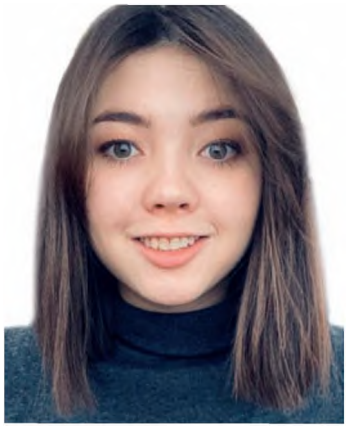
Обзор изменений в законодательстве

ФСТЭК и ФСБ России с 1 сентября начнут штрафовать за нарушение обеспечения безопасности КИИ

Анастасия Заведенская, *аналитик Аналитического центра Уральского центра систем безопасности*



Май-2021

В мае 2021 г. ФСТЭК России сообщила об изменении процедур аттестации объектов информатизации, обрабатывающих информацию, составляющую государственную тайну. Официально опубликованы изменения в КоАП РФ, вносящие штрафные санкции за нарушение обеспечения безопасности КИИ, и приказы ФСБ России, касающиеся обращения с электронной подписью. Изменены сроки реализации требований, в том числе по защите информации, для систем оформления воздушных перевозок.

Аттестация объектов информатизации

Информационным сообщением от 29 апреля 2021 г. № 240/24/2087 ФСТЭК России сообщает об утверждении Порядка организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации, содержащей сведения, составляющие государственную тайну[1] (далее – Порядок аттестации). В этом информационном письме отмечается, что Порядок аттестации был утвержден приказом ФСТЭК России от 28 сентября 2020 г. № 110.

Порядок аттестации вступает в силу с 1 июня 2021 г. и отменяет действие следующих документов при организации и проведении работ по аттестации объектов информатизации, обрабатывающих информацию, содержащую сведения, составляющие государственную тайну:

- Положение по аттестации объектов информатизации по требованиям безопасности информации, утвержденное председателем Гостехкомиссии России 25 ноября 1994 г.;
- Типовое положение об органе по аттестации объектов информатизации по требованиям безопасности информации, утвержденное председателем Гостехкомиссии России 5 января 1996 г. № 3;
- ГОСТ Р 58189–2018 Защита информации. Требования к органам по аттестации объектов информатизации;
- ГОСТ РО 0043-003–2012 Защита информации. Аттестация объектов информатизации. Общие положения.

С целью организации контроля за выполнением работ по аттестации объектов информатизации Порядком аттестации предусмотрено ведение ФСТЭК России единого реестра аттестованных объектов информатизации, а также представление организациями, проводившими аттестацию, материалов с результатами аттестационных испытаний каждого объекта информатизации в территориальные органы ФСТЭК России. В случае установления по результатам экспертизы указанных материалов факта несоответствия аттестованного объекта информатизации требованиям о защите информации действие аттестата соответствия может быть приостановлено до устранения выявленного несоответствия объекта информатизации установленным требованиям.

Перечень органов по аттестации и органов государственной власти, имеющих право проведения работ по аттестации объектов информатизации в соответствии с приказом ФСТЭК России от 28 сентября 2020 г. № 110, размещен на официальном сайте ФСТЭК России[2].

КоАП и КИИ

Федеральный закон от 26.05.2021 г. № 141-ФЗ "О внесении изменений в Кодекс Российской Федерации об административных правонарушениях"[3] (далее – Федеральный закон) был официально опубликован 26 мая 2021 г.

Федеральный закон вступил в силу с 6 июня 2021 г., за исключением п.1 ст. 13.12 об ответственности за нарушение требований к созданию систем безопасности значимых объектов КИИ, он вступит в силу с 1 сентября 2021 г. (см. табл. 1).

В рамках Федерального закона предлагается наделить ФСТЭК России и ФСБ России полномочиями по рассмотрению дел об административных правонарушениях.

Краткая сводка статей за нарушение обеспечения безопасности КИИ, вносимых в КоАП РФ, представлена в таблице ниже.

Электронная подпись

На официальном интернет-портале правовой информации в мае 2021 г. были опубликованы приказы ФСБ России, устанавливающие требования к использованию электронной подписи:

- приказ ФСБ России от 13.04.2021 г. № 142 "О внесении изменения в приказ ФСБ России от 27 декабря 2011 г. № 796 "Об утверждении Требований к средствам электронной подписи и Требований к средствам удостоверяющего центра"[4] (далее – приказ ФСБ России № 142);

[1] *https://fstec.ru/normotvorcheskaya/informatsionnye-i-analiticheskie-materialy/2220-informatsionnoe-soobshchenie-fstek-rossii-ot-29-aprelya-2021-g-n-240-24-2087*

[2] *https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty-po-sertifikatsii/153-sistema-sertifikatsii/590-perechen-organov-po-attestatsii-n-ross-ru-0001-01bi00*

[3] *http://publication.pravo.gov.ru/Document/View/0001202105260038*

[4] *http://publication.pravo.gov.ru/Document/View/0001202105200019*

Таблица 1

Правонарушитель	Административный штраф	Полномочный орган исполнительной власти	Административное правонарушение
Должностное лицо	От 10 тыс. до 50 тыс. руб.	ФСТЭК России	Нарушение требований к созданию систем безопасности значимых объектов КИИ и обеспечению их функционирования либо требований по обеспечению безопасности значимых объектов КИИ, если такие действия (бездействие) не содержат уголовно наказуемого деяния Непредставление или нарушение сроков представления во ФСТЭК России сведений о результатах категорирования объектов КИИ
		ФСБ России	Нарушение порядка информирования о компьютерных инцидентах, реагирования на них, принятия мер по ликвидации последствий компьютерных атак, проведенных в отношении значимых объектов КИИ Непредставление или нарушение порядка либо сроков представления информации, предусмотренной законодательством в области обеспечения безопасности КИИ, в ГосСОПКА
	От 20 тыс. до 50 тыс. руб.	ФСБ России	Нарушение порядка обмена информацией о компьютерных инцидентах между субъектами КИИ, между субъектами КИИ и уполномоченными органами иностранных государств, международными организациями, международными неправительственными и иностранными организациями, осуществляющими деятельность в области реагирования на компьютерные инциденты
Юридическое лицо	От 50 тыс. до 100 тыс. руб.	ФСТЭК России	Нарушение требований к созданию систем безопасности значимых объектов КИИ и обеспечению их функционирования либо требований по обеспечению безопасности значимых объектов КИИ, если такие действия (бездействие) не содержат уголовно наказуемого деяния Непредставление или нарушение сроков представления во ФСТЭК России сведений о результатах категорирования объектов КИИ
	От 100 тыс. до 500 тыс. руб.	ФСБ России	Нарушение порядка информирования о компьютерных инцидентах, реагирования на них, принятия мер по ликвидации последствий компьютерных атак, проведенных в отношении значимых объектов КИИ Нарушение порядка обмена информацией о компьютерных инцидентах между субъектами КИИ, между субъектами КИИ и уполномоченными органами иностранных государств, международными организациями, международными неправительственными и иностранными организациями, осуществляющими деятельность в области реагирования на компьютерные инциденты Непредставление или нарушение порядка либо сроков представления информации, предусмотренной законодательством в области обеспечения безопасности КИИ, в ГосСОПКА

● приказ ФСБ России от 13.04.2021 г. № 143 "О внесении изменения в пункт 2 приказа ФСБ России от 4 декабря 2020 г. № 554 "Об утверждении Порядка уничтожения ключей электронной подписи, хранимых аккредитованным удостоверяющим центром по поручению владельцев квалифицированных сертификатов электронной подписи"[5] (далее – приказ ФСБ России № 143);

● приказ ФСБ России от 13.04.2021 г. № 144 "О внесении изменения в пункт 2 приказа ФСБ России от 4 декабря 2020 г. № 556 "Об утверждении Требований к средствам доверенной третьей стороны, включая требования к используемым доверенной третьей стороной средствам электронной подписи"[6] (далее – приказ ФСБ России № 144);

● приказ ФСБ России от 20.04.2021 г. № 154 "Об утверждении Правил под-

[5] *http://publication.pravo.gov.ru/Document/View/0001202105200017*
[6] *http://publication.pravo.gov.ru/Document/View/0001202105200024*

тверждения владения ключом электронной подписи"[7] (далее – приказ ФСБ России № 154);

- приказы ФСБ России № 142, № 143, № 144 ограничивают действия приказов, в которые они, соответственно, вносят изменения до 1 января 2027 г.

Приказ ФСБ России № 154 вступает в силу с 1 марта 2022 г. и действует до 1 марта 2028 г., регламентирует порядок проверки удостоверяющим центром соответствия ключа электронной подписи (далее – ЭП) ключу проверки ЭП, указанному лицом в заявлении на получение сертификата ключа проверки ЭП. Правила не распространяется на случаи, когда ключевая пара была создана удостоверяющим центром.

Автоматизированные информационные системы оформления воздушных перевозок

Постановление Правительства Российской Федерации от 30.04.2021 г. № 685 "О внесении изменения в постановление Правительства Российской Федерации от 24 июля 2019 г. № 955"[8] (далее – ПП РФ № 685) было опубликовано 6 мая 2021 г.

Постановлением Правительства РФ от 24 июля 2019 г. № 955 были утверждены требования к автоматизированным информационным системам оформления воздушных перевозок (далее – АИС ОВП), к базам данных, входящим в их состав, к информационно-телекоммуникационным сетям, обеспечивающим работу указанных автоматизированных информационных систем, к их оператору, а также меры по защите информации, содержащейся в них, и порядку их функционирования. Постановление должно было вступить в силу с 31 октября 2021 г., однако ПП РФ № 685 сдвинуло срок до 30 октября 2022 г.

Напомним, что основной акцент в контексте информационной безопасности постановление Правительства РФ от 24 июля 2019 г. № 955 делает на защите обрабатываемых персональных данных[9] (далее – ПДн) пассажиров и персонала (экипажа) транспортных средств:

1. При оформлении внутренних воздушных перевозок базы данных (далее – БД) и серверы, входящие в состав АИС ОВП, должны располагаться на территории РФ. Хотя допускается использование БД и серверов, расположенных вне территории РФ, но только при условии исключения обработки в них ПДн пассажиров, осуществляющих внутренний перелет.
2. Операторам и пользователям АИС ОВП необходимо контролировать соответствие трансграничной передачи ПДн пассажиров требованиям законодательства РФ и порядку, установленному договором между операторами и пользователями.
3. При передаче данных по общедоступным каналам связи обязательно применение сертифицированных средств криптографической защиты информации.

Июнь-2021

В июне 2021 г. регуляторы вели активную нормотворческую деятельность. В продолжение обзора изменений законодательства рассмотрим регламентацию защиты средств дистанционной работы, новые процедуры контрольно-надзорной деятельности по обработке персональных данных, требования к защите информации в финансовом секторе, штрафные санкции за разглашение информации ограниченного доступа и многое другое.

ФСТЭК России. Средства безопасной дистанционной работы

Информационным сообщением от 23 июня 2021 г. № 240/24/3057 ФСТЭК России сообщает об утверждении Требований по безопасности информации к средствам обеспечения безопасной дистанционной работы в информационных (автоматизированных) системах[10] (далее – Требования). Требования утверждены приказом ФСТЭК России от 16 февраля 2021 г. № 32.

К средствам обеспечения безопасной дистанционной работы в информационных системах (ИС)/автоматизированных системах (АС) (далее – средства дистанционной работы) относятся средства защиты информации, использующие средства вычислительной техники, не входящие в состав указанных ИС/АС. Средства дистанционной работы не имеют дифференциации и должны использовать единообразную конфигурацию вне зависимости от категории значимости объектов критической информационной инфраструктуры (далее – КИИ), класса государственных информационных систем, класса защищенности автоматизированных систем управления производственными и/или технологическими процессами, уровня защищенности информационных систем персональных данных (далее – ПДн).

Субъекты КИИ в сфере здравоохранения

Информационным сообщением от 18 июня 2021 г. N 240/82/1037 ФСТЭК России[11] рекомендует порядок представления субъектами КИИ, осуществляющими деятельность в сфере здравоохранения, перечней объектов КИИ, подлежащих категорированию (далее – перечни), сведений о результатах присвоения объектам КИИ одной из категорий значимости либо об отсутствии необходимости присвоения им одной из таких категорий (далее – сведения).

Согласно информационному письму рассмотрение перечней и сведений осуществляется центральным аппаратом ФСТЭК России для субъектов КИИ, являющихся федеральными органами исполнительной власти, а также федеральными учреждениями здравоохранения. Управления ФСТЭК России по федеральному округу, на территории которых расположены соответствующие субъекты КИИ, осуществляют рассмотрение документов субъектов КИИ, являющихся органами власти субъектов РФ, учреждениями здравоохранения, подведомственными органам власти субъектов РФ, а также самостоятельными юридическими лицами.

[7] *http://publication.pravo.gov.ru/Document/View/0001202105310030*
[8] *http://publication.pravo.gov.ru/Document/View/0001202105060001*
[9] *https://www.ussc.ru/news/novosti/obzor-izmeneniy-v-zakonodatelstve-za-avgust-2019/*
[10] *https://fstec.ru/normotvorcheskaya/informatsionnye-i-analiticheskie-materialy/2243-informatsionnoe-soobshchenie-fstek-rossii-ot-23-iyunya-2021-g-n-240-24-3057*
[11] *https://fstec.ru/tekhnicheskaya-zashchita-informatsii/obespechenie-bezopasnosti-kriticheskoj-informatsionnoj-infrastruktury/290-inye/2240-informatsionnoe-soobshchenie-fstek-rossii-ot-18-iyunya-2021-g-n-240-82-1037*

Таблица 2

Группа тяжести	Признаки отнесения к группе тяжести	Группа вероятности	Признаки отнесения к группе вероятности
А	Обработка специальной категории ПДн и/или биометрических ПДн Сбор ПДн, в том числе в сети "Интернет", осуществляемый с использованием баз данных, находящихся за пределами РФ Трансграничная передача ПДн на территорию иностранных государств, не являющихся сторонами Конвенции Совета Европы о защите физических лиц при автоматизированной обработке ПДн и не включенных в перечень иностранных государств, не являющихся сторонами Конвенции Совета Европы о защите физических лиц при автоматизированной обработке ПД и обеспечивающих адекватную защиту прав субъектов ПДн Передача третьим лицам ПДн, полученных в результате обезличивания с использованием методов обезличивания, утвержденных в соответствии с законодательством РФ в области ПДн	1	Деятельность контролируемых лиц осуществляется с нарушениями требований законодательства РФ в области ПДн, ответственность за которые предусмотрена частями 1.1, 2.1, 5.1, 9 ст. 13.11 КоАП РФ
Б	Обработка ПДн в целях, отличных от заявленных целей обработки ПДн на этапе их сбора Обработка ПДн несовершеннолетних лиц в случаях, не предусмотренных федеральными законами Обработка ПДн в ИСПДн, содержащих ПДн более чем 20 тыс. субъектов ПДн в пределах субъекта РФ или РФ в целом Сбор ПДн, в том числе в сети "Интернет", осуществляемый с использованием иностранных программ и сервисов	2	Деятельность контролируемых лиц осуществляется с нарушениями требований законодательства РФ в области ПДн, ответственность за которые предусмотрена частями 1, 2, 5, 6, 8 ст. 13.11 КоАП РФ
В	Обработка ПДн близких родственников субъекта ПДн Обработка ПДн в ИСПДн, содержащих ПДн от 1 тыс. до 20 тыс. субъектов ПДн Трансграничная передача ПДн на территорию иностранных государств, не являющихся сторонами Конвенции Совета Европы о защите физических лиц при автоматизированной обработке ПДн и включенных в перечень иностранных государств, не являющихся сторонами Конвенции Совета Европы о защите физических лиц при автоматизированной обработке ПДн и обеспечивающих адекватную защиту прав субъектов ПДн Обезличивание ПДн, обработка ПДн, полученных в результате обезличивания, с использованием методов обезличивания, утвержденных в соответствии с законодательством РФ в области ПДн, без передачи третьим лицам	3	Деятельность контролируемых лиц осуществляется с нарушениями требований законодательства РФ в области ПДн, ответственность за которые предусмотрена частями 4, 7 ст. 13.11 КоАП РФ
Г	Обработка ПДн в ИСПДн, содержащих ПДн менее чем 1 тыс. субъектов ПДн Обработка ПДн без предоставления в Роскомнадзор информации уведомительного характера, предоставление которой предусмотрено ФЗ № 152 Обработка ПДн, полученных из общедоступных источников ПДн Трансграничная передача ПДн на территорию иностранных государств, являющихся сторонами Конвенции Совета Европы о защите физических лиц при автоматизированной обработке ПДн	4	Отсутствие обстоятельств, указанных в группах вероятности 1–3

Государственные информационные системы

Постановление Правительства Российской Федерации от 31.05.2021 г. № 837 "О внесении изменения в требования к порядку создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации государственных информационных систем и дальнейшего хранения содержащейся в их базах данных информации"[12] (далее – ПП РФ № 837) официально опубликовано 1 июня 2021 г.

ПП РФ № 837 увеличивает срок рассмотрения Минцифры России, ФСБ России и ФСТЭК России технических заданий на создание государственных информационных систем, а также срок рассмотрения ФСБ России и ФСТЭК России моделей угроз безопасности информации с 10 до 20 рабочих дней.

Персональные данные. Государственный контроль (надзор)

Постановление Правительства Российской Федерации от 29.06.2021 г. № 1046 "О федеральном государственном контроле (надзоре) за обработкой персональных данных"[13] (далее – ПП РФ № 1046) официально опубликовано 30 июня 2021 г.

ПП РФ № 1046 вступает в силу с 1 июля 2021 г. и утверждает положение, устанавливающее порядок организации и осуществления государственного контроля (надзора) за обработкой ПДн. Как и ранее, реализация полномочий контрольно-надзорного органа осуществляется Роскомнадзором. Ранее действующее постановление Правительства Российской Федерации от 13 февраля 2019 г. № 146 "Об утверждении Правил организации и осуществления государственного контроля и надзора за обработкой персональных данных" признано утратившим силу.

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

- инспекционный визит;
- документарная проверка;
- выездная проверка.

При этом согласно ПП РФ № 1046 Роскомнадзор может осуществлять мероприятия по контролю без взаимодействия с контролируемым лицом в целях предупреждения, выявления, прогнозирования и пресечения нарушения требований.

Для осуществления контроля (надзора) за обработкой вводится система оценки и управления рисками (см. табл. 2). При

[12] http://publication.pravo.gov.ru/Document/View/0001202106010044
[13] http://publication.pravo.gov.ru/Document/View/0001202106300053

осуществлении контроля (надзора) поднадзорные объекты классифицируются по одной из следующих категорий риска причинения вреда (ущерба) (далее – категории риска):

- высокий риск;
- значительный риск;
- средний риск;
- умеренный риск;
- низкий риск.

Единая биометрическая система

ФСБ России представила для общественного обсуждения проект постановления Правительства Российской Федерации "О порядке осуществления федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации, контроля и надзора за выполнением органами, организациями, индивидуальными предпринимателями, нотариусами, указанными в части 18.2 статьи 14.1 Федерального закона от 27 июля 2006 г. № 149-ФЗ, организационных и технических мер по обеспечению безопасности персональных данных с использованием средств защиты информации, указанных в части 18.3 статьи 14.1 Федерального закона от 27 июля 2006 г. № 149-ФЗ"[14] (далее – проект ПП РФ). Общественные обсуждения пройдут до 15 июля 2021 г.

Проект ПП РФ направлен на определение порядка осуществления ФСБ России и ФСТЭК России мероприятий по контролю за выполнением организационных и технических мер по обеспечению безопасности ПДн и использованием СрЗИ в единой биометрической системе (ЕБС). Контроль проводится в целях проверки соблюдения государственными органами, органами местного самоуправления, организациями, индивидуальными предпринимателями и нотариусами требований по обеспечению безопасности ПДн.

Согласие на обработку ПДн, разрешенных субъектом ПДн для распространения

В конце июня 2021 г. на сайте Роскомнадзора опубликована информация о действии с 1 июля 2021 г. сервиса для операторов ПДн[15], позволяющего оператору ПДн подготовить шаблон формы согласия на обработку ПДн, разрешенных субъектом ПДн для распространения, с учетом профессиональной специфики деятельности оператора.

Сформированный шаблон формы согласия оператор по желанию может направить в Роскомнадзор для получения рекомендаций по формированию такого согласия. Полученные рекомендации Роскомнадзора можно учесть при использовании указанного шаблона для непосредственного получения согласия от субъекта ПДн в соответствии с п.1 ч.6 ст.10.1 ФЗ № 152.

Напомним, что с 1 сентября 2021 г. для операторов вступают в силу обязательные требования к форме согласия на обработку ПДн, разрешенных для распространения. Обязанность операторов получать отдельное согласие гражданина на распространение его ПДн установлена Федеральным законом от 30 декабря 2020 г. № 519-ФЗ "О внесении изменений в Федеральный закон "О персональных данных", который вступил в силу 1 марта 2021 г.

Электронная подпись (ЭП)

Приказ ФСБ России от 01.05.2021 № 171 "Об утверждении организационно-технических требований в области информационной безопасности к доверенным лицам удостоверяющего центра федерального органа исполнительной власти, уполномоченного на осуществление государственной регистрации юридических лиц"[16] (далее – приказ ФСБ России № 171) официально опубликован 1 июня 2021 г. Приказ ФСБ России № 171 вступает в силу с 1 марта 2022 г. и действует до 1 марта 2028 г.

Ниже приведем несколько требований по информационной безопасности к доверенным лицам согласно приказу ФСБ России № 171:

- обеспечение контролируемой зоны в зданиях и помещениях, предназначенных для размещения технических средств, обеспечивающих выполнение доверенным лицом своих функций;
- организация и ведение учета машинных носителей информации, используемых средствами криптографической защиты информации (далее – СКЗИ), включая средства ЭП, а также обеспечение их защиты от несанкционированного доступа;
- соблюдение требований эксплуатационной документации на используемые СКЗИ, включая средства ЭП;
- применение для выполнения возложенных на доверенное лицо функций ИС, аттестованных на соответствие Требованиям о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденным приказом ФСТЭК России от 11 февраля 2013 г. № 17;
- разработка, введение и утверждение локальных актов, регламентирующих меры реализации требований по информационной безопасности.

Банк России. Кредитные организации

В июне 2021 г. Банк России опубликовал проект указания "О внесении изменений в положение Банка России от 17 апреля 2019 года № 683-П "Об установлении обязательных для кредитных организаций требований к обеспечению защиты информации при осуществлении банковской деятельности в целях противодействия осуществлению переводов денежных средств без согласия клиента" (683-П)"[17] (далее – указание). Предполагается, что изменения, вносимые указанием в 683-П, должны будут вступить в силу с 1 апреля 2022 г.

Приведем несколько основных пунктов изменений 683-П, предлагаемых указанием:

1. Требования по сертификации программного обеспечения (далее – ПО) по требованиям ФСТЭК России уточнены и унифицированы с положением Банка России от 4 июня 2020 г. № 719 "О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств".

2. Усилены требования по оценке соответствия прикладного ПО, также зафиксирована возможность для кредитных организаций самостоятельно выбирать, как провести оценку соответствия прикладного ПО – самостоятельно или с привлечением лицензиатов ФСТЭК России по технической защите конфиденциальной информации.

3. Уточнены требования по идентификации устройств клиентов, в том числе при организации удаленного доступа, а также требования по мониторингу поведения клиентов, осуществляющих операции с мобильных устройств.

4. Уточнено, что кредитные организации должны осуществлять информирование Банка России не только о выявленных инцидентах защиты информации, но и о предпринятых мерах реагирования на инцидент.

Некредитные финансовые организации

Положение Банка России от 20 апреля 2021 г. № 757-П "Об установлении обязательных для некредитных финансовых организаций требований к обеспечению защиты информации при осуществлении деятельности в сфере финансовых рынков в целях противодействия осу-

[14] *https://regulation.gov.ru/projects#npa=117301*
[15] *https://regulation.gov.ru/Projects/List#npa=116536*
[16] *http://publication.pravo.gov.ru/Document/View/0001202106010058*
[17] *https://regulation.gov.ru/projects#npa=116751*