положительным эффектом в принятии бизнес-решений. Это касается предоставления и повышения согласованности данных, и анализа тенденций развития бизнеса. Также искусственный интеллект способен определять возможные источники проблем, сбоев, рисков. Его как положительные, так и отрицательные прогнозы позволяют разрабатывать правильные, адекватные и более эффективные стратегии и избегать кризисных ситуаций.

Цифровизация и автоматизация задач имеют еще одно важное преимущество – снижение риска ошибок. Действительно, в этом вся разница между машиной и человеком. У искусственного интеллекта значительно более высокий уровень точности.

Искусственный интеллект является одной из самых важных технологий, которые доступны человеку в настоящее время. Уже сейчас благодаря искусственному интеллекту происходит рост мировой экономики, ускорение инноваций во всех областях науки, повышение качества жизни населения, доступности и качества медицинской помощи, качества образования, производительности труда и качества отдыха.

Технологии искусственного интеллекта являются областью международной конкуренции. Технологическое лидерство в области искусственного интеллекта может позволить государствам достичь значимых результатов по основным направлениям социально-экономического развития.

Искусственный интеллект становится важным игроком на рынке технологий. По всему миру организации создают инновационные инструменты искусственного интеллекта и машинного обучения.

Искусственный интеллект формирует будущее всех отраслей и способствует развитию новых технологий, таких как большие данные, робототехника и Интернет вещей (IoT).

Благодаря реализации Указа Президента РФ от 10.10.2019 № 490 «О развитии искусственного интеллекта в Российской Федерации»

(вместе с «Национальной стратегией развития искусственного интеллекта на период до 2030 года») должны быть созданы условия для эффективного взаимодействия государства, организаций, в том числе научных, и граждан в сфере развития искусственного интеллекта, что позволит российским технологиям искусственного интеллекта занять значительную долю мирового рынка.

Российская Федерация обладает существенным потенциалом для того, чтобы стать одним из международных лидеров в развитии и использовании технологий искусственного интеллекта.

Основные принципы развития и использования технологий искусственного интеллекта

- *Защита прав и свобод человека*: обеспечение защиты прав и свобод человека, гарантированных законодательством РФ, международными договорами РФ и общепризнанными принципами, и нормами международного права
- *Безопасность:* недопустимость использования ИИ в целях умышленного причинения вреда гражданам и организациям, предупреждение и минимизация рисков возникновения негативных последствий использования технологий ИИ
- *Прозрачность*: объяснимость работы ИИ и процесса достижения им результатов, недискриминационный доступ пользователей продуктов, которые созданы с использованием технологий ИИ
- *Технологический суверенитет*: обеспечение необходимого уровня самостоятельности РФ в области ИИ, в том числе посредством преимущественного использования отечественных технологий ИИ
- *Целостность инновационного цикла*: обеспечение тесного взаимодействия научных исследований и разработок в ИИ с реальным сектором экономики
- *Открытость и доступность*: недопущение ограничения доступа организаций-разработчиков отечественных технологий ИИ, граждан, организаций, осуществляющих деятельность в различных отраслях экономики
- *Защищенность*: безопасность и правовая охрана технологий ИИ, разграничение ответственности организаций-разработчиков и пользователей технологий ИИ исходя из характера и степени причиненного вреда

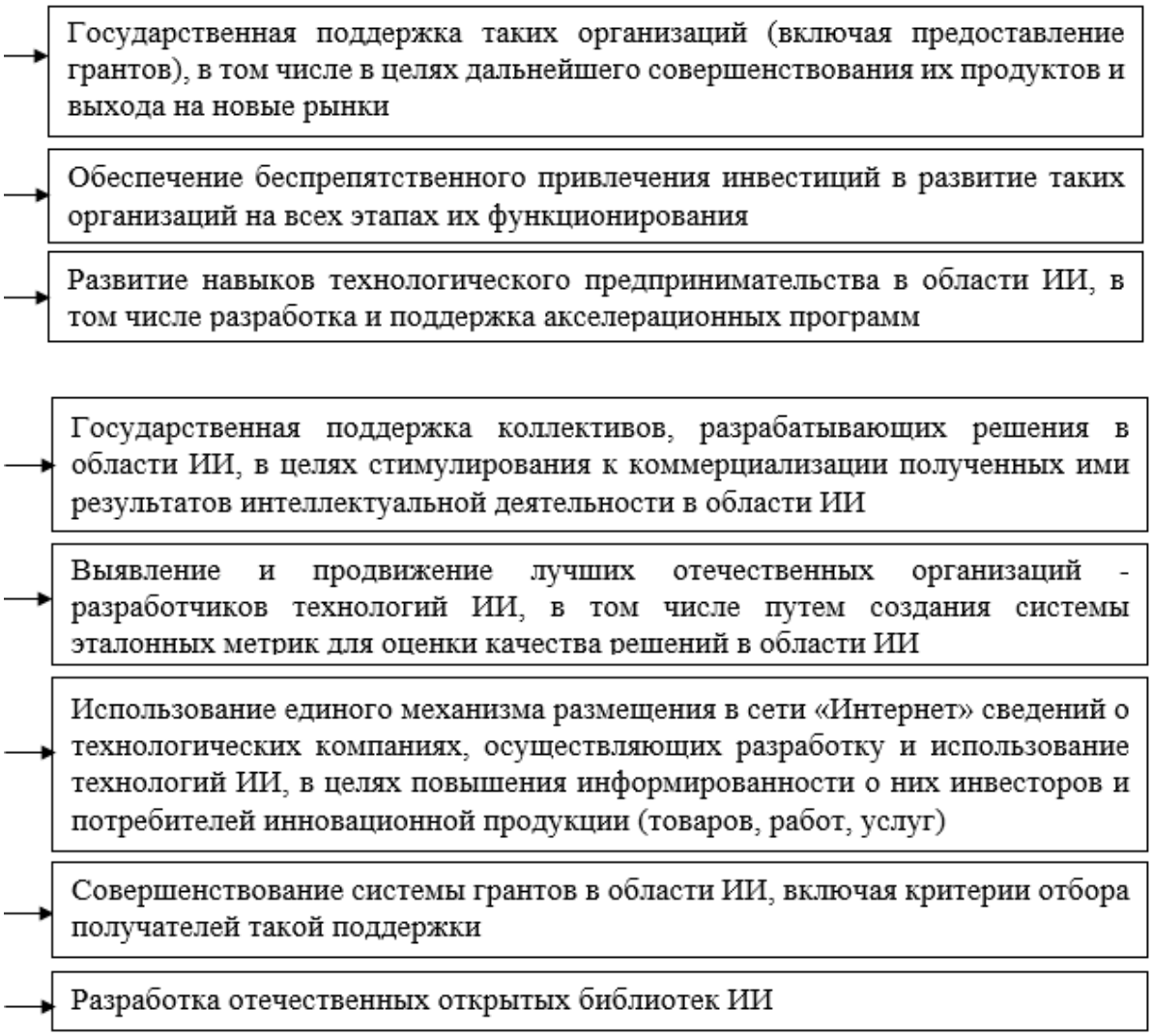
Целями развития искусственного интеллекта в Российской Федерации являются обеспечение роста благосостояния и качества жизни ее населения, обеспечение национальной безопасности и правопорядка,

достижение устойчивой конкурентоспособности российской экономики, в том числе лидирующих позиций в мире в области искусственного интеллекта.

Основные задачи развития искусственного интеллекта в Российской Федерации

- Повышение доступности инфраструктуры, необходимой для развития технологий искусственного интеллекта
- Поддержка организаций-разработчиков технологий искусственного интеллекта
- Поддержка научных исследований и разработок в целях обеспечения опережающего развития искусственного интеллекта
- Повышение уровня компетенций в области искусственного интеллекта и уровня информированности граждан о технологиях искусственного интеллекта
- Стимулирование внедрения технологий искусственного интеллекта в отраслях экономики и социальной сферы
- Обязательное внедрение доверенных технологий искусственного интеллекта в тех областях его использования, в которых может быть нанесен ущерб безопасности РФ
- Создание комплексной системы нормативно-правового регулирования общественных отношений, связанных с развитием и использованием технологий искусственного интеллекта, обеспечение безопасности применения таких технологий
- Укрепление международного сотрудничества в области использования технологий искусственного интеллекта

Основные направления оказания поддержки организациям-разработчикам технологий искусственного интеллекта



Основными направлениями повышения уровня компетенций в области искусственного интеллекта и уровня информированности граждан о технологиях искусственного интеллекта являются:

– внедрение в образовательных организациях высшего образования комплексной системы подготовки квалифицированных кадров в области разработки и использования технологий искусственного интеллекта;

– развитие навыков создания моделей искусственного интеллекта, в том числе на основе передовых научных достижений, у специалистов в области искусственного интеллекта;

– развитие навыков использования технологий искусственного интеллекта у выпускников образовательных организаций высшего об-

разования посредством включения модулей по искусственному интеллекту в каждую образовательную программу (с учетом особенностей, связанных с отраслевой принадлежностью и направлениями подготовки);

– развитие навыков сбора достоверной информации о событиях, явлениях и процессах в целях использования такой информации для развития технологий искусственного интеллекта;

– повышение качества математического и естественно-научного образования, включая информатику, а также качества обучения основам искусственного интеллекта (в рамках как основных, так и дополнительных образовательных программ), создание условий для привлечения обучающихся к углубленной подготовке по этим направлениям;

– развитие у талантливой молодежи интереса к изучению и разработке технологий искусственного интеллекта;

– создание для специалистов в области искусственного интеллекта, проживающих за рубежом, стимулов работать в российских организациях, включая упрощенный процесс получения виз такими специалистами и их родственниками и обеспечение им комфортных условий для работы и проживания в Российской Федерации;

– информирование граждан и организаций о принципах использования технологий искусственного интеллекта;

– популяризация и продвижение отечественных платформ онлайн-обучения, предоставляющих возможность получения свободного доступа к сертифицированным обучающим материалам в области искусственного интеллекта и современных информационных технологий.

Основной целью совершенствования нормативно-правового регулирования общественных отношений, связанных с развитием и использованием технологий искусственного интеллекта, на период до 2030 г. должно стать создание в Российской Федерации благоприятных нормативно-правовых условий для разработки, внедрения и использования технологий искусственного интеллекта и решений, разработанных на их основе, с учетом обеспечения защиты прав и свобод человека и безопасности Российской Федерации.

Принцип нормативно-правового регулирования общественных отношений, связанных с развитием и использованием технологий искусственного интеллекта перечислен в табл. 16.

Таблица 16

Основные принципы нормативно-правового регулирования общественных отношений, связанных с развитием и использованием технологий искусственного интеллекта

Принцип	Содержание принципа
Безопасность	Разработка, создание и использование технологий ИИ для тех областей их применения, в которых может быть нанесен ущерб безопасности РФ, осуществляются в соответствии с требованиями информационной безопасности доверенных технологий ИИ
Гуманистический подход	При развитии и регулировании технологий ИИ человек, его права и свободы должны рассматриваться как высшая ценность
Уважение автономии и свободы воли человека	Сохранение автономии и свободы воли человека в принятии им решений нормативно-правовое регулирование в области НИ не должно умалять право выбора и интеллектуальные способности человека
Отсутствие дискриминации	Алгоритмы и наборы данных, методы обработки используемых для машинного обучения данных, применяемые для группирования и (или) классификации данных, касающихся отдельных лиц или групп лиц, не должны способствовать их умышленной дискриминации
Риск – ориентированный подход	Уровень проработки, характер и детализация изменений при регулировании вопросов в области ИИ должны соответствовать уровню рисков, создаваемых конкретными технологиями и системами ИИ для интересов человека и общества
Ответственность	Не допускается делегирование системам ИИ ответственного нравственного выбора, а также делегирование ответственности за последствия принятия решений
Квалифицированная экспертная оценка	При разработке нормативно-правового регулирования, касающегося развития технологий искусственного интеллекта, должно быть обеспечено проведение его соответствующей оценки специалистами в области искусственного интеллекта

Основными направлениями создания комплексной системы нормативно-правового регулирования общественных отношений, связанных с развитием и использованием технологий искусственного интеллекта, и обеспечения безопасности применения таких технологий являются:

1) закрепление благоприятных нормативно-правовых условий для разработки и внедрения технологий искусственного интеллекта (отсутствие излишних нормативно-правовых барьеров, ограничивающих развитие технологий искусственного интеллекта) в документах стратегического планирования во всех сферах использования таких технологий;

2) законодательное обеспечение возможности доступа разработчиков технологий искусственного интеллекта к различным видам данных;

3) устранение необоснованных нормативно-правовых ограничений для разработки, внедрения и использования отечественных больших генеративных моделей (в том числе определение границ ответственности разработчиков таких моделей и создание возможностей для обучения больших генеративных моделей на больших массивах информации с учетом требований законодательства Российской Федерации);

4) разработка правил использования технологий искусственного интеллекта на основе результатов обсуждений с участием широкого круга заинтересованных сторон для решения наиболее сложных вопросов развития технологий искусственного интеллекта, в частности касающихся условий делегирования информационным системам, функционирующим на основе искусственного интеллекта, возможности принятия отдельных решений (за исключением решений, которые могут привести к нарушению прав и законных интересов граждан), в том числе при исполнении государственными органами государственных функций (за исключением решений, связанных с осуществлением функций по обеспечению безопасности населения и государства);

5) совершенствование механизмов регулирования экспериментальных правовых режимов посредством упрощения процедур создания и изменения таких режимов;

6) совершенствование этических правил в области искусственного интеллекта, распространение их действия на российские и иностранные организации, а также на органы публичной власти, проведение широкого общественного обсуждения для выявления и решения основных спорных этических вопросов, связанных с внедрением технологий искусственного интеллекта и взаимодействием человека с искусственным интеллектом;

7) формирование механизма оценки рисков нарушения этических норм при внедрении технологий искусственного интеллекта в отраслях экономики и социальной сферы;

8) формирование перечня областей использования технологий искусственного интеллекта, в которых может быть нанесен ущерб безопасности Российской Федерации;

9) разработка требований информационной безопасности в отношении технологий искусственного интеллекта;

10) совершенствование комплекса национальных стандартов в области искусственного интеллекта, в том числе направленных на унификацию терминологии и способов оценки соответствия технологий искусственного интеллекта требованиям законодательства Российской Федерации, а также на описание разработанных российскими специалистами лучших практик использования технологий искусственного интеллекта и обеспечения их совместимости с иной информационной инфраструктурой;

11) создание системы оценки соответствия технологий искусственного интеллекта требованиям законодательства Российской Федерации, в том числе в области информационной безопасности;

12) определение правил работы с большими генеративными моделями и их использования;

13) создание эффективной системы оценки результатов внедрения технологий искусственного интеллекта, включая экономические, социальные, этические, экологические и институциональные результаты;

14) разработка нормативно-правового регулирования в области обеспечения качества и доступности государственных данных;

15) создание и ежегодное обновление мирового индекса комфортности регулирования использования технологий искусственного интеллекта с оценкой законодательства не менее чем 30 государств – лидеров в сфере искусственного интеллекта;

16) обеспечение информационной безопасности при разработке, внедрении и использовании технологий искусственного интеллекта;

17) создание условий для разработки и развития нормативно-правового регулирования обеспечения достоверности исходных данных;

18) ежегодное проведение национальных и международных форумов и общественных дискуссий об этических аспектах разработки и внедрения технологий искусственного интеллекта, о социально-гуманитарных последствиях массового внедрения таких технологий.

ФЕДЕРАЛЬНЫЙ ГОСУДАРСТВЕННЫЙ КОНТРОЛЬ (НАДЗОР) ЗА СОБЛЮДЕНИЕМ ТРЕБОВАНИЙ В СВЯЗИ С РАСПРОСТРАНЕНИЕМ ИНФОРМАЦИИ В ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЯХ, В ТОМ ЧИСЛЕ В СЕТИ «ИНТЕРНЕТ»

Государственный контроль (надзор) осуществляется Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций и ее территориальными органами.

Предмет государственного контроля (надзора) – соблюдение контролируемыми лицами обязательных требований в связи с распространением информации в информационно-телекоммуникационных сетях, в том числе в сети «Интернет», установленных Федеральным законом «Об информации, информационных технологиях и о защите информации», другими федеральными законами и принимаемыми в соответствии с ними иными нормативными правовыми актами Российской Федерации.

Объект государственного контроля (надзора) – деятельность контролируемых лиц в области распространения информации в информационно-телекоммуникационных сетях, в том числе в сети «Интернет».

Учет объекта государственного контроля (надзора) осуществляется с использованием единой информационной системы контрольного (надзорного) органа посредством сбора, обработки, анализа и учета информации об объекте государственного контроля (надзора), представляемой в контрольный (надзорный орган и его территориальные органы в соответствии с нормативными правовыми актами Российской Федерации, информации, получаемой в рамках межведомственного информационного взаимодействия, а также общедоступной информации.

При осуществлении государственного контроля (надзора) применяется система оценки и управления рисками.

Контрольный (надзорный) орган и его территориальные органы при осуществлении государственного контроля (надзора) относят поднадзорный объект государственного контроля (надзора) к одной из следующих категорий риска причинения вреда (ущерба):

– значительный риск;
– умеренный риск;
– низкий риск.

Плановые контрольные (надзорные) мероприятия в отношении объекта контроля в зависимости от присвоенной категории риска проводятся со следующей периодичностью:

– в отношении объекта контроля, отнесенного к категории значительного риска, – документарная или выездная проверка с периодичностью один раз в три года;

– в отношении объекта контроля, отнесенного к категории умеренного риска, – документарная или выездная проверка с периодичностью один раз в пять лет;

– в отношении объекта, отнесенного к категории низкого риска, плановые контрольные (надзорные) мероприятия не проводятся.

При осуществлении государственного контроля (надзора) могут проводиться следующие виды профилактических мероприятий:

1. Информирование.

Информирование контролируемых лиц по вопросам соблюдения обязательных требований осуществляется посредством размещения соответствующих сведений на официальном сайте контрольного (надзорного) органа в сети «Интернет», в средствах массовой информации, в личных кабинетах контролируемых лиц в информационной системе.

Контрольный (надзорный) орган размещает и поддерживает в актуальном состоянии на своем официальном сайте в сети «Интернет» сведения, предусмотренные ст. 46 Федерального закона «О государственном контроле (надзоре) и муниципальном контроле в Российской Федерации».

2. Обобщение правоприменительной практики.

Обобщение правоприменительной практики организации и проведения государственного контроля (надзора) осуществляется один раз в год. По итогам обобщения правоприменительной практики готовится доклад о правоприменительной практике.

Доклад о правоприменительной практике утверждается приказом (распоряжением) руководителя контрольного (надзорного) органа не позднее 31 марта года, следующего за отчетным, и размещается на официальном сайте в сети «Интернет» не позднее трех рабочих дней со дня его утверждения.

3. Объявление предостережения.

В случае наличия у контрольного (надзорного) органа и (или) его территориального органа сведений о готовящихся нарушениях обязательных требований или о признаках нарушений обязательных требований и (или) в случае отсутствия подтвержденных данных о том, что нарушение обязательных требований причинило вред (ущерб) охраняемым законом ценностям либо создало угрозу причинения вреда (ущерба) охраняемым законом ценностям, контрольный (надзорный) орган или его территориальный орган в соответствии со ст. 49 Федерального закона «О государственном контроле (надзоре) и муниципальном контроле в Российской Федерации» объявляет контролируемому лицу предостережение о недопустимости нарушения обязательных требований, предлагает ему принять меры по обеспечению соблюдения обязательных требований.

Контролируемое лицо вправе в течение десяти рабочих дней со дня получения предостережения подать в контрольный (надзорный) орган или его территориальный орган возражение в отношении предостережения (далее – возражение).

В возражении контролируемым лицом указываются:

– наименование юридического лица или фамилия, имя, отчество (при наличии) индивидуального предпринимателя;

– дата и номер предостережения, направленного в адрес контролируемого лица;

– обоснование позиции в отношении указанных в предостережении действий (бездействия) контролируемого лица, которые приводят или могут привести к нарушению обязательных требований;

– иные документы, подтверждающие обоснованность таких возражений, или их заверенные копии (при наличии).

Возражения направляются контролируемым лицом в электронной форме на адрес электронной почты контрольного (надзорного) органа или его территориального органа, либо в бумажном виде почтовым отправлением, либо посредством личного кабинета контролируемого лица в информационной системе или иными указанными в предостережении способами.

Возражение рассматривается в течение 20 рабочих дней со дня регистрации возражения.

По результатам рассмотрения возражения принимается одно из следующих решений:

– удовлетворить возражение в форме отмены объявленного предостережения;

– отказать в удовлетворении возражения.

Не позднее дня, следующего за днем принятия решения, контролируемому лицу, подавшему возражение, направляется в письменной форме и по его желанию в электронной форме мотивированный ответ о результатах рассмотрения возражения.

4. Консультирование.

Консультирование может осуществляться должностным лицом контрольного (надзорного) органа или его территориального органа по телефону, посредством видео-конференц-связи, на личном приеме либо в ходе проведения профилактического мероприятия, контрольного (надзорного) мероприятия.

Консультирование осуществляется по следующим вопросам:

– порядок осуществления государственного контроля (надзора);

– порядок совершения контрольных (надзорных) действий должностными лицами контрольного (надзорного) органа;

– положения обязательных требований, ограничений, порядков и правил, установленных законодательством Российской Федерации в связи с распространением информации в информационно-телекоммуникационных сетях, в том числе в сети «Интернет».

В случае поступления в контрольный (надзорный) орган и (или) его территориальные органы пяти и более однотипных обращений контролируемых лиц или их представителей консультирование осуществляется посредством размещения на официальных сайтах в сети «Интернет» контрольного (надзорного) органа и (или) его территориальных органов письменных разъяснений по изложенным в обращениях вопросам.

5. Профилактический визит.

Обязательные профилактические визиты проводятся в отношении контролируемых лиц, приступающих к осуществлению деятельности в связи с распространением информации в информационно-телекоммуникационных сетях, в том числе в сети «Интернет», а также в отношении объекта контроля, отнесенного к категории значительного риска.

Профилактический визит проводится контрольным (надзорным) органом или его территориальным органом в форме профилактической беседы по месту осуществления деятельности контролируемого лица либо путем использования видео-конференц-связи в следующем порядке:

– уполномоченным должностным лицом контрольного (надзорного) органа или его территориального органа принимается решение

о проведении профилактического визита в отношении контролируемого лица в форме профилактической беседы или путем использования видео-конференц-связи, определяются дата, время и лица контрольного (надзорного) органа или его территориального органа, уполномоченные на его проведение;

– контролируемое лицо уведомляется любым доступным способом, позволяющим проконтролировать получение уведомления, не позднее чем за пять рабочих дней до даты проведения профилактического визита;

– в уведомлении контролируемому лицу предлагается определить лицо (лица), уполномоченное (уполномоченные) на взаимодействие с уполномоченными лицами контрольного (надзорного) органа или его территориального органа в ходе проведения профилактического визита;

– в случае принятия решения о проведении профилактического визита путем использования видео-конференц-связи в уведомлении указываются сведения, необходимые для установления связи между контрольным (надзорным) органом или его территориальным органом и контролируемым лицом;

– в ходе профилактического визита контролируемое лицо информируется об обязательных требованиях, предъявляемых к объекту контроля, его соответствии критериям риска, основаниях и о рекомендуемых способах снижения категории риска, а также о видах, содержании и об интенсивности контрольных (надзорных) мероприятий, проводимых в отношении объекта контроля, исходя из его отнесения к соответствующей категории риска.

Контролируемое лицо вправе отказаться от проведения обязательного профилактического визита, уведомив об этом контрольный (надзорный) орган или его территориальный орган не позднее чем за три рабочих дня до даты его проведения.

Профилактический визит проводится в течение одного рабочего дня.

При проведении профилактического визита гражданам, организациям не могут выдаваться предписания об устранении нарушений обязательных требований. Разъяснения, полученные контролируемым лицом в ходе профилактического визита, носят рекомендательный характер.

В случае если при проведении профилактического визита установлено, что объект контроля представляет явную непосредственную угрозу причинения вреда (ущерба) охраняемым законом ценностям

или такой вред (ущерб) причинен, должностное лицо (лица) незамедлительно направляет информацию об этом уполномоченному должностному лицу контрольного (надзорного) органа или его территориального органа для принятия решения о проведении контрольных (надзорных) мероприятий.

Контрольный (надзорный) орган или его территориальные органы осуществляют учет профилактических визитов.

Государственный контроль (надзор) осуществляется посредством проведения следующих контрольных (надзорных) мероприятий:

– документарная проверка;
– выездная проверка.

При осуществлении государственного контроля (надзора) могут проводиться внеплановые контрольные (надзорные) мероприятия. Организация внеплановых контрольных (надзорных) мероприятий осуществляется в соответствии с положениями ст. 66 Федерального закона «О государственном контроле (надзоре) и муниципальном контроле в Российской Федерации».

Плановые контрольные (надзорные) мероприятия проводятся на основании плана проведения плановых контрольных (надзорных) мероприятий на очередной календарный год, формируемого контрольным (надзорным) органом и подлежащего согласованию с органами прокуратуры.

В решении о проведении контрольного (надзорного) мероприятия указываются сведения, установленные ч. 1 ст. 64 Федерального закона «О государственном контроле (надзоре) и муниципальном контроле в Российской Федерации», а также срок проведения контрольного (надзорного) мероприятия.

Для фиксации инспектором и лицом, привлекаемым к совершению контрольных (надзорных) действий, доказательств нарушений обязательных требований могут использоваться фотосъемка, аудио- и видеозапись в случае выездной проверки.

Фиксация нарушений обязательных требований при помощи фотосъемки проводится не менее чем двумя снимками каждого из выявленных нарушений обязательных требований.

Аудио- и видеозапись осуществляется в ходе проведения контрольного (надзорного) мероприятия непрерывно, с уведомлением в начале и конце записи о дате, месте, времени начала и окончания осуществления записи. В ходе записи подробно фиксируются и указы-

ваются место и характер выявленного нарушения обязательных требований. Результаты проведения фотосъемки, аудио- и видеозаписи являются приложением к акту контрольного (надзорного) мероприятия.

Использование фотосъемки и видеозаписи для фиксации доказательств нарушений обязательных требований осуществляется с учетом требований законодательства Российской Федерации о защите государственной тайны.

Если в ходе контрольных (надзорных) мероприятий осуществлялись фотосъемка, аудио- и (или) видеозапись, то об этом делается отметка в акте контрольного (надзорного) мероприятия. В этом случае материалы фотографирования, аудио- и (или) видеозаписи прилагаются к материалам контрольного (надзорного) мероприятия.

Индивидуальный предприниматель, гражданин, являющиеся контролируемыми лицами, вправе представить в контрольный (надзорный) орган информацию о невозможности присутствия при проведении контрольного (надзорного) мероприятия в случаях временной нетрудоспособности или смерти близкого родственника, подтвержденных соответствующими документами, в связи с чем проведение контрольного (надзорного) мероприятия переносится контрольным (надзорным) органом на срок, необходимый для устранения обстоятельств, послуживших поводом для данного обращения индивидуального предпринимателя, гражданина в контрольный (надзорный) орган.

В ходе документарной проверки могут совершаться следующие контрольные (надзорные) действия:

– получение письменных объяснений;
– истребование документов.

Сведения о принятом решении о проведении документарной проверки размещаются в едином реестре контрольных (надзорных) мероприятий в соответствии с правилами формирования и ведения единого реестра контрольных (надзорных) мероприятий, утверждаемыми Правительством Российской Федерации.

Документарная проверка проводится по месту нахождения контрольного (надзорного) органа или его территориального органа.

Предметом документарной проверки являются сведения, содержащиеся в документах контролируемых лиц, устанавливающих их организационно-правовую форму, права и обязанности, а также документы, используемые при осуществлении их деятельности и связанные с исполнением ими обязательных требований и решений контрольного (надзорного) органа.

В ходе документарной проверки рассматриваются документы контролируемых лиц, имеющиеся в распоряжении контрольного (надзорного) органа и (или) его территориальных органов, результаты предыдущих контрольных (надзорных) мероприятий, материалы рассмотрения дел об административных правонарушениях, иные документы о результатах осуществленного в отношении этих контролируемых лиц государственного контроля (надзора).

Срок проведения документарной проверки не может превышать десяти рабочих дней. В указанный срок не включается период с момента направления контролируемому лицу требования представить необходимые для рассмотрения в ходе документарной проверки документы до момента представления указанных в требовании документов, а также период с момента направления контролируемому лицу информации о выявлении ошибок и (или) противоречий в представленных контролируемым лицом документах либо о несоответствии сведений, содержащихся в этих документах, сведениям, содержащимся в имеющихся у контрольного (надзорного) органа и (или) его территориального органа документах и (или) полученных при осуществлении государственного контроля (надзора), и требования представить необходимые пояснения в письменной форме до момента представления указанных пояснений в контрольный (надзорный) орган или его территориальный орган.

В ходе выездной проверки могут совершаться следующие контрольные (надзорные) действия:

– осмотр;
– получение письменных объяснений;
– истребование документов.

Выездная проверка проводится посредством взаимодействия с конкретным контролируемым лицом в целях оценки соблюдения таким лицом обязательных требований, а также оценки выполнения решений контрольного (надзорного) органа и его территориального органа.

Выездная проверка проводится по месту нахождения (осуществления деятельности) контролируемого лица (его филиалов, представительств, обособленных структурных подразделений).

Выездная проверка проводится в случае, если не представляется возможным:

– удостовериться в полноте и достоверности сведений, которые содержатся в находящихся в распоряжении контрольного (надзорного)

органа и его территориального органа или в запрашиваемых им документах и объяснениях контролируемого лица;

– оценить соответствие деятельности, действий (бездействия) контролируемого лица обязательным требованиям без выезда на указанное место и совершить необходимые контрольные (надзорные) действия, предусмотренные в рамках проведения документарной проверки.

О проведении выездной проверки контролируемое лицо уведомляется в порядке, предусмотренном ст. 21 Федерального закона «О государственном контроле (надзоре) и муниципальном контроле в Российской Федерации», посредством направления копии решения о проведении выездной проверки не позднее чем за 24 часа до ее начала.

Срок проведения выездной проверки составляет 10 рабочих дней. В отношении одного субъекта малого предпринимательства общий срок взаимодействия в ходе проведения выездной проверки составляет 50 часов для малого предприятия и 15 часов для микропредприятия. Срок проведения выездной проверки в отношении организации, осуществляющей свою деятельность на территориях нескольких субъектов Российской Федерации, устанавливается отдельно по каждому филиалу, представительству, обособленному структурному подразделению организации.

По окончании проведения контрольного (надзорного) мероприятия, предусматривающего взаимодействие с контролируемым лицом, составляется акт контрольного (надзорного) мероприятия (далее – акт). Оформление акта производится в соответствии с порядком, установленным Федеральным законом «О государственном контроле (надзоре) и муниципальном контроле в Российской Федерации».

В случае выявления при проведении контрольного (надзорного) мероприятия нарушения обязательных требований контролируемым лицом контрольным (надзорным) органом или его территориальным органом в порядке, предусмотренном Федеральным законом «О государственном контроле (надзоре) и муниципальном контроле в Российской Федерации», выдается предписание об устранении выявленных нарушений обязательных требований.

В случае несогласия с фактами и выводами, изложенными в акте, контролируемое лицо вправе направить жалобу в порядке, предусмотренном Федеральным законом «О государственном контроле (надзоре) и муниципальном контроле в Российской Федерации».

Рассмотрение жалоб осуществляется контрольным (надзорным) органом или его территориальным органом в порядке и сроки, которые установлены Федеральным законом «О государственном контроле (надзоре) и муниципальном контроле в Российской Федерации».

Решение контрольного (надзорного) органа или его территориального органа, содержащее обоснование принятого решения, срок и порядок его исполнения, размещается в личном кабинете контролируемого лица на едином портале государственных и муниципальных услуг и (или) региональном портале государственных и муниципальных услуг не позднее одного рабочего дня со дня его принятия.

Ключевым показателем государственного контроля (надзора) является соотношение количества объектов контроля, отнесенных к категории значительного риска, к общему количеству объектов контроля.

Ключевой показатель государственного контроля (надзора) (КП) рассчитывается по формуле:

$$КП = \frac{\text{количество объектов контроля, отнесенных к категории значительного риска на конец отчетного года}}{\text{общее количество объектов контроля на конец отчетного года}} \cdot 100\ \%.$$

Целевое значение ключевого показателя государственного контроля (надзора) определяется, исходя из ежегодного снижения значения ключевого показателя на 0,25 %.

ГЛОССАРИЙ

Государственные органы – органы государственной власти Российской Федерации, органы государственной власти субъектов Российской Федерации и иные государственные органы, образуемые в соответствии с законодательством Российской Федерации законодательством субъектов Российской Федерации.

Гриф секретности – реквизиты, свидетельствующие о степени секретности сведений, содержащихся в их носителе, проставляемые на самом носителе и (или) в сопроводительной документации на него.

Документированная информация – зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или в установленных законодательством Российской Федерации случаях ее материальный носитель.

Допуск к государственной тайне – право лица на доступ к сведениям, составляющим государственную тайну, а предприятия, учреждения и организации – на проведение работ, связанных с использованием таких сведений, которое оформляется (переоформляется) в установленном порядке.

Доступ к сведббениям, составляющим государственную тайну, – санкционированное полномочным должностным лицом ознакомление конкретного лица со сведениями, составляющими государственную тайну.

Информационная безопасность Российской Федерации – состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие Российской Федерации, оборона и безопасность государства.

Информационная инфраструктура Российской Федерации (далее – информационная инфраструктура) – совокупность объектов информатизации, информационных систем, сайтов в сети «Интернет» и сетей связи, расположенных на территории Российской Федерации, а также на территориях, находящихся под юрисдикцией Российской Федерации или используемых на основании международных договоров Российской Федерации.

Информационная система – совокупность содержащейся в базах данных информации, и обеспечивающих ее обработку информационных технологий и технических средств.

Информационная система общего пользования – информационная система, участники электронного взаимодействия в которой составляют неопределенный круг лиц и в использовании которой этим лицам не может быть отказано.

Информационно-телекоммуникационная сеть – технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники.

Информационные технологии – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

Информация – сведения (сообщения, данные) независимо от формы их представления.

Информация, составляющая коммерческую тайну, – 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.

Искусственный интеллект – комплекс технологических решений, позволяющий имитировать когнитивные функции человека (включая поиск решений без заранее заданного алгоритма) и получать при выполнении конкретных задач результаты, сопоставимые с результатами интеллектуальной деятельности человека или превосходящие их. Комплекс технологических решений включает в себя информационно-коммуникационную инфраструктуру, программное обеспечение (в том числе в котором используются методы машинного обучения), процессы и сервисы по обработке данных и поиску решений.

Ключ электронной подписи – уникальная последовательность символов, предназначенная для создания электронной подписи.

Конфиденциальность информации – обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя.

Корпоративная информационная система – информационная система, участники электронного взаимодействия в которой составляют определенный круг лиц.

Модель искусственного интеллекта – программа для электронных вычислительных машин (ее составная часть), предназначенная для выполнения интеллектуальных задач на уровне, сопоставимом с результатами интеллектуального труда человека или превосходящем их, использующая алгоритмы и наборы данных для выведения закономерностей, принятия решений или прогнозирования результатов.

Набор данных – состав данных, которые структурированы или сгруппированы по определенным признакам, соответствуют требованиям законодательства Российской Федерации и необходимы для разработки программ для электронных вычислительных машин на основе искусственного интеллекта.

Национальные интересы Российской Федерации в информационной сфере – объективно значимые потребности личности, общества и государства в обеспечении их защищенности и устойчивого развития в части, касающейся информационной сферы.

Носители сведений, составляющих государственную тайну, – материальные объекты, в том числе физические поля, в которых сведения, составляющие государственную тайну, находят свое отображение в виде символов, образов, сигналов, технических решений и процессов.

Обеспечение информационной безопасности – осуществление взаимоувязанных правовых, организационных, оперативно-розыскных, разведывательных, контрразведывательных, научно-технических, информационно-аналитических, кадровых, экономических и иных мер по прогнозированию, обнаружению, сдерживанию, предотвращению, отражению информационных угроз и ликвидации последствий их проявления.

Перспективные методы искусственного интеллекта – методы, направленные на создание принципиально новой научно-технической продукции, в том числе в целях разработки универсального (сильного) искусственного интеллекта (автономное решение различных задач, автоматический дизайн физических объектов, автоматическое машинное обучение, алгоритмы решения задач на основе данных с частичной разметкой и (или) незначительных объемов данных, обработка информации на основе новых типов вычислительных систем, интерпретируемая обработка данных и другие методы).

Пользователь информацией – гражданин (физическое лицо), организация (юридическое лицо), общественное объединение, осуществляющие поиск информации о деятельности государственных органов и органов местного самоуправления.

Предоставление информации – действия, направленные на получение информации определенным кругом лиц или передачу информации определенному кругу лиц.

Предоставление персональных данных – действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.

Распространение информации – действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц.

Распространение персональных данных – действия, направленные на раскрытие персональных данных неопределенному кругу лиц;

Сайт в сети «Интернет» – совокупность программ для электронных вычислительных машин и иной информации, содержащейся в информационной системе, доступ к которой обеспечивается посредством информационно-телекоммуникационной сети «Интернет» по доменным именам и (или) по сетевым адресам, позволяющим идентифицировать сайты в сети «Интернет».

Сертификат ключа проверки электронной подписи – электронный документ или документ на бумажном носителе, выданные удостоверяющим центром либо доверенным лицом удостоверяющего центра и подтверждающие принадлежность ключа проверки электронной подписи владельцу сертификата ключа проверки электронной подписи.

Система защиты государственной тайны – совокупность органов защиты государственной тайны, используемых ими средств и методов защиты сведений, составляющих государственную тайну, и их носителей, а также мероприятий, проводимых в этих целях.

Средства защиты информации – технические, криптографические, программные и другие средства, предназначенные для защиты сведений, составляющих государственную тайну, средства, в которых они реализованы, а также средства контроля эффективности защиты информации.

Средства обеспечения информационной безопасности – правовые, организационные, технические и другие средства, используемые силами обеспечения информационной безопасности.

Средства электронной подписи – шифровальные (криптографические) средства, используемые для реализации хотя бы одной из следующих функций – создание электронной подписи, проверка электронной подписи, создание ключа электронной подписи и ключа проверки электронной подписи.

Технологии искусственного интеллекта – совокупность технологий, включающая в себя компьютерное зрение, обработку естественного языка, распознавание и синтез речи, интеллектуальную поддержку принятия решений и перспективные методы искусственного интеллекта.

Угроза информационной безопасности Российской Федерации – совокупность действий и факторов, создающих опасность нанесения ущерба национальным интересам в информационной сфере.

Удостоверяющий центр – юридическое лицо, индивидуальный предприниматель либо государственный орган или орган местного самоуправления, осуществляющие функции по созданию и выдаче сертификатов ключей проверки электронных подписей, а также иные функции, предусмотренные законом.

Уничтожение персональных данных – действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных.

Участники электронного взаимодействия – осуществляющие обмен информацией в электронной форме государственные органы, органы местного самоуправления, организации, индивидуальные предприниматели, а также граждане.

Формат электронного документа – описание структуры файла, содержащего сведения электронного документа.

Электронная подпись – информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию.

Электронное сообщение – информация, переданная или полученная пользователем информационно-телекоммуникационной сети.

Электронный документ – документированная информация, представленная в электронной форме, то есть в виде, пригодном для восприятия человеком с использованием электронных вычислительных

машин, а также для передачи по информационно-телекоммуникационным сетям или обработки в информационных системах.

Электронный документ – документированная информация, представленная в электронной форме, то есть в виде, пригодном для восприятия человеком с использованием электронных вычислительных машин, а также для передачи по информационно-телекоммуникационным сетям или обработки в информационных системах.

НОРМАТИВНО-ПРАВОВЫЕ ИСТОЧНИКИ

Конституция Российской Федерации : принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020 // КонсультантПлюс : [сайт]. URL: https://www.consultant.ru/document/cons_doc_LAW_28399/ (дата обращения: 01.11.2024).

Гражданский кодекс Российской Федерации : принят Государственной Думой 30.11.1994 № 51-ФЗ // КонсультантПлюс : [сайт]. URL: https://www.consultant.ru/document/cons_doc_LAW_5142/ (дата обращения: 01.11.2024).

Уголовный кодекс Российской Федерации : принят Государственной Думой 13.06.1996 № 63-ФЗ // КонсультантПлюс : [сайт]. URL: https://www.consultant.ru/document/cons_doc_LAW_10699/ (дата обращения: 01.11.2024).

Кодекс Российской Федерации об административных правонарушениях : принят Государственной Думой 30.12.2001 № 195-ФЗ // КонсультантПлюс : [сайт]. URL: https://www.consultant.ru/document/cons_doc_LAW_34661/ (дата обращения: 01.11.2024).

Трудовой кодекс Российской Федерации : принят Государственной Думой 30.12.2001 № 197-ФЗ // КонсультантПлюс : [сайт]. URL: https://www.consultant.ru/document/cons_doc_LAW_34683/ (дата обращения: 01.11.2024).

О коммерческой тайне : Федеральный закон от 29.07.2004 № 98-ФЗ // КонсультантПлюс : [сайт]. URL: https://www.consultant.ru/document/cons_doc_LAW_48699/ (дата обращения: 01.11.2024).

Об информации, информационных технологиях и о защите информации : Федеральный закон от 27.07.2006 № 149-ФЗ // КонсультантПлюс : [сайт]. URL: https://www.consultant.ru/document/cons_doc_LAW_61798/ (дата обращения: 01.11.2024).

О персональных данных : Федеральный закон от 27.07.2006 № 152-ФЗ. URL: https://ставрополь.рф/files/komitetgrad/myn_uslygi/8%20usluga/5/10%20федеральным%20законом%20от%2027%20июля%202006%20года%20№%20152-фз%20%20%20«о%20персональных%20данных».pdf (дата обращения: 01.11.2024).

О контроле за деятельностью лиц, находящихся под иностранным влиянием : Федеральный закон от 14.07.2022 № 255-ФЗ // КонсультантПлюс : [сайт]. URL: http://www.consultant.ru/ (дата обращения: 01.11.2024).

О государственном контроле (надзоре) и муниципальном контроле в Российской Федерации : Федеральный закон от 31.07.2020 № 248-ФЗ // КонсультантПлюс : [сайт]. URL: http://www.consultant.ru/ (дата обращения: 01.11.2024).

Об обеспечении доступа к информации о деятельности судов в Российской Федерации : Федеральный закон от 22.12.2008 № 262-ФЗ // КонсультантПлюс : [сайт]. URL: http://www.consultant.ru/ (дата обращения: 01.11.2024).

О прокуратуре Российской Федерации : Федеральный закон от 17.01.1992 № 2202-1 // КонсультантПлюс : [сайт]. URL: http://www.consultant.ru/ (дата обращения: 01.11.2024)

Об электронной подписи : Федеральный закон от 06.04.2011 № 63-ФЗ // КонсультантПлюс : [сайт]. URL: http://www.consultant.ru/ (дата обращения: 01.11.2024).

О государственной тайне : Закон Российской Федерации от 21.07.1993 №5485-1 // КонсультантПлюс : [сайт]. URL: http://www.consultant.ru/ (дата обращения: 01.11.2024).

О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года : Указ Президента Российской Федерации от 07.05.2018 № 204 // КонсультантПлюс : [сайт]. URL: http://www.consultant.ru/ (дата обращения: 01.11.2024).

О национальных целях развития Российской Федерации на период до 2030 года : Указ Президента Российской Федерации от 21.07.2020 № 474 // КонсультантПлюс : [сайт]. URL: http://www.consultant.ru/ (дата обращения: 01.11.2024).

О Стратегии национальной безопасности Российской Федерации : Указ Президента Российской Федерации от 02.07.2021 № 400 // КонсультантПлюс : [сайт]. URL: http://www.consultant.ru/ (дата обращения: 01.11.2024).

Об утверждении Доктрины информационной безопасности Российской Федерации : Указ Президента Российской Федерации от 05.12.2016 № 646 // КонсультантПлюс : [сайт]. URL: http://www.consultant.ru/ (дата обращения: 01.11.2024).

О мерах по ускорению создания центров правовой информации : Указ Президента Российской Федерации от 23.04.1993 № 477 // КонсультантПлюс : [сайт]. URL: http://www.consultant.ru/ (дата обращения: 01.11.2024).

Об утверждении Перечня сведений, отнесенных к государственной тайне : Указ Президента Российской Федерации от 30.11.1995 № 1203 // КонсультантПлюс : [сайт]. URL: http://www.consultant.ru/ (дата обращения: 01.11.2024).

Об утверждении Концепции правовой информатизации России : Указ Президента Российской Федерации от 28.06.1993 № 966 // КонсультантПлюс : [сайт]. URL: http://www.consultant.ru/ (дата обращения: 01.11.2024).

Об утверждении Доктрины информационной безопасности Российской Федерации : Указ Президента Российской Федерации от 05.12.2016 № 646 // КонсультантПлюс : [сайт]. URL: http://www.consultant.ru/ (дата обращения: 01.11.2024).

О развитии искусственного интеллекта в Российской Федерации : Указ Президента Российской Федерации от 10.10.2019 № 490 // КонсультантПлюс : [сайт]. URL: http://www.consultant.ru/ (дата обращения: 01.11.2024).

Об утверждении государственной программы Российской Федерации «Информационное общество» : Постановление Правительства Российской Федерации от 15.04.2014 № 313 // КонсультантПлюс : [сайт]. URL: http://www.consultant.ru/ (дата обращения: 01.11.2024).

Об утверждении Правил отнесения сведений, составляющих государственную тайну, к различным степеням секретности : Постановление Правительства Российской Федерации от 04.09.1995 № 870 // КонсультантПлюс : [сайт]. URL: http://www.consultant.ru/ (дата обращения: 01.11.2024).

Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных : Постановлением Правительства Российской Федерации от 01.11.2012 № 1119 // КонсультантПлюс : [сайт]. URL: http://www.consultant.ru/ (дата обращения: 01.11.2024).

Об использовании федеральной государственной информационной системы «Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме» : Постановление Правительства Российской Федерации от

10.07.2013 № 584 // КонсультантПлюс : [сайт]. URL: http://www.consultant.ru/ (дата обращения: 01.11.2024).

О Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций : Постановление Правительства Российской Федерации от 16.03.2009 № 228 // КонсультантПлюс : [сайт]. URL: http://www.consultant.ru/ (дата обращения: 01.11.2024).

Об утверждении Правил уведомления организаторами распространения информации в информационно-телекоммуникационной сети «Интернет» Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций о начале осуществления деятельности по обеспечению функционирования информационных систем и (или) программ для электронных вычислительных машин, которые предназначены и (или) используются для приема, передачи, доставки и (или) обработки электронных сообщений пользователей информационно-телекоммуникационной сети «Интернет», а также ведения реестра указанных организаторов» : Постановление Правительства Российской Федерации от 12.11.2020 № 1824 // КонсультантПлюс : [сайт]. URL: http://www.consultant.ru/ (дата обращения: 01.11.2024).

Об утверждении Правил взаимодействия организаторов распространения информации в информационно-телекоммуникационной сети «Интернет» с уполномоченными государственными органами, осуществляющими оперативно-розыскную деятельность или обеспечение безопасности Российской Федерации» : Постановление Правительства Российской Федерации от 31.07.2014 № 743 // КонсультантПлюс : [сайт]. URL: http://www.consultant.ru/ (дата обращения: 01.11.2024)

Об утверждении Правил направления провайдером хостинга уведомления о начале осуществления деятельности по предоставлению вычислительной мощности для размещения информации в информационной системе, постоянно подключенной к информационно-телекоммуникационной сети «Интернет» : Постановление Правительства Российской Федерации от 28.11.2023 № 2009 // КонсультантПлюс : [сайт]. URL: http://www.consultant.ru/ (дата обращения: 01.11.2024).

Об утверждении Правил взаимодействия провайдеров хостинга с уполномоченными государственными органами, осуществляющими оперативно-розыскную деятельность или обеспечение безопасности Российской Федерации : Постановление Правительства РФ от

22.11.2023 № 1952 // КонсультантПлюс : [сайт]. URL: http://www.consultant.ru/ (дата обращения: 01.11.2024).

Об утверждении Правил формирования и ведения реестра провайдеров хостинга : Постановление Правительства Российской Федерации от 28.11.2023 № 2008 // КонсультантПлюс : [сайт]. URL: http://www.consultant.ru/ (дата обращения: 01.11.2024).

Об определении критериев, в соответствии с которыми Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций может привлечь к формированию и ведению реестра провайдеров хостинга оператора такого реестра – организацию, зарегистрированную на территории Российской Федерации : Постановление Правительства Российской Федерации от 23.11.2023 № 1970 // КонсультантПлюс : [сайт]. URL: http://www.consultant.ru/ (дата обращения: 01.11.2024).

Об электронной подписи, используемой органами исполнительной власти и органами местного самоуправления при организации электронного взаимодействия между собой, о порядке ее использования, а также об установлении требований к обеспечению совместимости средств электронной подписи : Постановление Правительства Российской Федерации от 09.02.2012 № 111 // КонсультантПлюс : [сайт]. URL: http://www.consultant.ru/ (дата обращения: 01.11.2024)

Об утверждении Положения о федеральном государственном контроле (надзоре) в сфере электронной подписи : Постановление Правительства Российской Федерации от 29.06.2021 № 1044 // КонсультантПлюс : [сайт]. URL: http://www.consultant.ru/ (дата обращения: 01.11.2024).

Об утверждении Правил осуществления взаимодействия в электронной форме граждан (физических лиц) и организаций с органами государственной власти, органами местного самоуправления, с организациями, осуществляющими в соответствии с федеральными законами отдельные публичные полномочия : Постановление Правительства Российской Федерации от 09.06.2016 № 516 // КонсультантПлюс : [сайт]. URL: http://www.consultant.ru/ (дата обращения: 01.11.2024).

Об утверждении Порядка идентификации информационных ресурсов в целях принятия мер по ограничению доступа к информационным ресурсам : Приказ Роскомнадзора от 11.02.2019 № 21 // КонсультантПлюс : [сайт]. URL: http://www.consultant.ru/ (дата обращения: 01.11.2024).

Об утверждении требований к способам (методам) ограничения доступа к информационным ресурсам, а также требований к размещаемой информации об ограничении доступа к информационным ресурсам : Приказ Роскомнадзора от 14.12.2017 № 249 // КонсультантПлюс : [сайт]. URL: http://www.consultant.ru/ (дата обращения: 01.11.2024)

Об утверждении требований о защите информации при предоставлении вычислительной мощности для размещения информации в информационной системе, постоянно подключенной к информационно-телекоммуникационной сети «Интернет» : Приказ Минцифры России от 01.11.2023 № 936 // КонсультантПлюс : [сайт]. URL: http://www.consultant.ru/ (дата обращения: 01.11.2024)

Об утверждении требований к содержанию информации о применении информационных технологий предоставления информации на основе сбора, систематизации и анализа сведений, относящихся к предпочтениям пользователей сети «Интернет», находящихся на территории Российской Федерации, и размещению такой информации на информационном ресурсе : Приказ Роскомнадзора от 06.10.2023 № 149 // КонсультантПлюс : [сайт]. URL: http://www.consultant.ru/ (дата обращения: 01.11.2024).

Об утверждении порядка взаимодействия Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций с владельцами сайтов и (или) страниц сайтов в сети «Интернет», и (или) информационных систем, и (или) программ для электронных вычислительных машин, на которых применяются информационные технологии предоставления информации на основе сбора, систематизации и анализа сведений, относящихся к предпочтениям пользователей сети «Интернет», находящихся на территории Российской Федерации : Приказ Роскомнадзора от 06.10.2023 № 150 // КонсультантПлюс : [сайт]. URL: http://www.consultant.ru/ (дата обращения: 01.11.2024).

Об утверждении Правил подтверждения владения ключом электронной подписи : Приказ ФСБ России от 20.04.2021 № 154 // КонсультантПлюс : [сайт]. URL: http://www.consultant.ru/ (дата обращения: 01.11.2024).

Для заметок

Учебное издание

Щепеткина *Инна Вадимовна*
Андреев *Александр Владимирович*
Щепеткин *Евгений Николаевич*

ПРАВОВОЕ РЕГУЛИРОВАНИЕ В ИНФОРМАЦИОННОЙ СФЕРЕ

ISBN 978-5-94984-948-4

Редактор Л. Д. Черных
Оператор компьютерной верстки О. А. Казанцева

Подписано в печать 26.06.2025. Формат 60×84/16.
Бумага офсетная. Цифровая печать.
Уч.-изд. л. 9,6. Усл.-печ. л. 10,23.
Тираж 300 экз. (1-й завод 26 экз.).
Заказ № 8146

ФГБОУ ВО «Уральский государственный лесотехнический университет». 620100,
Екатеринбург, Сибирский тракт, 37.
Редакционно-издательский отдел.
Тел. 8 (343) 221–21–44.

Типография ООО «ИЗДАТЕЛЬСТВО УЧЕБНО-МЕТОДИЧЕСКИЙ ЦЕНТР УПИ».
620062, РФ, Свердловская область, Екатеринбург, пер. Лобачевского, 1, оф. 15.
Тел. 8 (343) 362–91–16.