Экспертный центр Электронного государства

ОБЗОР
положений действующего законодательства для ИТ-компаний

2016

Оглавление

1. Экономические вопросы

1.1. Вопросы уплаты страховых взносов

Российская организация, осуществляющая деятельность в области информационных технологий (далее - ИТ-компания), может получить государственную аккредитацию независимо от организационно-правовой формы и формы собственности при условии, что данная организация осуществляет разработку и реализацию программ для ЭВМ и баз данных на материальном носителе или в электронном виде по каналам связи независимо от вида договора и (или) оказывает услуги (выполняет работы) по адаптации программ ЭВМ и баз данных (программных средств и информационных продуктов вычислительной техники), установке, тестированию и сопровождению программ ЭВМ и баз данных[1].

Для аккредитованных ИТ-компаний законодательством предусмотрены пониженные тарифы страховых взносов (не более 14 процентов) при соблюдении дополнительных условий о доле «профильных» доходов и численности работников.

Для того чтобы применять пониженные тарифы страховых взносов в государственные внебюджетные фонды[2], ИТ-компании необходимо соблюсти 3 условия:

доля доходов от реализации экземпляров программ для ЭВМ, баз данных, передачи исключительных прав на программы для ЭВМ, базы данных, предоставления прав использования программ для ЭВМ, баз данных по лицензионным договорам, от оказания услуг (выполнения работ) по разработке, адаптации и модификации программ для ЭВМ, баз данных (программных средств и информационных продуктов вычислительной техники), а также услуг (работ) по установке, тестированию и сопровождению указанных программ для ЭВМ, баз данных по итогам девяти месяцев года, предшествующего году перехода организации на уплату страховых взносов по пониженным тарифам, составляет не менее 90 процентов в сумме всех доходов организации за указанный период без учета доходов в виде курсовых разниц, указанных в пунктах 2 и 11 части второй статьи 250 Налогового кодекса Российской Федерации;

[1] Положение о государственной аккредитации организаций, осуществляющих деятельность в области информационных технологий, утверждено постановлением Правительства Российской Федерации от 6 ноября 2007 г. № 758

[2] Часть 3 статьи 58 Федерального закона от 24 июля 2009 г. № 212-ФЗ «О страховых взносах в Пенсионный фонд Российской Федерации, Фонд социального страхования Российской Федерации, Федеральный фонд обязательного медицинского страхования»

средняя численность работников за девять месяцев года, предшествующего году перехода организации на уплату страховых взносов по тарифам страховых взносов, составляет не менее 7 человек;

организацией получен документ о государственной аккредитации.

Пониженные тарифы страховых взносов составляют (в процентах от суммы выплат и иных вознаграждений в пользу физических лиц):

на обязательное пенсионное страхование – 8 процентов от выплат в пределах базы для начисления страховых взносов (обычный порядок - 22 процента);

на обязательное социальное страхование на случай временной нетрудоспособности и в связи с материнством – 2 процента от выплат в пределах базы для начисления страховых взносов (обычный порядок - 2,9 процента);

на обязательное медицинское страхование – 4 процента от выплат (обычный порядок - 5,1 процента).

Вновь созданные организации вправе применять пониженные тарифы страховых взносов после получения документа о государственной аккредитации, если по итогам отчетного (расчетного) периода они выполнят вышеуказанные условия о доле «профильных» доходов и численности работников (то есть, допустимо использование преференции «авансом», но если по итогам отчетного (расчетного) периода организация не выполнит хотя бы одно условие, она должна уплатить страховые взносы за данный период по общим тарифам).

1.2. Особенности налогообложения отечественных ИТ-компаний

В ряде субъектов Российской Федерации (Новосибирской, Пензенской и Ульяновской областях) установлена льготная ставка по налогу на прибыль организаций (15,5 процентов, ранее 20 процентов).

Для исчисления налога по льготной ставке организации, осуществляющей деятельность в области информационных технологий, достаточно получить аккредитацию в Минкомсвязи России. Доход такой организации от реализации информационных технологий — работ или услуг — должен составлять не менее 70 процентов от общего дохода.[3]

ИТ-компании имеют право не применять установленный статьей 259 Налогового кодекса Российской Федерации порядок амортизации в отношении электронно-вычислительной техники, а включать расходы на ее приобретение в полном

[3]Пониженная ставка налога на прибыль организаций (15,5%) максимально приближена к ставке налога, уплачиваемого при применении упрощенной системы налогообложения (УСН) с доходов, уменьшенных на величину расходов (15%). Льготный режим позволит ИТ-компаниям преодолеть «боязнь роста» в случае, когда их доходы достигают порога, после которого невозможно дальнейшее применение УСН.

размере в состав материальных расходов сразу после ввода в эксплуатацию при выполнении трех условий:

доля доходов от реализации экземпляров программ для ЭВМ, баз данных, передачи имущественных прав на программы для ЭВМ, базы данных, от оказания услуг (выполнения работ) по разработке, адаптации и модификации программ для ЭВМ, баз данных (программных средств и информационных продуктов вычислительной техники), а также услуг (работ) по установке, тестированию и сопровождению указанных программ для ЭВМ, баз данных по итогам отчетного (налогового) периода составляет не менее 90 процентов в сумме всех доходов организации за указанный период, в том числе от иностранных лиц не менее 70 процентов;

среднесписочная численность работников за отчетный (налоговый) период составляет не менее 50 человек;

организацией получен документ о государственной аккредитации.

1.3. Особенности налогообложения иностранных ИТ-компаний

С 1 января 2017 г. иностранная организация, подлежащая на день вступления закона[4] в силу постановке на учет в налоговом органе, подает заявление о постановке на учет.

Закон предполагает взимание НДС (15,25%) с операций в Интернете по продаже иностранными компаниями россиянам электронных услуг, игр, музыкальных произведений, книг и видеопродукции.

К услугам, облагаемым НДС, будет относиться предоставление через Интернет прав на использование программ для компьютеров, в том числе компьютерных игр и баз данных, оказание рекламных услуг в Интернете, оказание услуг по размещению предложений

о приобретении товаров и услуг, по поддержке электронных ресурсов, предоставлению доменных имен и услуг хостинга, предоставление прав на использование электронных книг, музыкальных произведений, графических изображений и видео.

К услугам в электронной форме не будет относиться реализация товаров, если их поставка осуществляется без использования Интернета, а также продажа программ (баз данных) на материальных носителях и оказание услуг по предоставлению доступа к Интернету.

Местом реализации контента иностранными компаниями будет считаться Россия.

[4] Федеральный закон от 3 июля 2016 г. № 244-ФЗ «О внесении изменений в части первую и вторую Налогового кодекса Российской Федерации»

2. Кадровые вопросы ИТ-компаний

Аккредитованные ИТ-компании, созданные в форме коммерческой организации, а также ИТ-компании, которые аккредитованы в установленном порядке на территории Российской Федерации и являются филиалами, представительствами иностранных юридических лиц[5] вправе привлекать к трудовой деятельности в Российской Федерации высококвалифицированных специалистов из числа иностранных граждан в упрощенном порядке.

Для выдачи высококвалифицированному специалисту разрешения на работу и продления в этих целях срока его временного пребывания в Российской Федерации, а также для оформления ему приглашения на въезд в Российскую Федерацию в целях осуществления трудовой деятельности (при необходимости) ИТ-компания представляет в территориальное подразделение МВД России необходимые документы.

Срок рассмотрения ходатайства о привлечении высококвалифицированного специалиста составляет не более 14 рабочих дней.

Такой подход дает следующие преференции:

для привлечения ИТ-компанией высококвалифицированных специалистов из числа иностранных граждан не требуется разрешение на привлечение и использование иностранных работников;

на высококвалифицированных специалистов и членов их семей (супруг или супруга), дети, в том числе усыновленные, супруги детей, родители, в том числе приемные, супруги родителей, бабушки, дедушки, внуки) не распространяются квоты на выдачу иностранным гражданам приглашений на въезд в Российскую Федерацию в целях осуществления трудовой деятельности и на выдачу иностранным гражданам разрешений на работу, установленные Правительством Российской Федерации;

прибывшим в Российскую Федерацию высококвалифицированным специалистам и членам их семей на срок действия трудового договора или гражданско-правового договора на выполнение работ (оказание услуг) по их заявлению в письменной форме территориальным органом Федеральной миграционной службы может быть оформлен вид на жительство.

Высококвалифицированным специалистом признается иностранный гражданин, имеющий опыт работы, навыки или достижения в конкретной области деятельности, если условия привлечения его к трудовой деятельности в Российской Федерации предполагают получение им заработной платы

[5] Подпункт 1 пункта 5 статьи 13.2 Федерального закона от 25 июля 2002 г. № 115-ФЗ «О правовом положении иностранных граждан в Российской Федерации»

(вознаграждения) в размере не менее восьмидесяти трех тысяч пятисот рублей из расчета за один календарный месяц.

ИТ-компания самостоятельно осуществляет оценку компетентности и уровня квалификации иностранных граждан, которых они желают привлечь в качестве высококвалифицированных специалистов, и несет соответствующие риски.

Привлечение иностранного гражданина – высококвалифицированного специалиста влечет возложение на ИТ-компанию следующих обязанностей:

включить в трудовой договор или гражданско-правовой договор на выполнение работ (оказание услуг) с высококвалифицированным специалистом обязательное условие об обеспечении гарантий получения медицинской помощи высококвалифицированным специалистом и прибывающими вместе с ним членами его семьи в течение срока действия соответствующего договора путем обеспечения наличия действующего на территории Российской Федерации договора (полиса) медицинского страхования либо предоставления права на получение первичной медико-санитарной помощи и специализированной медицинской помощи на основании договора, заключенного ИТ-компанией с медицинской организацией;

ежеквартально не позднее последнего рабочего дня месяца, следующего за отчетным кварталом, уведомлять МВД России об исполнении обязательств по выплате заработной платы (вознаграждения) высококвалифицированным специалистам, а также о случаях расторжения трудовых договоров или гражданско-правовых договоров на выполнение работ (оказание услуг) с данными высококвалифицированными специалистами и случаях предоставления им отпусков без сохранения заработной платы продолжительностью более одного календарного месяца в течение года в порядке и по формам, утвержденным приказом ФМС России от 28 июня 2010 г. №147.

Неуведомление или нарушение установленного порядка и (или) формы уведомления влечет административную ответственность, предусмотренную частью 5 статьи 18.15 Кодекса Российской Федерации об административных правонарушениях.

3. Персональные данные

3.1. ИТ-компании как операторы персональных данных

Большинство ИТ-компаний работают с персональными данными граждан и являются операторами, осуществляющими обработку персональных данных.

Роскомнадзор является уполномоченным органом по защите прав субъектов персональных данных и ведет Реестр операторов, осуществляющих обработку персональных данных[6] (далее - оператор).

В соответствии п. 2 ст. 3 Закона № 152-ФЗ оператором является государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

При этом операторами указанные органы и лица являются независимо от включения в реестр операторов, осуществляющих обработку персональных данных, который ведет Роскомнадзор.

Согласно п. 9 ст. 3 Закона № 152-ФЗ информационная система персональных данных - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

В случае соответствия разрабатываемых или эксплуатируемых ИТ-компаниями информационных систем, в том числе интернет-сайтов указанным требованиям, компании должны быть включены в Реестр операторов, осуществляющих обработку персональных данных.

Статья 22 Закона № 152-ФЗ закрепила за операторами обязанность до начала обработки персональных данных уведомить Роскомнадзор о своем намерении осуществлять обработку персональных данных. Уведомления должны быть направлены в письменной форме и подписаны уполномоченным лицом или направлены в электронной форме и подписаны электронной подписью в территориальные управления Роскомнадзор, на подведомственной территории которых оператор осуществляет (будет осуществлять) обработку персональных данных.

Согласно статье 24 Закона № 152-ФЗ лица, виновные в нарушении требований указанного Федерального закона, несут предусмотренную законодательством Российской Федерации ответственность[7].

[6] Пункт 3 ч. 5 ст. 23 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (далее – Закон № 152-ФЗ)

При нарушении законодательства Российской Федерации о персональных данных в трудовых отношениях дополнительно предусмотрены следующие виды ответственности: дисциплинарная (подпункт «в» п. 6 ст. 81 ТК РФ), материальная (ст. 238 ТК РФ) и гражданско-правовая.

3.2. Ограничение доступа к информации, обрабатываемой с нарушением законодательства о персональных данных

В целях ограничения доступа к информации в сети Интернет, обрабатываемой с нарушением законодательства Российской Федерации в области персональных данных, создается автоматизированная информационная система «Реестр нарушителей прав субъектов персональных данных» (далее - реестр нарушителей).

Основанием для включения в реестр нарушителей является вступивший в законную силу судебный акт.

В течение трех рабочих дней со дня получения вступившего в законную силу судебного акта Роскомнадзор определяет провайдера хостинга или иное лицо, обеспечивающее обработку информации в Интернет, с нарушением законодательства Российской Федерации в области персональных данных. Затем направляет провайдеру хостинга или иному вышеназванному лицу в электронном виде уведомление на русском и английском языках о нарушении законодательства Российской Федерации в области персональных данных.

В течение одного рабочего дня с момента получения уведомления провайдер хостинга или иное указанное выше лицо обязаны проинформировать об этом обслуживаемого ими владельца информационного ресурса и уведомить его о необходимости незамедлительно принять меры по устранению нарушения законодательства Российской Федерации в области персональных данных, указанного в уведомлении, или принять меры по ограничению доступа к информации, обрабатываемой с нарушением законодательства Российской Федерации в области персональных данных.

В течение одного рабочего дня с момента получения от провайдера хостинга или иного указанного выше лица уведомления о необходимости устранения нарушения законодательства Российской Федерации в области персональных данных владелец информационного ресурса обязан принять меры по устранению указанного в уведомлении нарушения. В случае отказа или бездействия владельца информационного ресурса провайдер хостинга обязан ограничить доступ к соответствующему информационному ресурсу не позднее истечения трех рабочих дней с момента получения уведомления.

---

[7] Административная ответственность предусмотрена статьями 5.39, 13.11, 13.14 и 19.7 КоАП РФ), уголовная – статьями 137, 140 и 272 УК РФ.

В случае непринятия провайдером хостинга и (или) владельцем информационного ресурса мер, доменное имя сайта в сети Интернет, его сетевой адрес, указатели страниц сайта в сети Интернет, позволяющие идентифицировать информацию, обрабатываемую с нарушением законодательства Российской Федерации в области персональных данных, а также иные сведения об этом сайте и информация направляются по автоматизированной информационной системе операторам связи для принятия мер по ограничению доступа к данному информационному ресурсу, в том числе к сетевому адресу, доменному имени, указателю страниц сайта в сети Интернет.

4. Обеспечение национальной безопасности

4.1. Обязанности ИТ-компаний предоставлять информацию

С 1 июля 2018 г. ИТ-компании - организаторы распространения информации обязаны хранить на территории Российской Федерации[8]:

информацию о фактах приема, передачи, доставки и (или) обработки голосовой информации, текстовых сообщений, изображений, звуков, видео- или иных сообщений пользователей услугами связи - в течение трех лет с момента окончания осуществления таких действий;

текстовые сообщения пользователей услугами связи, голосовую информацию, изображения, звуки, видео-, иные сообщения пользователей услугами связи - до шести месяцев с момента окончания их приема, передачи, доставки и (или) обработки.

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

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.

4.2. Обязанность по размещению технических средств информационных систем на территории Российской Федерации

ИТ-компаниям необходимо помнить, что технические средства информационных систем, используемых государственными органами, органами местного самоуправления, государственными и муниципальными унитарными

[8] Часть 3 статьи 10.1 Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»

предприятиями или государственными и муниципальными учреждениями, должны размещаться на территории Российской Федерации[9].

Статьей 13.27.1 Кодекса Российской Федерации об административных правонарушениях предусмотрен штраф за нарушение требования о размещении на территории Российской Федерации технических средств информационных систем на должностных лиц в размере от трех тысяч до пяти тысяч рублей; на юридических лиц - от тридцати тысяч до пятидесяти тысяч рублей.

4.3. Импортозамещение программного обеспечения

В Российской Федерации функционирует Единый реестр российских программ для ЭВМ и БД. Его цель - расширить использование программ для ЭВМ и БД, оказать правообладателям государственную поддержку. Российским признается программное обеспечение, сведения о котором внесены в реестр[10].

С 1 января 2016 г. установлен запрет на допуск происходящего из иностранных государств программного обеспечения при закупках для государственных и муниципальных нужд[11]. Заказчики обязаны осуществлять закупки только российского программного обеспечения. Исключение из запрета составят случаи, когда программное обеспечение с необходимыми характеристиками отсутствует в реестре российских программ или российское программное обеспечение не соответствует требованиям заказчика.

Заказчик при исполнении заключенного контракта, предметом которого является поставка программного обеспечения и (или) прав на него, не вправе допускать замену российского программного обеспечения, сведения о котором включены в реестр, на иное программное обеспечение.

4.4. Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах

Приказом ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» установлены требования к обеспечению защиты информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну, от утечки по

[9] Федеральный закон от 31 декабря 2014 г. № 531-ФЗ «О внесении изменений в статьи 13 и 14 Федерального закона «Об информации, информационных технологиях и о защите информации» и Кодекс Российской Федерации об административных правонарушениях»

[10] Федеральный закон от 29 июня 2015 г. № 188-ФЗ «О внесении изменений в Федеральный закон «Об информации, информационных технологиях и о защите информации» и статью 14 Федерального закона «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд»

[11] Постановление Правительства Российской Федерации от 16 ноября 2015 г. № 1236 «Об установлении запрета на допуск иностранного программного обеспечения при закупках для государственных и муниципальных нужд»

техническим каналам, несанкционированного доступа, специальных воздействий на такую информацию (носители информации) в целях ее добывания, уничтожения, искажения или блокирования доступа к ней при обработке указанной информации в государственных информационных системах.

Требования являются обязательными при обработке информации в государственных информационных системах, функционирующих на территории Российской Федерации, а также в муниципальных информационных системах, если иное не установлено законодательством Российской Федерации о местном самоуправлении.

4.5. Требования к разработке безопасного программного обеспечения

С 1 июля 2017 г. вводится Национальный стандарт Российской Федерации ГОСТ Р 56939-2016 «Защита информации. Разработка безопасного программного обеспечения. Общие требования».

Стандарт направлен на достижение целей, связанных с предотвращением появления и/или устранением уязвимостей программ, и содержит перечень мер, которые рекомендуется реализовать на соответствующих этапах жизненного цикла программного обеспечения.

Стандарт предназначен для разработчиков программного обеспечения, а также для организаций, выполняющих оценку соответствия процесса разработки программного обеспечения требованиям настоящего стандарта.

Стандарт устанавливает общие требования к содержанию и порядку выполнения работ, связанных с созданием безопасного (защищенного) программного обеспечения и формированием (поддержанием) среды обеспечения оперативного устранения выявленных пользователями ошибок программного обеспечения и уязвимостей программы.

5. Распространение информации

5.1. Функционирование «Реестра запрещенных сайтов»

В 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 (далее – Единый реестр) включаются доменные имена и (или) указатели страниц сайтов в сети Интернет, содержащие информацию, распространение которой в Российской Федерации запрещено, а также сетевые адреса, позволяющие идентифицировать сайты в сети Интернет, содержащие информацию, распространение которой в Российской Федерации запрещено[12].

Указанные сведения включаются в Единый реестр на основании решения уполномоченных Правительством Российской Федерации федеральных органов исполнительной власти, принятые в соответствии с их компетенцией в порядке, установленном Правительством Российской Федерации, в отношении распространяемых посредством сети Интернет:

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

б) информации о способах, методах разработки, изготовления и использования наркотических средств, психотропных веществ и их прекурсоров, местах приобретения таких средств. Веществ и их прекурсоров, о способах и местах культивирования наркосодержащих растений;

в) информация о способах совершения самоубийства, а также призывов к совершению самоубийства;

г) информации о несовершеннолетнем, пострадавшем в результате противоправных действий (бездействия) распространение которой запрещено федеральными законами;

д) информации о деятельности по организации и проведению азартных игр и лотерей с использованием сети Интернет и иных средств связи[13].

Кроме того, указанные сведения включаются в Единый реестр на основании вступившего в законную силу решение суда о признании информации,

[12] Предусмотрено частью 2 статьи 15.1 Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (далее – Закон № 149-ФЗ)
[13] Федеральный закон от 29 декабря 2006 г. № 244-ФЗ «О государственном регулировании деятельности по организации и проведению азартных игр и о внесении изменений в некоторые законодательные акты Российской Федерации» и Федеральным законом от 11 ноября 2003 г. № 138-ФЗ «О лотереях»

распространяемой посредством сети Интернет, информацией, распространение которой в Российской Федерации запрещено.

На ИТ-компании – провайдеров хостинга и владельцев сайтов возложены следующие обязанности:

в течение суток с момента получения от оператора реестра уведомления о включении доменного имени и (или) указателя страницы сайта в сети Интернет в Единый реестр провайдер хостинга обязан проинформировать об этом обслуживаемого им владельца сайта в сети Интернет и уведомить его о необходимости незамедлительного удаления интернет-страницы, содержащей информацию, распространение которой в Российской Федерации запрещено;

в течение суток с момента получения от провайдера хостинга уведомления о включении доменного имени и (или) указателя страницы сайта в сети Интернет в реестр владелец сайта в сети Интернет обязан удалить интернет-страницу, содержащую информацию, распространение которой в Российской Федерации запрещено. В случае отказа или бездействия владельца сайта в сети Интернет провайдер хостинга обязан ограничить доступ к такому сайту в сети Интернет в течение суток;

в случае непринятия провайдером хостинга и (или) владельцем сайта в сети Интернет вышеуказанных мер, сетевой адрес, позволяющий идентифицировать сайт в сети Интернет, содержащий информацию, распространение которой в Российской Федерации запрещено, включается в Единый реестр.

5.2. Ограничение доступа к информации, распространяемой с нарушением закона

Статьей 15.3 Закона № 149-ФЗ установлен порядок ограничения доступа к информации, распространяемой с нарушением закона.

В случае обнаружения в сети Интернет, информации, содержащей призывы к массовым беспорядкам, осуществлению экстремистской деятельности, участию в массовых (публичных) мероприятиях, проводимых с нарушением установленного порядка, включая случай поступления уведомления о распространении такой информации от федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации, органов местного самоуправления, организаций или граждан, Генеральный прокурор Российской Федерации или его заместители направляют требование в Роскомнадзор, о принятии мер по ограничению доступа к информационным ресурсам, распространяющим такую информацию.

Роскомнадзор на основании обращения незамедлительно определяет провайдера хостинга или иное лицо, обеспечивающее размещение в сети Интернет, указанного информационного ресурса, обслуживающего владельца сайта в сети Интернет, на котором размещена информация, содержащая

призывы к массовым беспорядкам, осуществлению экстремистской деятельности, участию в массовых (публичных) мероприятиях, проводимых с нарушением установленного порядка. Затем провайдеру хостинга или иным вышеназванным лицам направляется уведомление в электронном виде на русском и английском языках о нарушении порядка распространения информации с указанием доменного имени и сетевого адреса, позволяющих идентифицировать сайт в сети Интернет, на котором размещена информация, содержащая призывы к массовым беспорядкам, осуществлению экстремистской деятельности, участию в массовых (публичных) мероприятиях, проводимых с нарушением установленного порядка, а также указателей страниц сайта в сети Интернет, позволяющих идентифицировать такую информацию, и с требованием принять меры по удалению такой информации;

В течение суток с момента получения уведомления провайдер хостинга или иное вышеуказанное лицо обязаны проинформировать об этом обслуживаемого ими владельца информационного ресурса и уведомить его о необходимости незамедлительно удалить информацию, содержащую призывы к массовым беспорядкам, осуществлению экстремистской деятельности, участию в массовых (публичных) мероприятиях, проводимых с нарушением установленного порядка.

5.3. Обязанности ИТ-компаний - организаторов распространения информации и владельцев сайта в сети Интернет

ИТ-компании могут выступать в качестве организаторов распространения информации[14] и владельцев сайта в сети Интернет[15], при этом их деятельность регулируется Законом № 149-ФЗ.

На организаторов распространения информации распространяются следующие обязанности:

в установленном Правительством Российской Федерации порядке 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 свой деятельности.

хранить на территории Российской Федерации информацию о фактах приема, передачи, доставки и (или) обработки голосовой информации, письменного текста, изображений, звуков или иных электронных сообщений пользователей сети Интернет и информацию об этих пользователях в течение шести месяцев с момента окончания осуществления таких действий, а также предоставлять

[14] Лицо, осуществляющее деятельность 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 сети Интернет.

[15] Лицо, самостоятельно и по своему усмотрению определяющее порядок использования сайта в сети Интернет, в том числе порядок размещения информации на таком сайте.

указанную информацию уполномоченным государственным органам, осуществляющим оперативно-разыскную деятельность или обеспечение безопасности Российской Федерации, в случаях, установленных федеральными законами.

обеспечивать реализацию установленных федеральным органом исполнительной власти в области связи по согласованию с уполномоченными государственными органами, осуществляющими оперативно-разыскную 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.

предоставлять информацию, запрашиваемую Роскомнадзором, необходимую для ведения реестра сайтов и (или) страниц сайтов в сети Интернет, не позднее чем в течение десяти дней со дня получения запроса.

Вправе обжаловать в суде решение о включении в реестр «запрещенных сайтов» 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. Обжаловать такое решение можно в течение трех месяцев со дня его принятия.

Для владельцев сайтов в сети Интернет установлено право обращаться в Роскомнадзор с заявлением об исключении из реестра «запрещенных сайтов» доменного имени, указателя страницы сайта в сети Интернет или сетевого адреса, позволяющего идентифицировать сайт в сети Интернет после принятия мер по удалению информации, распространение которой в Российской Федерации запрещено. Обязанности владельцев сайтов указаны в пунктах 1-4 данного раздела.

Статьей 13.31. Кодекса Российской Федерации об административных правонарушениях установлена ответственность за неисполнение обязанностей организатором распространения информации в сети Интернет, в частности:

неисполнение организатором распространения информации в сети Интернет обязанности уведомить Роскомнадзор 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 сети Интернет влечет наложение административного штрафа на граждан в размере от одной тысячи до трех тысяч рублей; на

должностных лиц - от десяти тысяч до тридцати тысяч рублей; на юридических лиц - от ста тысяч до трехсот тысяч рублей;

неисполнение организатором распространения информации в сети Интернет установленной федеральным законом обязанности хранить и (или) предоставлять уполномоченным государственным органам, осуществляющим оперативно-разыскную деятельность или обеспечение безопасности Российской Федерации, информацию о фактах приема, передачи, доставки и (или) обработки голосовой информации, письменного текста, изображений, звуков или иных электронных сообщений пользователей сети Интернет и информацию о таких пользователях влечет наложение административного штрафа на граждан в размере от трех тысяч до пяти тысяч рублей; на должностных лиц - от тридцати тысяч до пятидесяти тысяч рублей; на юридических лиц - от трехсот тысяч до пятисот тысяч рублей;

неисполнение организатором распространения информации в сети Интернет обязанности обеспечивать реализацию установленных в соответствии с федеральным законом требований к оборудованию и программно-техническим средствам, используемым указанным организатором в эксплуатируемых им информационных системах, для проведения уполномоченными государственными органами, осуществляющими оперативно-разыскную деятельность или обеспечение безопасности Российской Федерации, в случаях, установленных федеральными законами, мероприятий в целях осуществления таких видов деятельности, а также принимать меры по недопущению раскрытия организационных и тактических приемов проведения указанных мероприятий влечет наложение административного штрафа на граждан в размере от трех тысяч до пяти тысяч рублей; на должностных лиц - от тридцати тысяч до пятидесяти тысяч рублей; на юридических лиц - от трехсот тысяч до пятисот тысяч рублей.[16]

Статьей 19.7.10 Кодекса Российской Федерации об административных правонарушениях установлена ответственность за непредставление или несвоевременное представление в Роскомнадзор, провайдером хостинга или иным лицом, обеспечивающим размещение сайта или страницы сайта в сети Интернет, данных, позволяющих идентифицировать блогера, либо представление в указанный орган заведомо недостоверных сведений (административный штраф на граждан в размере от десяти тысяч до тридцати тысяч рублей; на юридических лиц - от пятидесяти тысяч до трехсот тысяч рублей). Повторное в течение года совершение административного вышеуказанного правонарушения влечет наложение административного штрафа на граждан в размере от тридцати тысяч до пятидесяти тысяч рублей;

[16]За административные правонарушения, предусмотренные настоящей статьей, лица, осуществляющие предпринимательскую деятельность без образования юридического лица, несут административную ответственность как юридические лица.

на юридических лиц - от трехсот тысяч до пятисот тысяч рублей или административное приостановление деятельности на срок до тридцати суток.

5.4. Обязанности ИТ-компаний – новостных агрегаторов

На владельцев новостных агрегаторов возлагаются обязанности по недопущению распространения информации противоправного и порочащего характера, по проверке достоверности общественно значимых сведений, а также по соблюдению требований законодательства Российской Федерации, регулирующих порядок распространения массовой информации[17].

Предусматривается, что Роскомнадзор будет формировать и вести Реестр новостных агрегаторов в целях контроля за их функционированием. Установлена административная ответственность за неисполнение владельцем новостного агрегатора своих обязанностей.

[17] Федеральный закон от 23 июня 2016 г. № 208-ФЗ «О внесении изменений в Федеральный закон «Об информации, информационных технологиях и о защите информации» и Кодекс Российской Федерации об административных правонарушениях»

6. Оформление авторских прав на программы для ЭВМ

По российскому законодательству права на программное обеспечение охраняются так же, как авторские права на произведения литературы, и поэтому охраняют конкретную реализацию алгоритма, а не сам алгоритм.

В отличие от литературных произведений государство предусмотрело в отношении программы для ЭВМ дополнительное средство защиты — регистрация в федеральном органе исполнительной власти по интеллектуальной собственности (Роспатент).

Регистрация необходима для подтверждения авторства и факта приобретения интеллектуальных прав на ПО, а значит и для последующей их коммерциализации, желательно дополнительно обеспечить себя более надежными доказательствами и документами.

Непосредственно регистрацией программ ЭВМ занимается ФИПС - Федеральное государственное бюджетное учреждение Федеральный институт промышленной собственности.

7. Особенности работы ИТ-компаний с государственными заказчиками

7.1. Соблюдение требований к взаимодействию информационных систем

При разработке ИТ-компаниями информационных систем для государственного сектора следует соблюдать правила интеграции информационных систем федеральных органов исполнительной власти, государственных внебюджетных фондов, исполнительных органов государственной власти субъектов Российской Федерации, органов местного самоуправления, государственных и муниципальных учреждений, многофункциональных центров, иных органов и организаций, используемых при предоставлении государственных и муниципальных услуг и исполнении государственных и муниципальных функций в электронной форме (далее - информационные системы), с единой системой межведомственного электронного взаимодействия, а также требования к техническому обеспечению информационного обмена, осуществляемого с применением системы взаимодействия, между информационными системами в целях предоставления государственных и муниципальных услуг и исполнения государственных и муниципальных функций в электронной форме[18].

7.2. Соблюдение требований к официальным сайтам

При создании ИТ-компаниями официальных сайтов для органов государственной власти необходимо помнить, о необходимости соблюдения требований к технологическим, программным и лингвистическим средствам обеспечения пользования официальными сайтами государственных органов и органов местного самоуправления, так как статьей 13.27. Кодекса Российской Федерации об административных правонарушениях предусматривается наложение административного штрафа на должностных лиц в размере от трех тысяч до пяти тысяч рублей за их неисполнение.

7.3. Подключение к инфраструктуре электронного правительства

В соответствии с Правилами присоединения информационных систем организаций к инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг и исполнения государственных и муниципальных функций в электронной форме (далее –

[18] Установлены приказом Минкомсвязи России от 23 июня 2015 г. № 210 «Об утверждении Технических требований к взаимодействию информационных систем в единой системе межведомственного электронного взаимодействия

инфраструктура электронного правительства)[19] присоединение информационных систем подключаемых организаций к инфраструктуре электронного правительства осуществляется случае, если необходимость информационного взаимодействия этих организаций с органами и организациями, предоставляющими или участвующими в предоставлении государственных и (или) муниципальных услуг либо исполнении государственных и муниципальных функций, предусмотрена федеральными законами, актами Президента Российской Федерации или актами Правительства Российской Федерации.

Подключение информационной системы разработанной ИТ-компаниями к инфраструктуре электронного правительства возможно только при наличии оснований указанных в федеральных законах, актах Президента Российской Федерации или Правительства Российской Федерации.

7.4. Порядок создания и эксплуатации государственных информационных систем

При создании ИТ-компаниями информационных систем для органов власти следует соблюдать требования к порядку реализации мероприятий по созданию, развитию, вводу в эксплуатацию, эксплуатации и выводу из эксплуатации государственных информационных систем и дальнейшему хранению содержащейся в их базах данных информации, осуществляемых федеральными органами исполнительной власти и органами исполнительной власти субъектов Российской Федерации.

Постановление Правительства Российской Федерации от 6 июля 2015 г. № 676 «О требованиях к порядку создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации государственных информационных систем и дальнейшего хранения содержащейся в их базах данных информации» устанавливает требования к «жизненному циклу» государственных информационных систем начиная от их создания и заканчивая выводом из эксплуатации.

[19] Постановление Правительства Российской Федерации от 22 декабря 2012 г. № 1382

8. Основные ГОСТ в области информационных технологий

Действующие межгосударственные стандарты (ГОСТ) и национальные стандарты Российской Федерации (ГОСТ Р) в области информационных технологий (на сегодняшний день действуют более 400 различных стандартов) размещаются для ознакомления на официальном сайте Федерального агентства по техническому регулированию и метрологии (http://www.gost.ru/wps/portal/pages.CatalogOfStandarts).

Ниже, например, приведены основные стандарты, регулирующие этапы «жизненного цикла» информационных систем:

а) ГОСТ 34.003-90 «Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения»

Стандарт устанавливает термины и определения основных понятий в области автоматизированных систем (АС) и распространяется на АС, используемые в различных сферах деятельности, содержанием которых является переработка информации.

б) ГОСТ 34.601-90 «Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания»

Стандарт распространяется на автоматизированные системы (АС), используемые в различных видах деятельности, включая их сочетания, создаваемые в организациях, объединениях и на предприятиях. Стандарт устанавливает стадии и этапы создания АС.

в) ГОСТ 34.602-89 «Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы»

Стандарт распространяется на автоматизированные системы для автоматизации различных видов деятельности и устанавливает состав, содержание, правила оформления документа «Техническое задание на создание (развитие или модернизацию) системы».

г) ГОСТ 34.603-92 «Информационная технология. Виды испытаний автоматизированных систем»

Стандарт распространяется на автоматизированные системы и устанавливает виды испытаний АС и общие требования к их проведению.

С 1 ноября 2017 г. вводится в действие ГОСТ ISO/IEC 17788-2016 «Информационные технологии. Облачные вычисления. Общие положения и терминология»

Стандарт является терминологической основой для стандартов облачных вычислений. Он содержит обзор концепции облачных вычислений наряду с рядом терминов и определений. Стандарт может использоваться организациями любых типов.

9. Нормативные правовые акты и методические документы по технической защите информации, национальные стандарты Российской Федерации в сфере информационной безопасности

С нормативными правовыми актами, организационно-распорядительными и методическими документами по технической защите информации, национальными стандартами Российской Федерации в сфере информационной безопасности можно ознакомится на сайте ФСТЭК России.

Ниже приведены основные документы:

а) методический документ «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11 февраля 2014 г.)

Методический документ детализирует организационные и технические меры защиты информации, принимаемые в государственных информационных системах в соответствии с требованиями о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденными приказом ФСТЭК России от 11 февраля 2013 г. № 17, а также определяет содержание мер защиты информации и правила их реализации. В методическом документе не рассматриваются содержание, правила выбора и реализации мер защиты информации, связанных с применением криптографических методов защиты информации и шифровальных (криптографических) средств защиты информации.

б) Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных. ФСТЭК России, 2008 год

Модель угроз содержит систематизированный перечень угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Эти угрозы обусловлены преднамеренными или непреднамеренными действиями физических лиц, действиями зарубежных спецслужб или организаций (в том числе террористических), а также криминальных группировок, создающих условия (предпосылки) для нарушения безопасности персональных данных (ПДн), которое ведет к ущербу жизненно важных интересов личности, общества и государства.

в) методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. ФСТЭК России, 2008 год

Методика определения актуальных угроз безопасности персональных данных (ПДн) при их обработке в информационных системах персональных данных

(ИСПДн) предназначена для использования при проведении работ по обеспечению безопасности персональных данных при их обработке в следующих автоматизированных информационных системах персональных данных: государственных или муниципальных ИСПДн; ИСПДн, создаваемых и (или) эксплуатируемых предприятиями, организациями и учреждениями независимо от форм собственности, необходимых для выполнения функций этих организаций в соответствии с их назначением; ИСПДн, создаваемых и используемых физическими лицами, за исключением случаев, когда последние используют указанные системы исключительно для личных и семейных нужд.

г) Руководящий документ. Приказ председателя Гостехкомиссии России от 19 июня 2002 г. № 187 «Безопасность информационных технологий. Критерии оценки безопасности информационных технологий»

Руководящий документ содержит систематизированный каталог требований к безопасности информационных технологий, порядок и методические рекомендации по его использованию при задании требований, разработке, оценке и сертификации продуктов и систем информационных технологий по требованиям безопасности информации.

д) Руководящий документ. Приказ председателя Гостехкомиссии России от 4 июня 1999 г. № 114 «Защита от несанкционированного доступа к информации. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей»

Руководящий документ устанавливает классификацию программного обеспечения (ПО) (как отечественного, так и импортного производства) средств защиты информации, в том числе и встроенных в общесистемное и прикладное ПО, по уровню контроля отсутствия в нем недекларированных возможностей.

е) Руководящий документ. Решение председателя Гостехкомиссии России от 25 июля 1997 г. «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа. Показатели защищенности от несанкционированного доступа к информации»

Руководящий документ устанавливает классификацию межсетевых экранов по уровню защищенности от несанкционированного доступа к информации на базе перечня показателей защищенности и совокупности описывающих их требований.

ж) Руководящий документ. Решение председателя Гостехкомиссии России от 30 марта 1992 г. «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации»

Руководящий документ устанавливает классификацию автоматизированных систем, подлежащих защите от несанкционированного доступа к информации, и требования по защите информации в АС различных классов.

з) Руководящий документ. Решение председателя Гостехкомиссии России от 30 марта 1992 г. «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации»

Руководящий документ устанавливает классификацию средств вычислительной техники по уровню защищенности от несанкционированного доступа к информации на базе перечня показателей защищенности и совокупности описывающих их требований.

и) Руководящий документ. Решение председателя Гостехкомиссии России от 30 марта 1992 г. «Защита от несанкционированного доступа к информации. Термины и определения»

Руководящий документ устанавливает термины и определения понятий в области защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации.

к) Руководящий документ. Решение председателя Гостехкомиссии России от 30 марта 1992 г. «Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации»

Документ излагает систему взглядов, основных принципов, которые закладываются в основу проблемы защиты информации от несанкционированного доступа, являющейся частью общей проблемы безопасности информации.

Концепция предназначена для заказчиков, разработчиков и пользователей СВТ и АС, которые используются для обработки, хранения и передачи требующей защиты информации.

л) ГОСТ РО 0043-003-2012 «Защита информации. Аттестация объектов информатизации. Общие положения»;

ГОСТ РО 0043-004-2013 «Защита информации. Аттестация объектов информатизации. Программа и методики аттестационных испытаний»;

ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения»;

ГОСТ Р 53114-2008 «Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения».

Стандарты устанавливают основные термины, применяемые при проведении работ по стандартизации в области обеспечения информационной безопасности в организации.

Термины, установленные стандартами, рекомендуется использовать в правовой, нормативной, технической и организационно-распорядительной документации, научной, учебной и справочной литературе.