

**Еженедельный правовой  
дайджест**

**(Интернет и информационные технологии)**

**Выпуск № 76  
(24.12.2021 г.)**

## Оглавление

<b>Российская Федерация</b> .....	3
Раздел 1. Законы и законопроекты .....	3
Раздел 2. Акты и проекты актов Правительства .....	5
Раздел 3. Ведомственные акты и проекты ведомственных актов .....	6
Раздел 4. Практические кейсы .....	7
<b>Зарубежные страны</b> .....	8
Раздел 1. Зарубежное нормотворчество .....	8
Раздел 2. Зарубежные практические кейсы .....	11
<b>Исследования, экспертные мнения, позиции государственных органов, организаций</b> .....	15

## РОССИЙСКАЯ ФЕДЕРАЦИЯ

### Раздел 1. Законы и законопроекты

#### Об удалённом участии в судебных заседаниях

Государственной Думой принят Федеральный закон «О внесении изменений в отдельные законодательные акты Российской Федерации в части регулирования дистанционного участия в судебном процессе» (законопроект № [1144921-7](#)).

Регламентируется дистанционное участие в судебных заседаниях с помощью систем веб-конференции, а также подача процессуальных документов в суд через Единый портал государственных и муниципальных услуг.

#### О единой биометрической системе и расширении полномочий Генеральной прокуратуры по блокировке сайтов

Государственной Думой принят Федеральный закон «О внесении изменений в статью 15-3 Федерального закона «Об информации, информационных технологиях и о защите информации» и статьи 3 и 5 Федерального закона «О внесении изменений в отдельные законодательные акты Российской Федерации»» (законопроект № [986111-7](#)).

Правительство Российской Федерации по согласованию с ФСБ России, Роскомнадзором и Банком России утвердит положение о единой биометрической системе, порядок размещения физическими лицами в указанной системе своих персональных данных, а также случаи и сроки их использования.

Кроме того, предусматривается блокировка распространяемых в сети «Интернет» предложений о приобретении поддельных документов, ложных

сообщений об актах терроризма, а также оправданий экстремизма по требованию Генерального прокурора или его заместителя.

### **О беспилотных гражданских воздушных судах**

Государственной Думой принят Федеральный закон «О внесении изменений в Воздушный кодекс Российской Федерации (об отдельных вопросах эксплуатации беспилотных авиационных систем и их элементов)» (законопроект № [1103872-7](#)).

В числе прочего предусматривается государственный учёт Росавиацией беспилотных гражданских воздушных судов с максимальной взлетной массой от 0,25 килограмма до 30 килограммов, а также нанесение опознавательных знаков на такие суда.

### **О штрафах за неисполнение обязанностей операторами связи**

Государственной Думой принят Федеральный закон «О внесении изменений в Кодекс Российской Федерации об административных правонарушениях» (законопроект № [328730-7](#)).

За неисполнение оператором связи обязанностей обязанности по передаче в неизменном виде абонентского номера или уникального кода идентификации вводится административный штраф в размере от 30 тысяч до 80 тысяч рублей для должностных лиц, от 200 до 800 тысяч рублей – для индивидуальных предпринимателей, от 500 до 800 тысяч рублей – для юридических лиц.

За неисполнение обязанности по прекращению оказания услуг связи и или услуг по пропуску трафика в предусмотренных законом случаях вводится административный штраф в размере от 50 тысяч до 100 тысяч рублей для должностных лиц, от 400 до 800 тысяч рублей – для индивидуальных предпринимателей, от 600 тысяч до 1 миллиона рублей – для юридических лиц.

Административный штраф аналогичного размера повлечёт неподключение оператора связи к системе радиочастотной службы, а также ненаправление в указанную систему необходимых данных.

## **Раздел 2. Акты и проекты актов Правительства**

### **О критериях социальной рекламы**

Опубликовано [постановление Правительства](#) Российской Федерации от 16 декабря 2021 года № 2312 «Об утверждении критериев отнесения информации, распространяемой в информационно-телекоммуникационной сети «Интернет», к социальной рекламе в целях определения объема социальной рекламы, предусмотренного частью 3 статьи 10 Федерального закона «О рекламе».

Для учёта в обязательном для распространения объёме социальная реклама должна соответствовать требованиям законодательства о рекламе, а также должна быть направлена на достижение одной или нескольких благотворительных и общественно полезных целей, в числе которых:

- социальная поддержка населения;
- помощь при бедствиях и катастрофах;
- повышение правовой, финансовой и иных видов грамотности;
- поддержка образования, просвещения, науки, культуры, искусства, профилактики и охраны здоровья населения;
- формирование в обществе нетерпимости к нарушениям законности;
- духовно-нравственное и патриотическое воспитание.

### **Об угрозах безопасности сети «Интернет» и сети связи общего пользования**

Опубликовано [постановление Правительства](#) Российской Федерации

от 17 декабря 2021 года № 2343 «О внесении изменений в постановление Правительства Российской Федерации от 12 февраля 2020 г. № 127».

Перечень угроз безопасности функционирования на территории Российской Федерации сети «Интернет» и сети связи общего пользования дополняется угрозами подмены абонентского номера или уникального кода идентификации абонента при осуществлении соединения, поступающего из-за пределов Российской Федерации.

### **Раздел 3. Ведомственные акты и проекты ведомственных актов**

#### **О предоставлении сведений из Единого реестра запрещённых ресурсов**

Роскомнадзор опубликовал для общественного обсуждения:

- [проект приказа](#) «О внесении изменений в Порядок получения доступа к содержащейся в единой автоматизированной информационной системе «Единый реестр доменных имен, указателей страниц сайтов в сети «Интернет» и сетевых адресов, позволяющих идентифицировать сайты в сети «Интернет», содержащие информацию, распространение которой в Российской Федерации запрещено» информации оператором связи, оказывающим услуги по предоставлению доступа к информационно-телекоммуникационной сети «Интернет», утвержденный приказом Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 21 февраля 2013 г. № 169»;

- [проект приказа](#) «О внесении изменения в Порядок доступа к информации, содержащейся в единой автоматизированной информационной системе «Единый реестр доменных имен, указателей страниц сайтов в информационно-телекоммуникационной сети «Интернет» и сетевых адресов, позволяющих идентифицировать сайты в информационно-телекоммуникационной сети «Интернет», содержащие информацию, распространение которой в Российской Федерации запрещено»,

утвержденный приказом Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 9 июня 2017 г. № 100».

Операторам связи в целях ограничения доступа к информационным ресурсам, на которых распространяются порочащие честь, достоинство или деловую репутацию сведения, будут предоставляться реквизиты постановления судебного пристава-исполнителя об ограничении доступа к такой информации.

Также предусматривается предоставление доступа к единой автоматизированной информационной системе «Единый реестр доменных имен, указателей страниц сайтов в информационно-телекоммуникационной сети «Интернет» и сетевых адресов, позволяющих идентифицировать сайты в информационно-телекоммуникационной сети «Интернет» содержащие информацию, распространение которой в Российской Федерации запрещено» ФССП России.

## **Раздел 4. Практические кейсы**

### **О штрафах за удаление противоправного контента**

Мировой судья судебного участка № 422 Таганского района города Москвы вынес постановления по делу № [05-3176/422/2021](#), о привлечении компании ГитХаб Инк (GitHub Ink) к административной ответственности за удаление противоправного контента по требованию Роскомнадзора.

Компании назначен штраф на сумму 1 миллион рублей.

Кроме того, компания Google LLC привлечена к административной ответственности за повторное совершение упомянутого правонарушения по делу № [05-3220/422/2021](#) на основании части 5 статьи 13.41 КоАП РФ в виде оборотного штрафа на сумму 7 221 916 235 рублей.

Компании Meta Platforms Inc. (бывшая Facebook Inc.) и Telegram Messenger Inc. выплатили назначенные им за аналогичное нарушение административные штрафы на сумму 17 миллионов рублей и 15 миллионов рублей соответственно.

В [банке данных исполнительных производств](#) ФССП России сведения в отношении компаний в настоящий момент не содержатся.

## ЗАРУБЕЖНЫЕ СТРАНЫ

### Раздел 1. Зарубежное нормотворчество

#### О поправках к Закону об авторском праве в Малайзии

В Малайзии были приняты [поправки](#) к Закону об авторском праве, предусматривающие уголовную ответственность за «пиратские» трансляции.

Под регулирования попадут те, кто нарушает авторские права или способствует их нарушению, занимаясь производством стриминговой технологии для продажи или аренды (как программ, так и оборудования).

Кроме того, запрещается импорт, продажа, сдача в аренду или реклама стриминговых сервисов, которые могут нанести ущерб владельцу авторских прав.

Нарушителям закона будет грозить штраф в размере не менее 10 тысяч ринггитов (2 377 долларов США), но не более 200 тысяч ринггитов (47 545 долларов США), а также лишение свободы на срок до 20 лет.

Владельцы стриминговых сервисов могут избежать наказания, если докажут, что не знали о совершении правонарушения либо пытались его предотвратить.



## Об обработке данных детей

Комиссией по защите данных Ирландии (DPC) были разработаны Основы ориентированного на детей подхода к обработке данных.

Вводятся принципы толкования защиты данных, ориентированные на детей, и рекомендуемые меры, которые позволят повысить уровень защиты детей от рисков обработки данных, возникающих при использовании ими услуг/доступа к ним как в онлайн, так и в офлайн пространстве.

Документ определяет 14 основ, которым должны следовать организации для усиления защиты детей при обработке их персональных данных, среди которых в частности:

1. Четкое согласие: Если ребенок дал согласие на обработку своих данных, это согласие должно быть свободно выраженным, конкретным, информированным и недвусмысленным, выраженным посредством четкого заявления или утвердительного действия;

2. Информирование на любой стадии: Дети имеют право на получение информации об обработке своих персональных данных независимо от того, даже если согласие на обработку было получено от имени родителей;

3. Прозрачность, ориентированная на детей: Информация о том, как используются персональные данные, должна предоставляться в понятной и доступной форме с использованием языка, который понятен и соответствует возрасту ребенка;

4. Согласие «не отменяет» детство: Согласие, полученное от детей или от опекунов/родителей, не должно использоваться в качестве оправдания для обращения с детьми любого возраста, как если бы они были взрослыми;

5. Профилирование: Поставщики онлайн-услуг не должны составлять профиль детей и/или осуществлять автоматизированное принятие решений в отношении детей, или иным образом использовать их персональные данные в маркетинговых/рекламных целях в связи с их особой уязвимостью и

восприимчивостью к поведенческой рекламе, если они не могут четко продемонстрировать, как и почему это делается в наилучших интересах ребенка.

### **Об оценке воздействия на защиту данных в Финляндии**

Управление по надзору за защитой данных Финляндии (EDPS) опубликовало [Руководство](#) по оценке воздействия на защиту данных для выявления и снижения рисков, связанных с обработкой персональных данных, а также для оказания помощи в соблюдении законодательства.

Вместе с руководством был разработан инструмент в Excel, который при желании можно использовать для проведения оценки воздействия.

Целью оценки воздействия на защиту данных является выявление и снижение рисков, связанных с обработкой персональных данных, и предоставление материала, который можно использовать для демонстрации соблюдения правил защиты данных.

Новое руководство и связанный с ним инструмент предназначены для поддержки контроллеров данных при проведении оценок воздействия в соответствии с GDPR.

### **О рекомендациях в сфере здравоохранения**

Управление комиссара по информации Великобритании (ICO) разработало [рекомендации](#) по внесению изменений в систему тестирования и отслеживания Национальной службы здравоохранения (NHS) для усиления защиты персональных данных.

Рекомендации включают:

- расширение программы обучения персонала NHS Test and Trace с включением специализированных курсов для различных функций. Например, обучение по передаче информации о конфиденциальности для сотрудников;

- разработка и доведение до сведения сотрудников дополнительных процессов и политик, таких как оценка рисков конфиденциальности и руководство по безопасности, для обеспечения сильной культуры конфиденциальности в NHS Test and Trace; и
- добавление механизмов аудита, таких как периодические проверки и мониторинг контрактов, для обеспечения того, чтобы сотрудники и третьи стороны следовали согласованным процессам.

### **Об ирландской Стратегии регулирования**

Комиссия по защите данных Ирландии (DPC) опубликовала свою [Стратегию регулирования](#) на 2022-2027 годы.

Определены следующие цели Стратегии:

- последовательное и эффективное регулирование;
- защита отдельных лиц и содействие повышению осведомленности о защите данных;
- уделение первоочередного внимания защите детей и других уязвимых групп;
- внесение ясности для заинтересованных сторон;
- поддержка организаций.

## **Раздел 2. Зарубежные практические кейсы**

### **О мерах компании Meta против слежки за пользователями**

Компания Meta (ранее Facebook) [выявила](#) семь компаний в четырех странах, которые использовали вредоносное программное обеспечение для получения несанкционированного доступа к данным пользователей.

Компания утверждает, что жертвами стали более 50 тысяч пользователей из более 100 государств.

Meta объявила, что прекратила отношения с данными организациями, удалила примерно 1,5 тысяч учетных записей, а также заблокировала URL-адреса, с которых распространялось вредоносное ПО.

В список компаний вошли израильские Cobwebs Technologies, Black Cube, Cognyte и Bluehawk CI, индийская BellTroх, северомакедонская Cytroх и одна неназванная китайская компания.

По утверждению Meta, их заказчиками оказались представители из 20 стран, среди которых Оман, Колумбия, ОАЭ, Мексика, Новая Зеландия, Гонконг, Вьетнам, Филиппины, Германия, Саудовская Аравия, Армения, Египет, Польша, Бангладеш, Греция, Кот-д'Ивуар и Египет.

Компании добивались установки шпионского ПО на устройства пользователей при помощи фейковых аккаунтов в Facebook и Instagram, в результате чего получали доступ к звонкам, контактам, фото, видео и местоположению.

### **О штрафе Amazon в Люксембурге**

Председатель административного суда вынес [постановление](#) о частичном удовлетворении ходатайства, поданного компанией Amazon Europe Core S.AR.L. с просьбой приостановить исполнение решения Национальной комиссии по защите данных (CNPД) от 15 июля 2021 года, наложившей на нее административный штраф в размере 746 000 000 евро, обязав ее в течение шести месяцев со дня уведомления принять меры по исправлению ситуации под угрозой ежедневного штрафа в размере 746 000 евро.

Председатель административного суда в предварительном порядке постановил, что различные предписания, направленные CNPD компании Amazon под угрозой ежедневного штрафа с требованием привести ее рекламную систему в соответствие с GDPR, не были сформулированы ясно, четко и без неопределенности, в условиях, которые позволили бы компании выполнить их в установленный срок (до 15 января 2022 года).

Вопрос о штрафе в размере 746 000 000 евро не рассматривался, так как взыскание этого штрафа в настоящее время приостановлено государством.

### **О иске компании Meta в отношении «фишинговых» сайтов**

Компания Meta обратилась в Окружной суд Северного округа Калифорнии с **иском** в отношении 39 тысяч сайтов, которые используются в «фишинговых» атаках на пользователей ее сервисов (Facebook, Facebook Messenger, WhatsApp и Instagram).

Как указано в иске, компания намеревается раскрыть личности владельцев таких сайтов и привлечь их к ответственности.

Meta утверждает, что количество поддельных сайтов, которые выманивают учетные данные пользователей под видом получения какого-то контента, с марта 2021 года увеличивается.

Впоследствии полученные данные используются для противоправных действий, отмечает истец.

### **О черном списке китайских компаний**

Министерство финансов США **добавило** восемь китайских компаний в черный список «китайского военно-промышленного комплекса» за поддержку наблюдения и слежки за мусульманами-уйгурами и этническими меньшинствами в Китае.

В список включена, в частности, компания DJI, являющаяся крупнейшим в мире производителем коммерческих дронов.

### **О решении ЕС и Южной Кореи**

Европейский комиссар по вопросам юстиции и председатель Комиссии по защите персональной информации Южной Кореи объявили о принятии **решения о достаточности мер** между ЕС и Южной Кореей в отношении передачи персональных данных.

На основании принятого решения персональные данные смогут безопасно перемещаться из ЕС в Республику Корея на благо граждан и экономик обеих сторон, без необходимости получения дополнительных разрешений или дополнительных инструментов.

Решение дополнит Соглашение о свободной торговле между ЕС и Республикой Корея в отношении потоков персональных данных.

Более того, охватывая обмен данными между государственными органами, решение о достаточности также будет способствовать сотрудничеству в сфере регулирования.

### **О споре FTC v. SupportKing**

Федеральная торговая комиссия США (FTC) [объявила](#) об окончательном урегулировании спора с компанией SupportKing, занимающейся поддержкой технологий, в связи с ее приложениями «stalkerware».

Приложения, предоставленные компанией, позволяли необоснованно следить за фотографиями, текстовыми сообщениями, веб-историей, местоположением GPS и другой личной информацией с мобильных устройств, на которых они были установлены.

Урегулирование, согласованное членами комиссии FTC, запрещает дальнейшую продажу и рекламу «преследовательского ПО» компанией SupportKing и ее руководителем, а также требует удаления всех персональных, собранных с помощью приложений компании.

В дополнение к этому, постановление также предписывает компании уведомить владельцев устройств, на которых были установлены приложения, о том, что за их устройствами, возможно, велось наблюдение, а сами устройства могут быть небезопасны.

## ИССЛЕДОВАНИЯ, ЭКСПЕРТНЫЕ МНЕНИЯ, ПОЗИЦИИ ГОСУДАРСТВЕННЫХ ОРГАНОВ, ОРГАНИЗАЦИЙ

### О тенденциях развития Интернета

Координационный центр национального домена сети Интернет опубликовал аналитический доклад «Тенденции развития Интернета: от цифровых возможностей к цифровой реальности», подготовленный по его заказу НИУ ВШЭ.

Как указывают эксперты, на российском рынке доменных имен наблюдается устойчивый спрос на национальные домены верхнего уровня.

Так, В 2020 году российский домен .ru сохранил тенденцию к росту, укрепившись на восьмой строчке топ-10 доменов верхнего уровня с результатом пять миллионов доменных имен.

Интернационализованный домен.рф (711,8 тысячи доменных имён) лидирует среди кириллических доменов и стабильно входит в топ-20 национальных доменов Европы.

В докладе отмечается сохраняющаяся тенденция к расширению рынка телекоммуникаций и смещению фокуса на технологии беспроводного доступа.

В 2020 году число абонентов фиксированного широкополосного доступа к интернету (ШПД) в России выросло по сравнению с 2019 годом на 3,7%, мобильного – на 3,3%. В условиях пандемии и с развитием технологий связи, позволяющих загружать большие объемы данных, стремительно вырос годовой объем интернет-трафика.

Отмечается, что о спросе на более быстрое соединение свидетельствует рост доли абонентов, подключающихся на скорости 100 Мбит/с и выше. Их доля в 2020 году впервые превысила долю тех, кто выходит в Сеть на скорости 10–100 Мбит/с (42,2% против 39,8%).

Спрос на надёжное высокоскоростное подключение к Интернету также растёт во всех отраслях экономики и социальной сферы. Доля компаний, использующих ШПД, в 2020 году достигла 93%, прирост за год составил 6,4 п.п. – это максимальное значение за последние семь лет.

### О мошенничестве с криптовалютой

Компания Chainalysis опубликовала [исследование](#), посвященное преступлениям в сфере криптовалют.

Как отмечают эксперты, за 2021 год пользователи потеряли 7,7 миллиардов долларов США в результате мошеннических действий с виртуальной валютой. Рост по сравнению с 2020 годом составил 81%.

Согласно выводам экспертов, крупную часть этого роста обеспечила пирамида iniko, которая действовала с декабря 2019 года по июль 2021 года.

Пирамида предлагала пользователям инвестировать в биткоин или Tether, обещая ежемесячную доходность до 30%, и в конечном итоге запустила собственную монету, которая торговалась на нескольких биржах. В течение примерно 19 месяцев активности Finiko собрала более 1,5 миллиарда долларов США на более чем 800 тысячах отдельных депозитов.

Кроме того, заметно возросла доля хищений по схеме rug pull, когда мошенники создают фальшивые токены и скрываются с деньгами инвесторов.

В 2021 году на эту схему пришлось 37% всего дохода от мошенничеств с криптовалютой по сравнению с всего лишь 1% в 2020 году. Злоумышленники получили более 2,8 миллиарда долларов США.



и р и  
• р ф

**+7 (495) 109 0080**

**info@iri.center**

119146, г. Москва,  
Комсомольский пр., д. 32, корп. 2

Москва 2021

© Автономная некоммерческая организация  
«Институт развития интернета» (ИРИ)