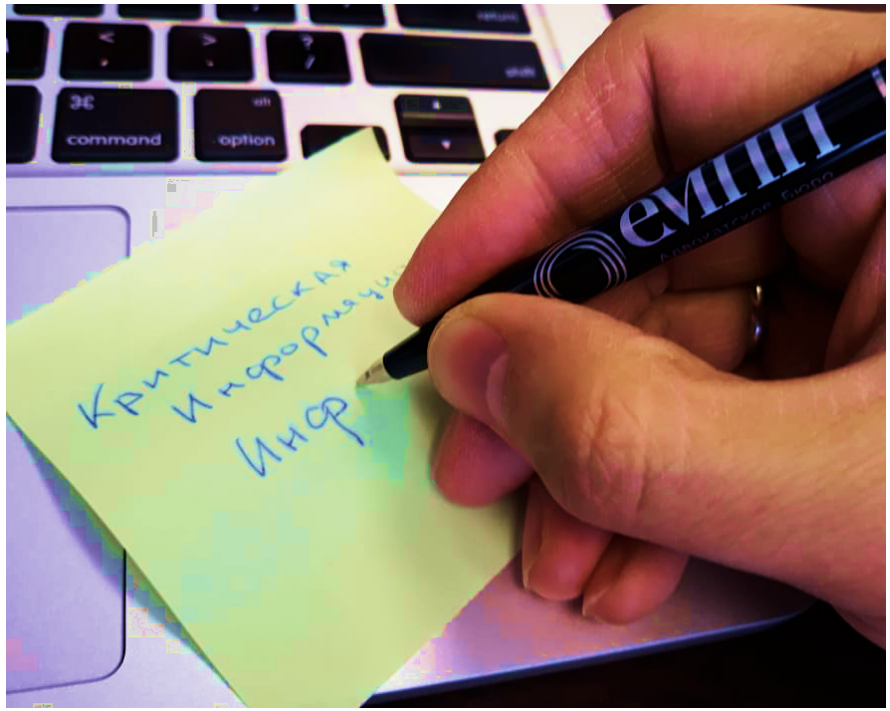
АБ ЕМПП
17|2 Скаковая ул. | Москва, Россия
БЦ Скаковая 17| 8 ой этаж
Тел: +7 495 945-51-90
E-mail: info@empp.ru | web: www.empp.ru

РЕГУЛИРОВАНИЕ IT / TMT: ОБЗОР ИЗМЕНЕНИЙ

Апрель 2020 – Март 2021



В апреле 2020 г. мы публиковали обзор предстоящих изменений законодательства в сфере IT / TMT[1], в котором рассматривались вопросы обязательного использования отечественного софта российскими госорганами, установления запрета на использование иностранного ПО в объектах российской критической инфраструктуры, обязательной предустановки российского ПО на «умные» эл. устройства и некоторые другие.

Вместе с тем, несмотря на введенные противоэпидемиологические ограничения, оставшаяся часть 2020 года также оказалась богата на нормотворческие инициативы. Уже после выхода прошлого обзора неоднократно появлялась информация о предложенных к обсуждению изменениях законодательства. В частности, обширный список, состоящий из 15 мер по поддержке IT-индустрии, был подготовлен Минцифры и направлен председателю Правительства РФ в конце весны 2020[2].

[1] URL: https://empp.ru/assets/files/empp-alert-ittmt-update.pdf
[2] URL: https://www.cnews.ru/news/top/2020-06-24_putin_predlozhil_ustanovit

АБ ЕМПП
17|2 Скаковая ул. | Москва, Россия
БЦ Скаковая 17| 8 ой этаж
Тел: +7 495 945-51-90
E-mail: info@empp.ru | web: www.empp.ru

Сообщается, что в качестве предложений была указана отсрочка уплаты налогов на доходы сотрудников IT-компаний, отмена уплаты ими страховых взносов в фонд оплаты труда до конца 2020, снижение налога на прибыль с 20% до 12% и обнуление НДС на различные онлайн-услуги. Также было предложено приостановить на один год реализацию требований так называемого «Закона Яровой» в части ежегодного увеличения операторами связи объёма абонентских данных, хранящихся в их базах, на 15%.

После этого, в июне 2020, главой Минцифры Максутом Шадаевым в рамках совещания с Владимиром Путиным было высказано мнение о том, что падение IT-отрасли возможно в полной мере компенсировать за счет перевода госкомпаний на отечественный софт в императивном порядке по аналогии с тем, как это реализуется в госорганах в течение последних нескольких лет.

В связи с этим, в настоящем обзоре мы намерены разобраться, какие из предложенных мер были в итоге приняты к исполнению и в каком виде, а также какие изменения претерпели инициативы, о которых мы писали ранее.

I. КРИТИЧЕСКАЯ ИНФОРМАЦИОННАЯ ИНФРАСТРУКТУРА

1.1. Отсрочка импортозамещения в объектах критической информационной инфраструктуры на три года

Министерством цифрового развития, связи и массовых коммуникаций России в мае 2020 был подготовлен проект указа Президента РФ «О мерах экономического характера по обеспечению технологической независимости и безопасности объектов критической информационной инфраструктуры».

Первоначальный проект содержал следующие положения:

- Правительство РФ в срок до 01.09.2020 должно было утвердить требования к ПО и оборудованию, используемому на объектах критической информационной инфраструктуры (***«КИИ»***)[3], и порядок перехода на преимущественное использование российского ПО и оборудования.
- Субъекты критической информационной инфраструктуры в порядке, установленном Правительством РФ, должны перейти на преимущественное использование отечественного ПО в срок до 01.01.2021 и на преимущественное использование отечественного оборудования – до 01.01.2022.

В процессе общественного обсуждения проекта по просьбам преимущественно финансовых организаций и Ассоциации банков

[3] Напомним, что к объектам КИИ, согласно ст. 2 Федерального закона от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» (***«Закон о КИИ»***), относят информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления субъектов критической информационной инфраструктуры. При этом закон отдельно выделяет понятие значимых объектов КИИ, которым присваивается соответствующая категория в зависимости от их политической, социальной, экономической, экологической и оборонной значимости и которые подлежат включению в специальный реестр.

АБ ЕМПП
17|2 Скаковая ул. | Москва, Россия
БЦ Скаковая 17| 8 ой этаж
Тел: +7 495 945-51-90
E-mail: info@empp.ru | web: www.empp.ru

России указанные сроки были изменены: переход на отечественное ПО должен будет завершиться 01.01.2024, а на отечественное оборудование – 01.01.2025.

Как отмечают эксперты, даже с учетом новых сроков выполнить поставленную задачу будет трудно. И если для перехода на отечественный софт сроки выглядят приемлемыми, то для перехода на российское оборудование они остаются нереальными, поскольку цикл его создания в 2-3 раза длиннее – приводит слова Кирилла Булгакова, управляющего директора компании «Техносерв Консалтинг», газета «Коммерсантъ»[4].

Некоторые также отмечают, что под российским оборудованием на сегодняшний день в основном понимаются устройства и комплектующие китайских производителей, но с нанесенной на них маркировкой отечественных компаний. В других же объектах КИИ до сих пор используется советское оборудование 50-60х годов прошлого века, и говорить о качественном переходе на оборудование, произведенное в России, в их случае не приходится, по крайней мере, в установленные сроки.

Помимо указанного указа Президента РФ Минцифры были также разработаны проекты следующих документов:

- требования к ПО и оборудованию, используемому на объектах КИИ (***«Требования»***);
- порядок перехода на преимущественное использование российского ПО и оборудования (***«Порядок»***);
- Постановление Правительства РФ об утверждении указанных требований и порядка.

В качестве основного требования к ПО и оборудованию, используемому во всех объектах КИИ, было указано, что такое ПО должно быть включено в единый реестр российского программного обеспечения (***«РПО»***) или единый реестр евразийского программного обеспечения (***«РЕП»***), а оборудование – в единый реестр российской радиоэлектронной продукции (***«РРП»***).

Очевидно, что далеко не всякое ПО или оборудование зарубежного происхождения может быть заменено отечественными аналогами. По этой причине в Требованиях в качестве исключений были указаны случаи, когда использование таких иностранных устройств и программ всё-таки возможно:

- если в РПО, РЕП или РРП отсутствуют сведения о ПО или оборудовании, которые могли бы заменить иностранные аналоги, используемые субъектом КИИ;
- если в РРП есть сведения о телекоммуникационном оборудовании, однако его характеристики не позволяют достичь тех целей и задач субъекта КИИ, которые установлены законом.

[4] URL: https://www.kommersant.ru/doc/4557385?from=four_tech

АБ ЕМПП
17|2 Скаковая ул. | Москва, Россия
БЦ Скаковая 17| 8 ой этаж
Тел: +7 495 945-51-90
E-mail: info@empp.ru | web: www.empp.ru

При использовании такого иностранного софта или оборудования должны быть обеспечены возможности по их модернизации, гарантийной и технической поддержке российскими компаниями, находящимися вне прямого или косвенного контроля иностранных физических или юридических лиц. Однако, кто именно должен обеспечивать такие возможности и как контролировать соблюдение этого требования, в проекте нормативного акта не указано.

Специальные требования установлены Федеральной службой по техническому и экспортному контролю (***«ФСТЭК»***) для ПО и устройств, которыми обеспечивается безопасность значимых объектов КИИ[5]. В частности, они должны пройти оценку на соответствие требованиям безопасности в форме обязательной сертификации, испытаний или приёмки. Такому ПО или оборудованию (по терминологии приказа – средства защиты информации) присваивается класс защиты и уровень доверия, в зависимости от которых определяется категория значимых объектов КИИ, в которых допустимо использование этих средств.

Требования к средствам защиты информации в значимых объектах КИИ:

- данные средства защиты должны быть обеспечены гарантийной и (или) технической поддержкой;
- не допускается наличие удаленного доступа к таким средствам. Если исключить наличие такого доступа невозможно, должны быть реализованы необходимые меры по осуществлению контроля удаленного доступа с идентификацией лиц, мониторингом их действий и защитой информации, передаваемой при таком доступе;
- не допускается наличие бесконтрольного локального доступа к указанным средствам защиты для обновления и управления со стороны лиц, не являющихся работниками субъекта КИИ, его дочерних или зависимых обществ;
- для значимых объектов КИИ 1 и 2 категорий средства защиты, осуществляющие хранение и обработку информации, должны размещаться на территории России. Исключение допустимы в случаях, когда средства защиты размещаются в филиалах или представительствах значимых объектов КИИ за рубежом, а также когда это предусмотрено российским законодательством или международными договорами.

1.2. Госкомпании и госкорпорации как субъекты КИИ

Осенью издание «Коммерсантъ» со ссылками на пресс-службу Правительства, Минюст, Минкомсвязи и Минпромторг сообщило, что на рассмотрении указанных ведомств находится пакет поправок к Закону о КИИ. Соответствующий законопроект был

[5] Раздел IV приказа ФСТЭК от 25.12.2017 № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры РФ» (в ред. приказа ФСТЭК от 20.02.2020 № 35).

АБ ЕМПП
17|2 Скаковая ул. | Москва, Россия
БЦ Скаковая 17| 8 ой этаж
Тел: +7 495 945-51-90
E-mail: info@empp.ru | web: www.empp.ru

внесен в Правительство членом Совета Федерации К. Долговым в августе 2020.

Суть предложенных поправок состоит в том, чтобы с 01.01.2021 приравнять статус госкомпаний и госкорпораций к субъектам КИИ. Как следствие, указанные организации будут обязаны в установленные сроки перейти на использование отечественного ПО и IT-оборудования. При этом будет определена степень обязательной локализации оборудования на территории РФ, а также случаи полного запрета на использование зарубежных программ и устройств.

Стоит заметить, что импортозамещение в госкомпаниях уже идет не первый год, однако, осуществляется оно либо на основании указаний Председателя Правительства РФ, либо по собственной инициативе руководства компаний. К примеру, об таком переходе сообщили в Госкорпорации «Ростех».

К настоящему моменту законопроект, представленный К. Долговым, не внесен в Государственную Думу, его текст отсутствует в свободном доступе, а министерства, на рассмотрении которых он находится, не делают каких-либо заявлений на его счет. В связи с этим затруднительно оценить вероятность принятия соответствующего закона.

II. КИБЕРБЕЗОПАСНОСТЬ

2.1. Отсрочка реализации Закона Яровой

23.09.2020 Правительством РФ был одобрен «Общенациональный план действий, обеспечивающих восстановление занятости и доходов населения, рост экономики и долгосрочные структурные изменения в экономике» (***«План»***). Срок действия Плана: с июня 2020 по декабрь 2021.

В качестве цели, помимо прочего, был указан *«выход на устойчивую траекторию экономического роста и роста доходов населения, обеспечивающую реализацию национальных целей развития экономики на основе использования новых технологий, включая цифровизацию»*.

Для достижения поставленных целей в Плане предусмотрен обширный перечень ключевых инициатив. Одна из таких инициатив именуется «Умной реабилитацией» и включает в себя комплекс мер по поддержке и развитию наиболее пострадавших отраслей промышленности, транспорта, сферы услуг, строительства и ЖКХ.

В рамках «Умной реабилитации» Планом предусмотрено приостановление на один год нормы о ежегодном 15 % увеличении емкости технических средств накопления информации (***«ТСНИ»***) и

АБ ЕМПП
17|2 Скаковая ул. | Москва, Россия
БЦ Скаковая 17| 8 ой этаж
Тел: +7 495 945-51-90
E-mail: info@empp.ru | web: www.empp.ru

исключение из расчета емкости ТСНИ тяжелого контента / видеотрафика[6]. Ниже вкратце напомним, о какой норме идет речь.

Федеральным законом от 06.07.2016 № 374-ФЗ «О внесении изменений в Федеральный закон «О противодействии терроризму» и отдельные законодательные акты Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности», более известным как «Закон Яровой», п. 1 ст. 64 Федерального закона от 07.07.2003 № 126-ФЗ «О связи» был изложен в новой редакции: операторов связи обязали хранить на территории РФ текстовые сообщения, голосовую информацию, изображения, звуки и видеосообщения пользователей в течение шести месяцев, а информацию о фактах приема, передачи, доставки таких сообщений – в течение трёх лет.

Порядок, сроки и объём хранения такой информации был установлен Правительством РФ в Постановлении от 12.04.2018 № 445 «Об утверждении Правил хранения операторами связи текстовых сообщений пользователей услугами связи, голосовой информации, изображений, звуков, видео- и иных сообщений пользователей услугами связи». Согласно п. 6 постановления хранение и автоматическое удаление информации по истечении установленных законом сроков должно осуществляться в ТСНИ. При этом емкость ТСНИ подлежит ежегодному увеличению на 15% в течение пяти лет с даты ввода ТСНИ в эксплуатацию.

Теперь же выполнение этого требования отсрочено на год, а видеоконтент в принципе не подлежит обязательному хранению. Как отмечают эксперты, последнее связано с увеличением трафика видеоданных в связи с пандемией и длительным режимом самоизоляции граждан в 2020 году.

Необходимо заметить, что отсрочка реализации Закона Яровой это не единственная мера, предусмотренная в Плане восстановления экономики. Среди предусмотренных мер поддержки операторов связи дополнительно можно выделить следующие:

- упрощение доступа операторам связи в многоквартирные дома для размещения сетей связи на принципах недискриминационного доступа (с января 2021);
- установление требований к нормативам при строительстве (ремонте, реконструкции) многоквартирных домов и автомобильных дорог федерального значения в части формирования необходимой инфраструктуры систем электропитания и линий связи (с января 2021);
- проработка вопроса о выходе операторов связи и центров обработки данных (***«ЦОД»***) на оптовый рынок электроэнергии.

[6] Отсрочка начала действовать с сентября 2020. Несмотря на указанный срок в один год, в самом Плане период действия меры определен по сентябрь 2022. Полагаем, в Плане допущена опечатка.

АБ ЕМПП
17|2 Скаковая ул. | Москва, Россия
БЦ Скаковая 17| 8 ой этаж
Тел: +7 495 945-51-90
E-mail: info@empp.ru | web: www.empp.ru

Для ЦОД соответствующий проект Постановления Правительства РФ был опубликован на сайте regulation.gov.ru в августе 2020 (ID проекта: 02/07/08-20/00106889) и в настоящий момент находится в стадии публичных обсуждений.

2.2. Штрафы за нарушение мер безопасности КИИ

На рассмотрении в Госдуме находится законопроект № 1048574-7 «О внесении изменений в КоАП РФ в части установления административной ответственности за нарушение законодательства в области обеспечения безопасности критической информационной инфраструктуры РФ». Как следует из его содержания, в законопроекте предлагается дополнить КоАП РФ несколькими статьями, устанавливающими административную ответственность субъектов КИИ за следующие правонарушения:

- нарушение требований к созданию систем безопасности значимых объектов КИИ;
- нарушение порядка информирования о компьютерных инцидентах, реагирования на них и принятия мер по устранению последствий компьютерных атак;
- нарушение порядка обмена информацией о компьютерных инцидентах между субъектами КИИ;
- непредставление или несвоевременное представление сведений о присвоении объекту КИИ категории значимости;
- непредставление или нарушение порядка или сроков предоставления информации в систему ГосСОПКА.

Размер штрафов по указанным статьям разнятся, однако для физических лиц не превышают 50 000 руб., а для юридических – 500 000 руб. Срок давности привлечения к административной ответственности составит 1 год. Рассматривать дела данной категории в зависимости от состава правонарушения будут сотрудники ФСТЭК или ФСБ.

В случае принятия закона поправки к КоАП вступят в силу с 01.09.2021.

Как указано в пояснительной записке к законопроекту, в настоящий момент требования по обеспечению безопасности КИИ не выполняются в должной степени. В частности, субъектами не производится своевременное обновление ПО, не утверждаются регламенты работы с электронной почтой, не выполняются минимальные требования по защите периметра информационных и автоматизированных систем. Такие нарушения в 2017 привели к заражению компьютеров в трёх государственных компаниях вирусом WannaCry. На восстановление работоспособности ЭВМ ушло до 3 суток, а затраты каждой из компаний составляли от трёх до пяти миллионов рублей без учета стоимости восстановления инфраструктурного и прикладного ПО, а также информации, хранящейся на компьютерах.

Также в пояснительной записке отмечается, что в 2019 Национальным координационным центром по компьютерным инцидентам было выявлено 120 таких инцидентов, однако, ни об одном из них сведения в ГосСОПКА не поступили.

АБ ЕМПП
17|2 Скаковая ул. | Москва, Россия
БЦ Скаковая 17| 8 ой этаж
Тел: +7 495 945-51-90
E-mail: info@empp.ru | web: www.empp.ru

На данном этапе сложно оценить перспективы введения ответственности за указанные нарушения. Из изложенного выше материала относительно ГосСОПКА, порядка присоединения к ней и её работы можно предположить, что не предоставление или несвоевременное предоставление информации в систему может быть вызвано объективными причинами, такими как сложность и дороговизна соответствующих мероприятий, а также техническими трудностями при работе с ГосСОПКА.

В любом случае эффективность норм в целом и предусмотренных ими санкций в частности станет понятна только в результате их практического применения.

2.3. Подключение к ГосСОПКА всех операторов персональных данных

В начале декабря прошлого года группа депутатов Госдумы представила законопроект № 1070431-7 «О внесении изменений в отдельные законодательные акты Российской Федерации в части обеспечения конфиденциальности сведений о защищаемых лицах и об осуществлении оперативно-розыскной деятельности». 30.12.2020 соответствующий федеральный закон № 515-ФЗ был подписан Президентом РФ.

Первоначально в законопроекте предлагалось дополнить ч. 2 ст. 19 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» (***«Закон о персональных данных»***) положениями о том, что безопасность персональных данных обеспечивается:

- принятием мер по обнаружению, предупреждению и ликвидации последствий компьютерных атак на информационные системы персональных данных и по реагированию на компьютерные инциденты (пп. 6 ч. 2 ст. 19);
- организацией и осуществлением взаимодействия с государственной системой обнаружения, предупреждения и ликвидации компьютерных атак на информационные ресурсы (***«ГосСОПКА»***) (пп. 9 ч. 2 ст. 19).

Последнее из положений вызвало бурную и преимущественно негативную реакцию со стороны IT-сообщества, в результате чего в итоговый текст закона не попало. Несмотря на это, считаем необходимым подробнее рассказать об этой инициативе ФСБ и её возможных последствиях, потому как появляется она не в первый раз и с большой вероятностью будет позднее повторно предложена к принятию. Так, в 2018 попытка реализовать аналогичный сбор информации от индивидуальных предпринимателей и субъектов малого бизнеса была предпринята в рамках нацпроекта «Цифровая экономика», однако, успехом так же не увенчалась.

Для начала напомним о том, что из себя представляет упомянутая ГосСОПКА. Концепция этой системы была утверждена Президентом РФ в 2014. Система представляет собой единый централизованный территориально-распределенный комплекс, включающий силы (то есть органы и учреждения) и средства (то есть ПО и оборудование) для обнаружения, предупреждения и

АБ ЕМПП
17|2 Скаковая ул. | Москва, Россия
БЦ Скаковая 17| 8 ой этаж
Тел: +7 495 945-51-90
E-mail: info@empp.ru | web: www.empp.ru

ЕМПП Адвокатское Бюро

ликвидации последствий компьютерных атак. Полномочия по созданию и обеспечению работы системы были возложены на ФСБ.

В дальнейшем по инициативе ведомства был разработан и принят упомянутый выше Закон о КИИ. Законом задачи ГосСОПКА по обнаружению, предупреждению и ликвидации последствий компьютерных атак были изложены только применительно к деятельности субъектов КИИ.

Одной из новых задач системы также стало обеспечение обмена информацией о компьютерных атаках между субъектами КИИ. Для координации этой деятельности приказом ФСБ от 24.07.2018 № 366 был учрежден национальный координационный центр по компьютерным инцидентам.

До настоящего времени на других субъектов требования по взаимодействию с ГосСОПКА не распространяется. Однако ранее упомянутая инициатива законопроекта № 1070431-7 о внесении изменений в пп. 9 ч. 2 ст. 19 Закона о персональных данных могла распространить такое требование на всех операторов персональных данных вообще. Под действие данной нормы могли попасть более 400 тысяч компаний.

Как отмечают эксперты, подключение к ГосСОПКА сложная и затратная процедура как в организационном, техническом, так и в финансовом плане. К примеру, для передачи информации в систему операторы персональных данных будут вынуждены приобретать дополнительное ПО, нанимать сотрудников либо обращаться к коммерческим центрам мониторинга киберугроз (к примеру, Ростелеком-Solar, Информзащита, Инфосистемы Джет, Positive Technologies, Kaspersky Lab и др.).

Следует принять во внимание и технические трудности, с которыми приходится сталкиваться даже субъектам КИИ. Так, ФСБ установлены требования относительно способов шифрования информации, передаваемой в ГосСОПКА, что безусловно требует наличия специального софта. При этом передача должна осуществляться в автоматическом режиме круглосуточно[7].

Безусловно, подключение к системе поможет защитить персональные данные от доступа к ним извне. Однако описанные

[7] См., например: Приказ ФСБ России от 06.05.2019 № 196 «Об утверждении Требований к средствам, предназначенным для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты»; Приказ ФСБ России от 19.06.2019 № 281 «Об утверждении Порядка, технических условий установки и эксплуатации средств, предназначенных для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты, за исключением средств, предназначенных для поиска признаков компьютерных атак в сетях электросвязи, используемых для организации взаимодействия объектов критической информационной инфраструктуры Российской Федерации»; Приказ ФСБ России от 24.07.2018 № 367 «Об утверждении Перечня информации, представляемой в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации и Порядка представления информации в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации».

АБ ЕМПП
17|2 Скаковая ул. | Москва, Россия
БЦ Скаковая 17| 8 ой этаж
Тел: +7 495 945-51-90
E-mail: info@empp.ru | web: www.empp.ru

меры не защитят от утечек информации, спровоцированных самими сотрудниками операторов персональных данных. Очевидно, что расширение ГосСОПКА в описанных масштабах потребует немалых затрат на развитие возможностей и самой системы.

III. РЕЕСТР РОССИЙСКОГО ПО

3.1. Требования к разработчикам ПО для получения льгот по НДС и участия в госзакупках будут отличаться

Фондом развития интернет инициатив в адрес Минцифры было направлено предложение разделить требования для разработчиков ПО, которые претендуют на получение льготы по НДС и участие в госзакупках.

Министерство считает возможным смягчить условия для получения льготы по НДС в рамках «налогового маневра» таким образом, чтобы её могли получить компании с иностранными бенефициарами. При этом не изменятся требования для включения в реестр российского ПО компаний, намеренных участвовать в госзакупках.

Проект Федерального закона «О внесении изменений в статью 12.1 Федерального закона "Об информации, информационных технологиях и о защите информации» (***«Закон о защите информации»***) был размещен Минцифры на сайте regulation.gov.ru 25.09.2020. Изначально предполагалось установить льготу с 2021 года, однако в настоящий период законопроект проходит общественные обсуждения и антикоррупционную экспертизу и ещё не внесен в Государственную Думу.

Как следует из проекта и пояснительной записки к нему, освободить от уплаты НДС планируется только операции по реализации и лицензированию ПО, сведения о котором включены единый реестр российских программ для ЭВМ и баз данных или единый реестр программ для ЭВМ и баз данных из государств-членов Евразийского экономического союза.

При этом из Закона о защите информации будут исключены требования к ПО, подлежащему включению в реестр. Это необходимо для исполнения Россией принятых в рамках ВТО обязательств в части предоставления иностранным товарам и услугам условий, не менее благоприятных, чем предоставляемые российским[8].

Требования к ПО и правообладателям, намеревающимся получить льготу по уплате НДС, должно будет определить Правительство РФ. Технически это будет происходить посредством внесения изменений в постановление Правительства РФ от 16.11.2015 №

[8] Соответствующие обязательства установлены Марракешским соглашением об учреждении Всемирной торговой организации (15.04.1994), Протоколом от 16.12.2011 «О присоединении Российской Федерации к Марракешскому соглашению об учреждении Всемирной торговой организации от 15 апреля 1994 г.», Соглашением по информационным технологиям (Сингапур, 1996).

АБ ЕМПП
17|2 Скаковая ул. | Москва, Россия
БЦ Скаковая 17| 8 ой этаж
Тел: +7 495 945-51-90
E-mail: info@empp.ru | web: www.empp.ru

1236 «Об установлении запрета на допуск программного обеспечения, происходящего из иностранных государств, для целей осуществления закупок для обеспечения государственных и муниципальных нужд» (***«Постановление Правительства № 1236»***).

В сам реестр российского ПО планируется добавить новый раздел, который не будет относиться к госзакупкам.

3.2. ПО для внутреннего использования госорганов планируется исключить из системы госзакупок

Как сообщает «Коммерсантъ», в рамках разработанного Минцифры пакета поправок, изменяющего критерии включения в РПО, было предложено дополнительно разделить софт, входящий в реестр на две категории:

- ПО, которое может участвовать в госзакупках;
- ПО, разрабатываемое госорганами, госкорпорациями и госкомпаниями «для внутреннего использования» и не предназначенное для участия в закупках.

Соответствующие положения предусмотрены в проекте изменений в Постановление Правительства № 1236. Отмечается, что нововведения никак не отразятся на возможности компаний, включенных в РПО, получать льготы по уплате НДС.

Раздел РПО, о котором идет речь, называется «Специализированное ПО органов исполнительной власти РФ, государственных корпораций, компаний и юридических лиц с преимущественным участием РФ для внутреннего использования». Появился он в 2019 с целью включения такого ПО в РПО как условия участия в программе импортозамещения[9]. Однако ознакомиться с проектом нормативного акта, на который ссылается «Коммерсантъ», в настоящее время не представляется возможным.

В тексте поправок к Постановлению Правительства № 1236, опубликованном на сайте regulation.gov.ru 04.09.2020, прямо такие положения не обозначены. Данным документом лишь вводится указание на то, что ПО, разработанное госорганами, госкорпорациями и компаниями с преимущественным участием РФ для внутреннего использования, является исключением из общего правила о свободном обращении на российском рынке всякого ПО, подлежащего включению в РПО[10].

3.3. Новые критерии включения в РПО: локализация, гарантийное обслуживание и техническая поддержка

[9] Приказ Минкомсвязи России от 01.04.2015 № 96 «Об утверждении плана импортозамещения программного обеспечения».

[10] Пп. «б» п. 5 Правил формирования и ведения единого реестра российских программ для электронных вычислительных машин и баз данных и единого реестра программ для электронных вычислительных машин и баз данных из государств - членов Евразийского экономического союза, за исключением Российской Федерации (утв. Постановления Правительства № 1236) (***«Правила ведения РПО»***).

АБ ЕМПП
17|2 Скаковая ул. | Москва, Россия
БЦ Скаковая 17| 8 ой этаж
Тел: +7 495 945-51-90
E-mail: info@empp.ru | web: www.empp.ru

В феврале 2021 Минцифры заявило о разработке проекта изменений в постановление Правительства РФ, определяющего условия включения в РПО[11]. Основная задача состоит в ограничении доступа зарубежного ПО в реестр. Как объясняется, в значительной степени меры обусловлены увеличением числа заявок на включение с конца 2020 и ускорением процедуры их рассмотрения самим министерством.

В качестве основных нововведений указаны следующие требования:

- размещение на территории РФ технических средств для выпуска, использования и обслуживания ПО;
- локализация исходного текста и объектного кода на территории России;
- оказание технической поддержки и гарантийного обслуживания ПО при его лицензировании. В развитие этого критерия установлены требования наличия технической возможности у компании и соответствующей квалификации у её сотрудников для оказания упомянутых услуг.

Изменится и процедура рассмотрения заявок на включение в реестр. В частности, для их рассмотрения можно будет привлекать сторонние экспертные организации, а срок рассмотрения будет сокращен вдвое.

По словам экспертов, важной положительной чертой проекта является сохранение требования о наличии российских бенефициаров у правообладателей ПО, заявленного к включению в реестр.

Однако такие заявления вызывают некоторые вопросы. Непонятно, как данную новость следует рассматривать в контексте ранее опубликованного на портале regulation.gov.ru (ID проекта: 01/01/09-20/00107927) того же самого проекта Постановления Правительства о внесении изменений в Постановление Правительства № 1236, о котором в сентябре 2020 писал «Коммерсантъ»[12].

Напомним, что «Ъ» упоминал прямо противоположные поправки к постановлению. В частности, ими допускалось предоставление доступа в реестр российским юридическим лицам с иностранными бенефициарами, а наличие исключительного права на ПО у лица, подавшего заявку, не было обязательным.

В нынешней редакции требование об исключительно российских конечных бенефициарах правообладателей по-прежнему не усматривается. При этом с вопросом о наличии исключительного права ситуация видится неоднозначной.

Изменения однозначно затронут п. 5 Правил ведения РПО, в котором устанавливаются требования непосредственно к ПО, представляемому для регистрации в реестре. В частности, по

[11] URL: https://digital.gov.ru/ru/events/40366/

[12] URL: https://www.kommersant.ru/doc/4483075

АБ ЕМПП
17|2 Скаковая ул. | Москва, Россия
БЦ Скаковая 17| 8 ой этаж
Тел: +7 495 945-51-90
E-mail: info@empp.ru | web: www.empp.ru

задумке Минцифры исключительным правом на такое ПО должны будут обладать одно или несколько созданных и функционирующих в соответствии с законодательством РФ юридических лиц или индивидуальных предпринимателей[13].

Буквальное толкование пункта не препятствует тому, чтобы заявления о включении ПО в РПО подавались, к примеру, лицензиатами при условии, что лицензиарами ПО являются упомянутые российские юридически лица или ИП.

В то же время в Правилах ведения РПО существует п. 9, устанавливающий требования непосредственно к заявителям. Согласно действующей редакции Правил ведения РПО заявителем может выступать только правообладатель ПО, т.е. лицо, владеющее исключительным правом на него, либо государственный орган, осуществляющий управление исключительными правами, принадлежащими публично-правовым образованиям.

Опубликованный в настоящий момент проект изменений в Постановление Правительства № 1236 п. 9 не затрагивает. В связи с этим, не вполне понятно, идет ли в СМИ речь о другом проекте изменений или же в проект, упомянутый нами, будут внесены правки по мере его рассмотрения.

IV. ЛЬГОТЫ ПО ОБЯЗАТЕЛЬНЫМ ПЛАТЕЖАМ

23.06.2020 Президентом РФ были предложены меры по снижению ставок страховых взносов и налога на прибыль для российских IT-компаний. Соответствующие изменения в НК РФ были внесены Федеральным законом от 31.07.2020 № 265-ФЗ «О внесении изменений в часть вторую Налогового кодекса Российской Федерации» (***«ФЗ № 265»***).

4.1. Льготы по страховым взносам

С 01.01.2021 ставка страховых взносов, подлежащих уплате такими организациями, составит 7,6% вместо 14% (пп. 3 ч. 1 и пп. 1.1 ч. 2 ст. 427 НК РФ). При этом законодатель внес правки и в ч. 5 ст. 427 НК РФ, уточнив условия для получения таких льгот. К примеру, в доход от IT-деятельности компании, который должен составлять не менее 90% от всех доходов компании за отчетный период, теперь в силу прямого указания закона включаются доходы от:

а) реализации экземпляров ПО, разработанного самой компанией;

б) передачи исключительных прав на такое ПО;

в) предоставления прав на использование ПО, разработанного самой компанией, по лицензионным договорам. К этой же категории теперь относится предоставление удаленного доступа к ПО собственной разработки, включая обновления

[13] К слову, сейчас правообладателями для целей регистрации ПО в реестре могут выступать и физические лица.

АБ ЕМПП
17|2 Скаковая ул. | Москва, Россия
БЦ Скаковая 17| 8 ой этаж
Тел: +7 495 945-51-90
E-mail: info@empp.ru | web: www.empp.ru

для него и дополнительные функциональные возможности, предоставляемые через Интернет. Однако из сферы применения нормы были исключены случаи, когда лицензируемое ПО предоставляет возможность:

- рекламировать товары в Интернете или получать доступ к такой информации;
- размещать предложения о приобретении или реализации товаров, работ или услуг;
- осуществлять поиск информации о потенциальных покупателя или продавцах, а также заключать сделки.

г) оказания услуг по разработке, адаптации и модификации ПО, в том числе разработанного организациями-партнерами[14];

д) оказания услуг по установке, тестированию и сопровождению ПО, которое компания самостоятельно разрабатывала, адаптировала или модифицировала.

При этом, если доход компании возник в результате уступки долга, возникшего при признании описанных доходов от IT-деятельности, он не учитывается для целей предоставления льготы (абз. 10 ч. 5 ст. 427 НК РФ).

Аналогичные послабления установлены для новой категории субъектов – российских организаций, осуществляющих деятельность по проектированию и разработке изделий электронной компонентной базы и электронной (радиоэлектронной) продукции (пп. 18 ч. 1 ст. 427 НК РФ). Указанная профильная деятельность должна составлять не менее 90% дохода по итогам отчетного периода, а сама компания должна быть включена в соответствующий реестр Минпромторга. Требования по численности сотрудников таких организаций идентичны требованиям к IT-компаниям.

Прежняя формулировка ч. 5 ст. 427 НК РФ отличалась меньшей определенностью и вводила в заблуждение компании, которые полагали, что в доход от IT-деятельности могут быть включены доходы от распространения ПО, разработанного третьими лицами, что приводило к отказам в предоставлении льгот со стороны налоговых органов. Представляется, что действующая редакция нормы с учетом упомянутых разъяснений ФНС должны исключить подобные разночтения.

4.2. Льготы по налогу на прибыль

В НК РФ введена ч. 1.15 ст. 284, которой для IT-компаний установлена ставка налога на прибыль в 3% вместо 20%. Условия для применения данной ставки практически идентичны условиям для получения льгот на уплату страховых взносов, за исключением требования о наличии у IT-компании аккредитации в Минцифры в

[14] Организации-партнеры не упоминаются в новой редакции закона, однако они прямо указаны в Письме ФНС России от 14.12.2020 № БС-4-11/20560@.

АБ ЕМПП
17|2 Скаковая ул. | Москва, Россия
БЦ Скаковая 17| 8 ой этаж
Тел: +7 495 945-51-90
E-mail: info@empp.ru | web: www.empp.ru

качестве организации, осуществляющей деятельность в области информационных технологий[15].

V. ИНЫЕ НОРМОТВОРЧЕСКИЕ ИНИЦИАТИВЫ

5.1. Разработка концепции по робототехнике и ИИ

Концепция развития регулирования отношений в сфере технологий искусственного интеллекта и робототехники до 2024 года (***«Концепция»***) была утверждена Распоряжением Правительства РФ от 19.08.2020 № 2129-Р.

Целью документа является определение основных принципов, на которых будет основываться дальнейшая реформа законодательства в сфере робототехники и искусственного интеллекта (***«ИИ»***). Сама реформа необходима, чтобы обеспечить развитие и внедрение указанных технологий в различных сферах экономики с соблюдением прав граждан, обеспечением безопасности личности, общества и государства.

В качестве целей Концепции были также указаны:

- формирование принципов регулирования правоотношений, возникающих в связи с разработкой и применением как самих технологий ИИ и робототехники, так и систем, созданных на их основе;
- определение правовых барьеров, препятствующих разработке и применению указанных систем.

Концепцией также предусмотрен достаточно обширный перечень принципов, с соблюдением которых должны достигаться поставленные цели. Приведем некоторые из них:

- стимулирование развития технологий ИИ и робототехники регуляторными средствами;
- обеспечение баланса интересов разработчиков, потребителей и иных лиц в сфере ИИ и робототехники;
- саморегулирование сферы разработок в области ИИ и робототехники участниками рынка;
- оценка воздействия технологий и систем ИИ и робототехники на все сферы жизни человека, общества и государства;
- технологический суверенитет, предусматривающий обеспечение необходимого уровня независимости России в области ИИ и робототехники;
- поддержка конкуренции, предусматривающая обеспечение равных для всех возможностей для применения экспериментальных правовых режимов и мер господдержки, а также для доступа к необходимым в целях разработки систем

[15] Порядок аккредитации определен Постановлением Правительства РФ от 06.11.2007 № 758 «О государственной аккредитации организаций, осуществляющих деятельность в области информационных технологий» и Приказом Минкомсвязи РФ от 03.11.2011 № 298 «Об утверждении Административного регламента предоставления Министерством связи и массовых коммуникаций Российской Федерации государственной услуги по государственной аккредитации организаций, осуществляющих деятельность в области информационных технологий».

АБ ЕМПП
17|2 Скаковая ул. | Москва, Россия
БЦ Скаковая 17| 8 ой этаж
Тел: +7 495 945-51-90
E-mail: info@empp.ru | web: www.empp.ru

ЕМПП Адвокатское Бюро

ИИ и робототехники данным из государственных и муниципальных информационных систем.

Среди этических основ развития рассматриваемой сферы следует обратить внимание на такие как:

- запрет на причинение вреда человеку по инициативе систем ИИ и робототехники;
- подконтрольность человеку;
- недопущение противоправной манипуляции поведением человека со стороны ИИ.

При общем отсутствии какой-либо конкретики в указанном документе необходимо признать, что некоторые из предложенных путей реформирования вызывают интерес, а некоторые – и настороженность.

Так, предложение по созданию экспериментальных правовых режимов или так называемых «регуляторных песочниц» prima facie представляется вполне удачным, поскольку позволяет апробировать различные новаторские решения в пределах определенной территории без изменения всей системы законодательства.

Здесь уместным выглядит пример Москвы, где с 01.07.2020 (т.е. до Концепции), был установлен экспериментальный правовой режим в целях создания необходимых условий для разработки и внедрения технологий ИИ, а также последующего возможного использования результатов применения ИИ[16]. Об этом подробнее в следующем подразделе настоящего обзора.

Другим механизмом, предложенным разработчиками Концепции, является предоставление разработчикам технологий ИИ и робототехники доступа к различного рода данным, в том числе персональным, собираемым государственными органами и медицинскими организациями. При этом персональные данные в обязательном порядке должны быть обезличены. Такое раскрытие информации, согласно Концепции, будет осуществляться в целях проведения научных исследований, обучения искусственного интеллекта и разработки технологических решений на их основе.

Не беремся оспаривать необходимость описанной меры, однако считаем, что при реализации её на практике законодателю и органам, отвечающим за технологическую сторону вопроса, следует быть крайне осторожными. Любое не в полной мере проработанное решение с их стороны может привести к глобальным утечкам данных миллионов граждан.

Среди иных предложенных направлений развития ИИ и робототехники можно отметить:

[16] Федеральный закон от 24.04.2020 № 123-ФЗ «О проведении эксперимента по установлению специального регулирования в целях создания необходимых условий для разработки и внедрения технологий искусственного интеллекта в субъекте Российской Федерации - городе федерального значения Москве и внесении изменений в статьи 6 и 10 Федерального закона «О персональных данных».

АБ ЕМПП
17|2 Скаковая ул. | Москва, Россия
БЦ Скаковая 17| 8 ой этаж
Тел: +7 495 945-51-90
E-mail: info@empp.ru | web: www.empp.ru

- совершенствование нормативно-правового регулирования гражданской ответственности за причинение вреда системами ИИ и робототехники;
- оптимизацию режима экспорта технологий ИИ и робототехники, к примеру, расширение и актуализация перечня технологий двойного назначения;
- развитие страховых институтов в сфере отношений с участием систем ИИ и робототехники, определение случаев и условий обязательного страхования ответственности за вред, причиненный применением роботов или систем ИИ и робототехники;
- обеспечение необходимого уровня безопасности систем ИИ и робототехники, к примеру, посредством интеграции «красной кнопки» и «черного ящика»;
- установление правового режима охраны прав на результаты интеллектуальной деятельности, полученные системами ИИ без творческого вклада человека.

В остальной части Концепции в принципе затруднительно выделить какие-либо предложения по развитию законодательства в сфере ИИ и робототехники, которые бы имели конкретный, прикладной характер. В связи с этим мы не будем на ней останавливаться в настоящем обзоре. Однако отметим, что у такой абстрактности документа, как говорят эксперты, есть свои причины. Заключаются они в слишком широком круге технических вопросов, которые охватывает Концепция, а также в полярности экспертных мнений.

Сама же Концепция по существу является развитием Модельной конвенции о робототехнике и ИИ 2017 г., разработанной Исследовательским центром проблем регулирования робототехники и ИИ, а также концепции закона о робототехнике, разработанной в 2016 году основателем Grishin Robotics Дмитрием Гришиным и партнером юридической фирмы Dentons Виктором Наумовым.

По мнению Д. Гришина, законы робототехники, впервые сформулированные Айзеком Азимовым в рассказе «Хоровод» (1942), применимы и при разработке нормативной базы для регулирования в рассматриваемой сфере. К примеру, принцип, согласно которому робот не может навредить человеку. В своей концепции 2016 г. Гришин предлагал частично применять в отношении роботов нормы законодательства о животных и юридических лицах, отмечая при этом, что ИИ является особой юридической конструкцией.

Наиболее существенное отличие Концепции от её предшественниц специалисты видят в достижении консенсуса между разработчиками по ряду принципиальных моментов, таких как ответственность разработчиков систем ИИ, расширение перечня открытых данных и установление принципа рыночного саморегулирования отрасли.

АБ ЕМПП
17|2 Скаковая ул. | Москва, Россия
БЦ Скаковая 17| 8 ой этаж
Тел: +7 495 945-51-90
E-mail: info@empp.ru | web: www.empp.ru

Разработка предложений по реализации Концепции возложена на Минэкономразвития, которое, как отмечается на его сайте, в настоящий момент осуществляет сбор предложений по реализации Концепции в рамках федеральных проектов национальной программы «Цифровая экономика Российской Федерации».

5.2. Экспериментальный правовой режим в Москве

Упомянутым выше Федеральным законом № 123-ФЗ экспериментальный правовой режим был установлен на территории г. Москвы на 5 лет. Целями эксперимента являются, помимо прочего, формирование комплексной системы регулирования общественных отношений, возникающих в связи с развитием и использованием технологий ИИ, а также повышение эффективности деятельности хозяйствующих субъектов.

Полномочия по определению условий и порядка разработки, создания, внедрения и технологий ИИ и использования их результатов возложены на Правительство г. Москвы. Для мониторинга экспериментального правового режима и определения направлений его совершенствования создается специальный координационный совет. Участником эксперимента может быть юридическое лицо или индивидуальный предприниматель, включенный в соответствующий реестр.

По данным сайта Мэрии г. Москвы по состоянию на ноябрь 2020 участие в эксперименте принимали почти 300 медицинских организаций, использовавшие ИИ для диагностики заболеваний.

5.3. Предустановка российского ПО на «умные» устройства

В ноябре 2020 Правительство РФ своим Постановлением № 1867 (***«Постановление № 1867»***) определило перечень видов электронных товаров, на которые распространяется требование об обязательной предустановке российского ПО. Помимо этого, нормативным актом был регламентирован порядок составления и ведения этого перечня, а также правила предустановки ПО на указанные товары (***«Правила предустановки ПО»***).

Предполагалось, что требование о предустановке будет распространяться на гаджеты, произведенные после 01.01.2021, однако, в дальнейшем Правительство решило сдвинуть этот срок на три месяца до 01.04.2021 (Распоряжение Правительства РФ от 31.12.2020 № 3704-р (***«Распоряжение № 3704-р»***).

Перечень гаджетов, на которые распространяется Постановление № 1867, соответствует проекту постановления, разработанному ФАС в феврале 2020 (о нем мы писали в предыдущем обзоре)[17]. Перечень ПО, которое подлежит установке был утвержден Распоряжением № 3704-р. В него вошли 16 программ для смартфонов и планшетов, 11 программ для смарт-телевизоров и 1

[17] Напомним, что в этот перечень вошли гаджеты с сенсорными экранами, предназначенные для бытового использования, системные блоки, стационарные и портативные компьютеры с предустановленной операционной системой, а также смарт-телевизоры.

АБ ЕМПП
17|2 Скаковая ул. | Москва, Россия
БЦ Скаковая 17| 8 ой этаж
Тел: +7 495 945-51-90
E-mail: info@empp.ru | web: www.empp.ru

программа для ПК. Большая часть приложений для смартфонов – это программы, разработанные ООО «Мэйл.ру» и ООО «Яндекс». Также применительно к смартфонам большая часть из указанных программ подлежит обязательной предустановке на гаджеты с операционными системами как Android, так и iOS.

Правила, утвержденные Постановлением № 1867, предполагают три допустимых способа предустановки ПО:

- посредством установки ПО в полном объёме на жесткий диск устройства;
- посредством размещения на экране устройства ярлыка для загрузки программы;
- посредством диалогового окна, всплывающего при первом включении устройства, с предложением загрузить ПО.

Производитель гаджета вправе сам выбрать любой из этих способов.

Сам софт и его предустановка, должны быть бесплатными для потребителя. Изготовителям гаджетов запрещено взимать дополнительную плату с правообладателей ПО за его предустановку, равно как и последним запрещено требовать того же от производителей устройств.

Если технические требования программы не соответствуют техническим характеристикам гаджета или не являются совместимыми с его операционной системой, то производитель устройства или уполномоченные им лица освобождаются от обязательной предустановки отечественного ПО (п. 10. Правил предустановки ПО).

Безусловно заслуживает отдельного внимания вопрос о том, будет ли выполнять эти описанные требования такой IT-гигант, как Apple inc. Ранее именно эта компания заявляла о том, что предустановка российского софта на производимые ею устройства невозможна. В обоснование указывалось, что Apple не сможет обеспечить корректную работу этих приложений с другим софтом в операционной системе iOS из-за закрытого характера последней. Помимо этого, указывалось, что iOS не позволяет производить бесконтактную оплату с помощь NFC-чипа через платежную систему «Мир».

На этом фоне в СМИ даже обсуждалась вероятность ухода IT-гиганта с российского рынка, в случае если описанные выше требования вступят в силу. Вероятно, проблему с MirPay решить так и не удалось, поскольку в Распоряжении № 3704-р приложение предписано предустанавливать только на Android.

В случае же с остальными программами не исключено, что Apple воспользуется оговоркой п. 10 Правил предустановки ПО, чтобы не исполнять требования Правительства. В частности, такое мнение

АБ ЕМПП
17|2 Скаковая ул. | Москва, Россия
БЦ Скаковая 17| 8 ой этаж
Тел: +7 495 945-51-90
E-mail: info@empp.ru | web: www.empp.ru

высказывает информационный портал Appleinsider.ru[18]. Позволим себе предположить, что некоторые из производителей смартфонов на Android также попытаются использовать эту возможность.

В отношении же двух остальных категорий гаджетов, на которые предписано устанавливать отечественные программы, существенных проблем не усматривается в принципе. Многие из сервисов для смарт-телевизоров, указанные в Распоряжении № 3704-р, уже давно устанавливаются на них производителями, а программа «Мой Офис», предназначенная для инсталляции в ПК, как представляется, окажет лишь положительное воздействие на процесс эксплуатации устройств и создаст благоприятные условия для развития отечественного аналога Microsoft Office.

5.4. Регистрация доменных имён через портал Госуслуг

В октябре 2020 «Коммерсантъ» сообщал ещё об одной инициативе Минцифры: осуществлять идентификацию администраторов доменных имен в зоне «.ru» и «.рф» через Единую систему идентификации и аутентификации (***«ЕСИА»***), используемую на портале госуслуг.

Вопрос был предложен для обсуждения на заседании президиума Правительственной комиссии по цифровому развитию, использованию информационных технологий для улучшения качества жизни и условий ведения предпринимательской деятельности, однако на данный момент каких-либо сведений о результатах его рассмотрения в открытом доступе нет. Тем не менее, считаем возможным осветить новость в настоящем обзоре, чтобы подготовить читателей на случай, если инициатива всё-таки получит развитие.

Технически для реализации задуманного предлагается подключить к ЕСИА регистраторов доменных имен, аккредитованных в Координационном центре национального доменов «.ru» и «.рф». Лейтмотивом такой инициативы стала борьба с участившимися в период пандемии случаями мошенничества в Интернете.

Предполагается, что при новой системе идентификации регистратор доменного имени, а что важнее, и правоохранительные органы смогут получать информацию об администраторе сайта гораздо быстрее, без направления дополнительных запросов.

Однако у экспертов инициатива вызывает ряд сомнений.

Во-первых, для доступа к такой информации в ЕСИА регистраторам доменов будет необходимо получить соответствующую лицензию.

Во-вторых, пока неизвестно, возможно ли будет зарегистрировать сайт с любого аккаунта на госуслугах (в том числе с неподтвержденными данными) или только через

[18] URL: https://appleinsider.ru/sudy-i-skandaly/apple-razreshili-ne-ustanavlivat-rossijskij-soft-na-iphone-v-poryadke-isklyucheniya.html

АБ ЕМПП
17|2 Скаковая ул. | Москва, Россия
БЦ Скаковая 17| 8 ой этаж
Тел: +7 495 945-51-90
E-mail: info@empp.ru | web: www.empp.ru

верифицированную учетную запись. В первом случае предложенные Минцифры меры теряют всякий смысл.

В-третьих, правоохранительные органы и сейчас не имеют проблем с получением сведений об администраторах доменов. По сути, изменится лишь то, что необходимую информацию они смогут получать без обращения к регистратору доменного имени, который будет освобожден от обязанности хранить её.

В-четвертых, добиться повышения информационной безопасности с помощью описанной меры будет возможно, только если привязка к ЕСИА станет обязательной. Это потребует кардинального пересмотра всей системы регистрации доменов, о чем на данный момент речи не идет.

* * *

КОНТАКТНАЯ ИНФОРМАЦИЯ

Мерген Дораев
Партнер
doraev@empp.ru

Петр Шевцов
Партнер
shevtsov@empp.ru

Леонид Мисник
Юрист
misnik@empp.ru