Обзор нормативных правовых актов в сфере информационной безопасности и цифровой экономики по итогам 2021 года

© Экспертно-Аналитический центр InfoWatch. 2022 г.

Оглавление

Аннотация ... 3
Области исследования ... 3
Источники информации ... 4
Принятые нормативные правовые акты ... 4
Цифровая экономика ... 8
Информационная безопасность ... 21
Импортозамещение ... 26
Другие нормативные правовые акты ... 30
Проекты нормативных правовых актов ... 33
Цифровая экономика ... 38
Информационная безопасность ... 41
Импортозамещение ... 43
Другие проекты нормативных правовых актов ... 46
Выводы ... 49
Мониторинг утечек на сайте InfoWatch ... 51

Аннотация

Экспертно-аналитический центр группы компаний InfoWatch представляет отчет о нормативных правовых актах в сфере информационной безопасности и цифровой экономики по итогам 2021 года. Исследование охватывает проекты и принятые нормативные правовые акты, касающиеся информационной безопасности, средств защиты информации, обработки персональных данных, импортозамещения в сфере ИТ, цифровой экономики в целом.

За 2021 год нами было исследовано более 10 000 нормативных правовых актов и их проектов, и выбрано более 500 актов, относящихся к исследуемым направлениям, в том числе 287 из них - принятых. В данном отчете мы постарались охватить все вышеперечисленные темы, однако внимание акцентировали именно на аспектах обеспечения информационной безопасности в рамках тех или иных инициатив и подробнее рассмотрели несколько, на наш взгляд, ключевых документов, вышедших за год.

Области исследования

Нормативные правовые акты и их проекты федерального уровня Российской Федерации по направлениям и с точки зрения информационной безопасности (ИБ):

- Цифровая экономика.
- Национальная безопасность (стратегия и основы государственной политики).
- Импортозамещение.
- Биометрия и персональные данные.
- Информационная безопасность (защита информации, техническая защита информации), без учета актов и проектов о безопасности критической информационной инфраструктуры (КИИ) и защите государственной тайны.
- Государственная тайна (перечни сведений, поправки в законодательство и т.д.).
- Безопасность критической информационной инфраструктуры (КИИ).
- Лицензирование деятельности по ТЗИ[1] и УНСИ[2] (конфиденциальная информация, государственная тайна).
- Аккредитация и экспертиза в сфере информационной безопасности и информационных технологий.
- Сертификация средств защиты информации (СЗИ) и средств криптографической защиты информации (СКЗИ), аттестация объектов информатизации (конфиденциальная информация и государственная тайна).

[1] Техническая защита информации
[2] Устройства для несанкционированного съёма информации

Источники информации

Для мониторинга нормативных правовых актов использовались следующие источники:

Федеральный портал проектов нормативных правовых актов: https://regulation.gov.ru/

Официальное опубликование правовых актов: http://publication.pravo.gov.ru/

Сайт Федеральной службы по техническому и экспортному контролю: https://fstec.ru/

Сайт Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации: https://digital.gov.ru

Принятые нормативные правовые акты

За 2021 год всего было **принято 287 нормативных правовых актов** в области информационной безопасности, средств защиты информации, обработки персональных данных, импортозамещения в сфере ИТ и цифровой экономики в целом.

Разбивку по месяцам можно увидеть в таблице ниже.

Таблица 1. Количество принятых нормативных правовых актов

Итоги:	
I квартал 2021	28
II квартал 2021	57
III квартал 2021	91
IV квартал 2021	111
Итого принятых НПА[3] за 2021	**287**

Как видно из таблицы выше, нормотворческая активность в течение года шла по нарастающей, и самый активный период пришелся на **4 квартал 2021 года** — было принято 111 нормативных правовых актов, что составляет почти **40% от общего объема принятых актов**.

Далее рассмотрим подробнее структуру принятых нормативных правовых актов в разрезе их тем:

Таблица 2. Принятые нормативные правовые акты в области информационной безопасности и цифровой экономики, по темам

Тема нормативного правового акта	**Количество принятых актов**	**Доля от общего количества, %**
Цифровая экономика	129	45%
Биометрия и персональные данные	51	18%
Информационная безопасность (ЗИ, ТЗИ)	45	16%
Импортозамещение	18	6%
Национальная безопасность	10	3%

[3] Нормативные правовые акты

Тема нормативного правового акта	Количество принятых актов	Доля от общего количества, %
Безопасность КИИ	9	3%
Лицензирование деятельности по ТЗИ и УНСИ	9	3%
Государственная тайна	8	3%
Сертификация СЗИ и СКЗИ, аттестация объектов информатизации	6	2%
Аккредитация и экспертиза в сфере ИБ и ИТ	2	1%
Общий итог	**287**	**100%**

На рисунке ниже можно наглядно увидеть распределение по темам принятых нормативных правовых актов.

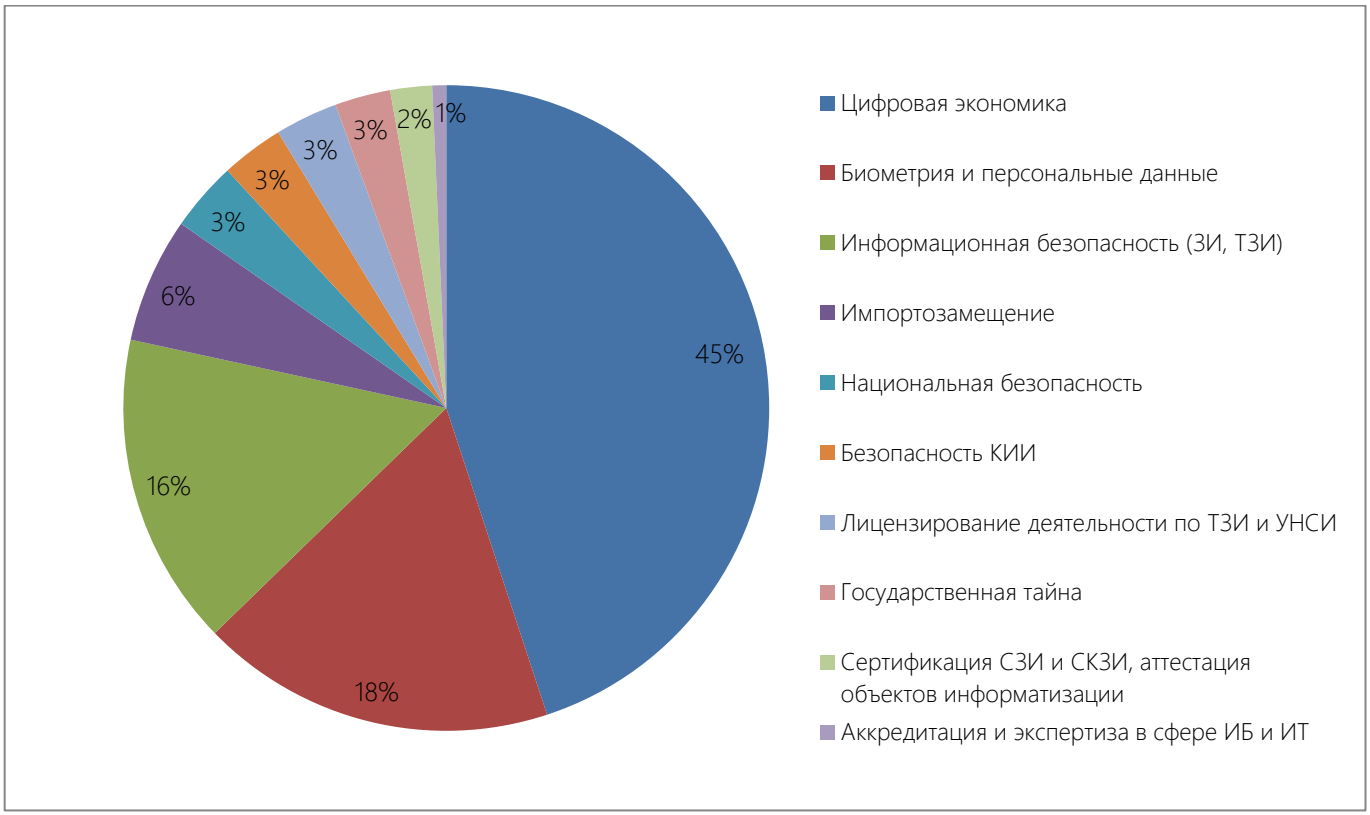

Рисунок 1. Принятые нормативные правовые акты в области информационной безопасности и цифровой экономики, по темам

Как видно из таблицы и рисунка выше, почти половина принятых нормативных правовых актов касается цифровой экономики – **45% (129 актов)** от общего числа принятых в исследуемой области. Следующее место по количеству принятых актов заняла тема биометрии и персональных данных – на ее долю пришлось **18% (51 акт)** всех принятых в сфере актов. Третье место с долей **16% (45 актов)** заняла тема информационной безопасности (защиты информации, технической защиты информации).

В области **импортозамещения** и **безопасности критической информационной инфраструктуры** количество принятых нормативных правовых актов составило **6% и 3%** соответственно.

В разрезе по ведомствам, принявшим нормативные правовые акты, картина складывается следующим образом (Таблица 3):

Таблица 3. Принятые нормативные правовые акты в области информационной безопасности и цифровой экономики по ведомствам

Министерство/ведомство	Количество актов, выпущенных ведомством	Доля от общего количества, %
Правительство РФ	186	65%
Минцифры России	31	11%
Президент РФ	22	8%
ФСТЭК России	16	6%
Роскомнадзор	13	5%
ФСБ России	12	4%
Другие	7	1%
Общий итог	**287**	100%

Наглядно также представлено на рисунке ниже:

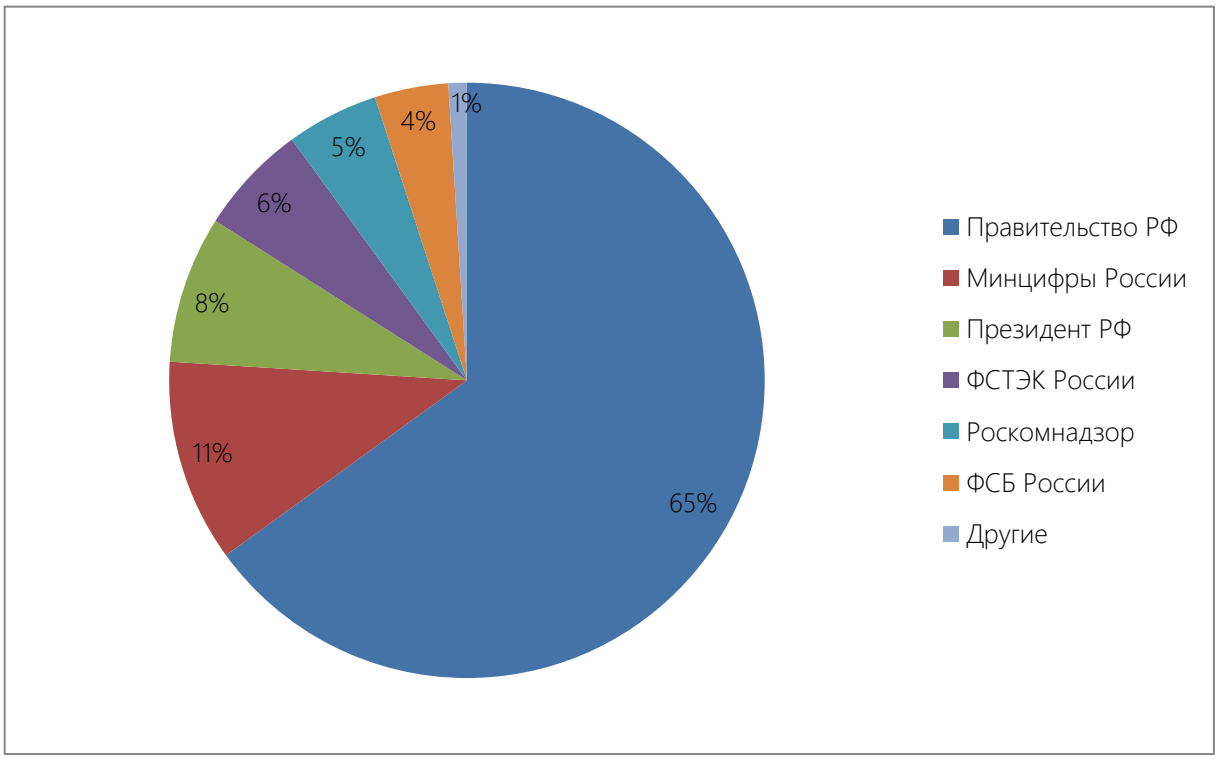

Рисунок 2. Принятые нормативные правовые акты в области информационной безопасности и цифровой экономики по ведомствам

Большинство всех принятых нормативных правовых актов принадлежит Правительству Российской Федерации – его доля по итогам года составила **65%** (по итогам 3 квартала доля составляла порядка 50%) от всех принятых актов, им было выпущено 186 актов. На долю Минцифры России пришлось **11%** от общего объема принятых актов, третье место с долей **8%** занял Президент РФ. ФСТЭК России выпустила **6%** актов, и **5%** - Роскомнадзор.

Таблица 4

Тема нормативного правового акта и принявший его орган	Доля от общего количества принятых актов, %
Цифровая экономика	**45%**
Правительство РФ	38%
Минцифры России	3%
Президент РФ	2%
Роскомнадзор	1%
Минспорт России	1%
Биометрия и персональные данные	**18%**
Правительство РФ	8%
Минцифры России	5%
Роскомнадзор	2%
ФСБ России	1%
Президент РФ	1%
Другие	1%
Информационная безопасность (ЗИ, ТЗИ)	**16%**
Правительство РФ	8%
Роскомнадзор	2%
ФСТЭК России	2%
Президент РФ	2%
Минцифры России	1%
ФСБ России	1%
Импортозамещение	**6%**
Правительство РФ	6%
Минцифры России	1%
Национальная безопасность	**3%**
Правительство РФ	2%
Президент РФ	1%
Безопасность КИИ	**3%**
ФСТЭК России	2%
Правительство РФ	1%
Лицензирование деятельности по ТЗИ и УНСИ	**3%**
Правительство РФ	1%
ФСБ России	1%
Другие	1%
Государственная тайна	**3%**
Правительство РФ	1%
Президент РФ	1%
ФСБ России	1%
Сертификация СЗИ и СКЗИ, аттестация объектов информатизации	**2%**
ФСТЭК России	2%

Тема нормативного правового акта и принявший его орган	Доля от общего количества принятых актов, %
Аккредитация и экспертиза в сфере ИБ и ИТ	**1%**
Правительство РФ	1%
Общий итог	100%

Как видно из таблицы выше, почти во всех категориях лидирует Правительство РФ – это области цифровой экономики, информационной безопасности, биометрии и персональных данных, а также нормативные правовые акты в области импортозамещения, национальной безопасности, аккредитации и экспертизы.

Однако стоит заметить, что инициаторами нормативных правовых актов, которые подписывают Президент РФ и Правительство РФ, могут быть другие министерства и ведомства, поэтому количество принятых ими актов не в полной мере отражает их активность, более показательна картина по ведомствам, внесшим проекты на обсуждение. Это мы рассмотрим подробнее в следующем разделе.

Для более детального рассмотрения было выбрано несколько тем, по которым приняты нормативные правовые акты в 2021 году — это цифровая экономика, информационная безопасность и импортозамещение.

Цифровая экономика

По данному направлению за 2021 год принято 129 нормативных правовых актов (45% от общего количества принятых документов). Далее рассмотрены некоторые акты или группы актов с точки зрения наличия в них мер и требований по обеспечению информационной безопасности, поскольку с повышением уровня цифровизации отраслей и появлением новых цифровых платформ, появляются и новые объекты защиты. Ярким примером является Единая биометрическая система, которая в конце 2021 года получила статус государственной.

Единый регистр населения

В 2023 году[4] в России заработает федеральный регистр сведений о населении (ЕРН), который из множества ведомств объединит в себе данные о гражданах РФ: Ф.И.О., дату, и место рождения, СНИЛС, ИНН, гражданство и семейное положение. Вести ресурс будет Федеральная налоговая служба (ФНС) на основании имеющихся у нее данных, а также данных, поступающих из МВД России, Минобороны России, Минобрнауки, государственных внебюджетных фондов. ФНС будет обязана обеспечить безопасность всех имеющихся в реестре сведений.

[4] Постановление Правительства Российской Федерации от 12.10.2021 № 1738 «О сроках перехода субъектов Российской Федерации и муниципальных образований на использование сведений, содержащихся в едином федеральном информационном регистре, содержащем сведения о населении Российской Федерации, в целях, определенных пунктом 3 части 2 статьи 4 Федерального закона «О едином федеральном информационном регистре, содержащем сведения о населении Российской Федерации», на переходный период» http://publication.pravo.gov.ru/Document/View/0001202110140029

Закон № 168-ФЗ «О едином федеральном информационном регистре, содержащем сведения о населении РФ»[5] был принят Государственной Думой еще в 2020 году, но в течение 2021 года продолжались публикации законодательных актов, регулирующих ЕРН, например, правила его формирования[6]

В 168-ФЗ существует раздел, посвященный обеспечению защиты сведений, содержащихся в федеральном регистре сведений о населении, включая персональные данные.

Информационная безопасность ЕРН. Сведения о населении будут находиться в центре обработки данных, «протестированном на безопасность уполномоченными на это органами» (ФСБ России, в первую очередь).

Также 9 января 2021 года было выпущено постановление Правительства Российской Федерации от 31.12.2020 № 2440 «Об утверждении Правил использования **усиленной квалифицированной электронной подписи** при формировании и ведении единого федерального информационного регистра, содержащего сведения о населении Российской Федерации»[7].

Цифровая трансформация отраслей

Выпущен ряд нормативных правовых актов, утверждающих концепции и стратегические направления цифровой трансформации различных сфер и отраслей. Ниже рассмотрено, какое внимание в данных концепциях и направлениях уделено информационной безопасности.

1. Концепция цифровой и функциональной трансформации **социальной сферы, относящейся к сфере деятельности Министерства труда и социальной защиты РФ, на период до 2025 г.**[8]:

   Проектирование целевой архитектуры ландшафта информационных систем и информационно-технической инфраструктуры (ИТ-инфраструктуры) Министерства труда и социальной защиты Российской Федерации, Пенсионного фонда Российской Федерации, Фонда социального страхования Российской Федерации и федеральных учреждений медико-социальной экспертизы необходимо осуществлять **на основе принципов**, в их числе:

   - **использования импортозамещенных решений;**

[5] Федеральный закон от 08.06.2020 № 168-ФЗ «О едином федеральном информационном регистре, содержащем сведения о населении Российской Федерации» http://publication.pravo.gov.ru/Document/View/0001202006080019

[6] Постановление Правительства Российской Федерации от 31.12.2020 № 2426 «Об утверждении Правил формирования записей единого федерального информационного регистра, содержащего сведения о населении Российской Федерации, и внесения в них изменений, включая порядок действий в случае обнаружения неточностей в сведениях, полученных федеральным органом исполнительной власти, осуществляющим функции по контролю и надзору за соблюдением законодательства о налогах и сборах, при формировании и ведении единого федерального информационного регистра, содержащего сведения о населении Российской Федерации»: http://publication.pravo.gov.ru/Document/View/0001202101090013

[7] Постановление Правительства Российской Федерации от 31.12.2020 № 2440 «Об утверждении Правил использования усиленной квалифицированной электронной подписи при формировании и ведении единого федерального информационного регистра, содержащего сведения о населении Российской Федерации» http://publication.pravo.gov.ru/Document/View/0001202101090018

[8] Распоряжение Правительства Российской Федерации от 20.02.2021 № 431-р: http://publication.pravo.gov.ru/Document/View/0001202103010045

- **высокой актуальности информационной безопасности**.

В целях обеспечения конфиденциальности, целостности и доступности обрабатываемой в единой цифровой платформе информации будет создана **система обеспечения кибербезопасности**, **реализующая необходимые меры защиты от утечек информации**, мошенничества, которая позволит своевременно пресекать посягательства на информационные системы, входящие в состав единой цифровой платформы, а также минимизировать ущерб, наносимый информационным системам, входящим в состав единой цифровой платформы, при реализации угроз.

Защита информации, содержащейся в единой цифровой платформе, обеспечивается посредством применения организационных и технических мер и осуществления контроля за функционированием единой цифровой платформы. Для обеспечения защиты информации в ходе создания, обеспечения функционирования и развития единой цифровой платформы осуществляются:

- формирование требований к защите информации, содержащейся в единой цифровой платформе;
- разработка и внедрение системы защиты информации единой цифровой платформы (комплексной системы обеспечения информационной безопасности единой цифровой платформы);
- применение сертифицированных (по требованиям безопасности информации) средств защиты информации, а также проверка единой цифровой платформы на соответствие требованиям защиты информации;
- защита информации при ее передаче по информационно-телекоммуникационным сетям;
- обеспечение защиты информации в ходе функционирования единой цифровой платформы.

2. Концепция цифровой трансформации **государственного управления.**[9]

Вызовами (задачами) цифровой трансформации государственного управления являются: **повышение уровня надежности и безопасности информационных систем**, **технологической независимости** информационно-технологической инфраструктуры **от оборудования и программного обеспечения, происходящих из иностранных государств**.

Стратегические риски:

- отсутствие нормативного правового регулирования, которое может блокировать автоматизированный сбор социально-экономических показателей, так как в настоящее время коммерческие организации не

[9] Распоряжение Правительства Российской Федерации от 22.10.2021 № 2998-р: http://publication.pravo.gov.ru/Document/View/0001202110260034

обязаны предоставлять такую информацию в органы государственной власти (за исключением налоговой отчетности);

- недостаточный уровень цифровых компетенций у сотрудников органов государственной власти и органов местного самоуправления, отсутствие заинтересованности в переводе взаимодействия в электронный вид у всех участников такого взаимодействия;
- наличие зависимости от поставок аппаратной части от зарубежных поставщиков и сопутствующих этому рисков в области **информационной безопасности.**

3. Стратегическое направление цифровой трансформации **обрабатывающих отраслей промышленности.**[10]

Целью цифровой трансформации обрабатывающих отраслей промышленности является **обеспечение технологической независимости государства**, **возможности коммерциализации российских исследований и разработок**, а также ускорение технологического развития российских компаний и обеспечение конкурентоспособности разрабатываемых ими продуктов и решений на глобальном рынке путем достижения «цифровой зрелости» при помощи модернизации управления производственными процессами, что должно привести к значительному повышению производительности труда и росту валового внутреннего продукта в производственном секторе и, следовательно, к росту уровня благосостояния граждан страны.

В ходе реализации стратегического направления будут внедрены следующие технологии:

- искусственный интеллект (далее – ИИ);
- новые производственные технологии;
- робототехника и сенсорика;
- новые коммуникационные интернет-технологии;
- интернет вещей;
- технологии виртуальной и дополненной реальности.

В данном стратегическом направлении информационной безопасности внимание не уделяется, однако поставлен акцент на использование российского программного и технологического обеспечения.

4. Стратегическое направление в области цифровой трансформации **строительной отрасли.**[11]

[10] Распоряжение Правительства Российской Федерации от 06.11.2021 № 3142-р: http://publication.pravo.gov.ru/Document/View/0001202111090018
[11] Распоряжение Правительства Российской Федерации от 27.12.2021 № 3883-р: http://publication.pravo.gov.ru/Document/View/0001202112290003

В документе проблемами текущего состояния строительной отрасли, городского и жилищно-коммунального хозяйства Российской Федерации, решаемыми при цифровизации, являются, в том числе:

- **недостаточный уровень импортозамещения систем информационной безопасности**, используемых в жилищно-коммунальном хозяйстве и городском хозяйстве.

Большинство проектов, включенных в направление, также нацелены на создание безопасных сервисов для физических и юридических лиц.

5. Стратегическое направление в области цифровой трансформации **сферы образования[12].**

   В данном документе упоминается, что направление разработано в соответствии, в том числе, с Указом Президента Российской Федерации от 5 декабря 2016 г. N 646 «Об утверждении Доктрины информационной безопасности Российской Федерации». Однако информационной безопасности в документе внимание не уделено.

В ходе реализации стратегического направления будут внедрены следующие технологии:

- искусственный интеллект в части рекомендательных систем и интеллектуальных систем поддержки принятия решений, перспективных методов и технологий («Цифровой помощник ученика», «Цифровой помощник родителя», «Цифровой помощник учителя»);
- большие данные в части использования методов интеллектуального анализа значительных объемов информации для поддержки принятия управленческих решений и повышения качества данных («Создание и внедрение системы управления в образовательной организации»);
- системы распределенного реестра («Цифровое портфолио ученика»);
- облачные технологии («Библиотека цифрового образовательного контента»).

Стратегическое направление в области цифровой трансформации **транспортной отрасли[13].**

Одним из его проектов является «Цифровизация для транспортной безопасности» — **создание единого защищенного информационного пространства и защищенных технологических сетей транспортного комплекса**, цифровизация государственных услуг в области транспортной безопасности с использованием сведений ограниченного доступа, **внедрение механизмов по обеспечению информационной безопасности на объектах транспортного комплекса** и системы предварительного информирования, а

[12] Распоряжение Правительства Российской Федерации от 02.12.2021 № 3427-р: http://publication.pravo.gov.ru/Document/View/0001202112070025

[13] Распоряжение Правительства Российской Федерации от 21.12.2021 № 3744-р: http://publication.pravo.gov.ru/Document/View/0001202112270030

также обеспечение мониторинга защищенности транспортной информационной инфраструктуры.

Среди текущих проблем цифровизации отрасли выделяют низкую информированность и скоординированность действий органов власти, субъектов транспортной деятельности по вопросам обеспечения безопасности на транспорте (включая транспортную безопасность, **кибербезопасность**).

Установлены показатели цифровой трансформации транспортной отрасли Российской Федерации до 2030 года, и одним из них является «сокращение количества актов незаконного вмешательства к 2023 году на 5%, к 2030 – на 50%».

6. Стратегическое направление в области цифровой трансформации **здравоохранения[14].**

   В ходе реализации стратегического направления будут внедрены следующие технологии:

   - большие данные;
   - управление показателями достижения национальных целей в режиме инцидент-менеджмента.

   Указанные технологии будут применены для информационного сопровождения граждан и контроля объемов, сроков, качества и условий предоставления медицинской помощи по обязательному медицинскому страхованию, для организации процессов управления в сфере здравоохранения на основе результатов обработки медицинских данных в электронной форме **и перехода к электронному документообороту в сфере здравоохранения** Российской Федерации, **цифровизации процессов планирования и управления** в сфере здравоохранения Российской Федерации **при условии обеспечения защиты персональных данных граждан.**

   В рамках реализации стратегического направления будет осуществлена реализация следующих 2 ключевых проектов:

   - «Создание единого цифрового контура в здравоохранении на основе единой государственной информационной системы в сфере здравоохранения»;
   - «Медицинские платформенные решения федерального уровня».

   В результате реализации проекта «Создание единого цифрового контура в здравоохранении на основе единой государственной информационной системы в сфере здравоохранения» будет обеспечено решение задач, необходимых для цифровой трансформации, среди перечня указывается:

   - **обеспечение защиты информации.**

[14] Распоряжение Правительства Российской Федерации от 29.12.2021 № 3980-р (31.12.2021): http://publication.pravo.gov.ru/Document/View/0001202112310112

В рамках реализации стратегического направления **предусмотрено внедрение радиоэлектронной продукции** (в том числе систем хранения данных и серверного оборудования, автоматизированных рабочих мест, программно-аппаратных комплексов, коммуникационного оборудования и систем видеонаблюдения) **российского происхождения.**

7. Стратегическое направление цифровой трансформации отрасли **экологии и природопользования[15].**

   Одной из целей цифровой трансформации является **повышение доли российских цифровых решений и доступности российских критических цифровых технологий**;

   Для повышения доли российских цифровых решений и доступности российских критических цифровых технологий определены следующие задачи:

   - **обеспечение устойчивости и безопасности информационной инфраструктуры отрасли**, конкурентоспособности российских разработок и технологий, масштабирование российского программного обеспечения, а также развитие таких перспективных высокотехнологичных направлений, как квантовые коммуникации, облачные вычисления, использование мобильных сетей связи пятого поколения;

   - **обеспечение информационной безопасности на основе российских разработок при передаче, обработке и хранении данных**, гарантирующей защиту интересов личности, бизнеса и государства, а также организация доступа к данным для различных категорий потребителей, в том числе в целях соблюдения режимов ограничения доступа к информации, составляющей государственную, коммерческую или иную охраняемую законом тайну;

   - запуск в отрасли инновационных решений и критических цифровых технологий на основе больших данных, искусственного интеллекта, интернета вещей, применение беспилотного летательного аппарата, автоматизированных датчиков и постов наблюдения на период 2024 - 2030 годов **предпочтительно на апробированном и сертифицированном российском оборудовании и программном обеспечении.**

8. Стратегическое направление в области цифровой трансформации **отраслей агропромышленного и рыбохозяйственного комплекса[16].**

   В рамках реализации Стратегического направления предусмотрено **внедрение радиоэлектронной продукции** (в том числе систем хранения данных и серверного оборудования, автоматизированных рабочих мест, программно-аппаратных комплексов, коммуникационного оборудования, систем видеонаблюдения) **российского происхождения и снижение**

---

[15] Распоряжение Правительства Российской Федерации от 08.12.2021 № 3496-р: http://publication.pravo.gov.ru/Document/View/0001202112140019

[16] Распоряжение Правительства Российской Федерации от 29.12.2021 № 3971-р (31.12.2021) http://publication.pravo.gov.ru/Document/View/0001202112310100

импортозависимости от программно-аппаратных средств и программного обеспечения и увеличение доли российской электронной продукции, используемой при реализации проектов в области цифровой трансформации агропромышленного и рыбохозяйственного комплексов..

Информационной безопасности в данном документе внимание не уделено.

9. Концепция создания и функционирования государственной информационной системы «Единая цифровая платформа «**Физическая культура и спорт**» http://www.consultant.ru/document/cons_doc_LAW_386543/#dst0

Одними из основных направлений реализации Концепции являются:

- совершенствование нормативной правовой и методической базы в области использования информационно-телекоммуникационных технологий в сфере ФКиС — **регламентация вопросов автоматизированной обработки персональных данных** субъектов сферы ФКиС, перехода к электронному документообороту между субъектами сферы ФКиС, в том числе при предоставлении государственных и муниципальных услуг, использования электронной подписи, **обеспечения информационной безопасности;**

- формирование нового подхода к управлению данными - формирование и реализация политики по работе с данными, нацеленной на создание экосистемы, и процессов, обеспечивающих максимально быстрое получение, обработку и анализ данных, их безопасное хранение, извлечение максимальной ценности из используемых данных, соблюдение требований законодательства о персональных данных, разработку и внедрение правил обмена данными, в том числе единого электронного формата обмена данными, **формирование политики информационной безопасности**, формирование системы принятия решений на основе данных, включающей сочетание автоматизированных систем принятия решений и систем поддержки принятия управленческих решений.

В документе также есть отдельные разделы **«Классификация Системы в соответствии с требованиями по защите информации»** и **«Обеспечение информационной безопасности».**

Согласно документу, задачами обеспечения безопасности информации, формируемой в системе, являются:

1. создание организационных и технических решений, обеспечивающих противодействие угрозам безопасности информации;
2. обеспечение выполнения требований нормативных правовых актов по защите информации в государственных информационных системах, в том числе по защите персональных данных (далее - ПДн);
3. минимизация рисков нанесения (пресечение, нейтрализация, отражение) субъектам ПДн, интересы которых затрагиваются при использовании объекта защиты, материального ущерба, морального или иного случайного или

преднамеренного вреда, а также ущемления их законных прав в результате нарушения заданных характеристик безопасности ПДн;

4. минимизация негативных последствий нарушения одного из свойств безопасности информации (конфиденциальности, целостности, доступности).

Важно отметить, что в 2022 году издан указ Президента Российской Федерации №166[17], регулирующий вопросы приобретения и применения российских средств радиоэлектроники и программного обеспечения рядом организаций, являющихся субъектами критической информационной инфраструктуры.

Исследовательские центры в сфере искусственного интеллекта

Опубликовано положение о рабочей группе по **исследовательским центрам в сфере искусственного интеллекта**[18] (организованы Аналитическим центром при Правительстве Российской Федерации).

Поддерживаемые направления центров:

Общесистемные и кросс-отраслевые центры:

3 общесистемных (инфраструктурно-отраслевых):

- **Доверенный искусственный интеллект** (создание стека системного ПО для анализа и верификации систем, основанных на применении технологий ИИ);
- Этические аспекты применения ИИ;
- **ИИ для обеспечения кибербезопасности.**

2 универсальных (кросс-отраслевых) центра:

- Биометрические технологии ИИ (построении наиболее точных и надежных алгоритмов идентификации человека по его биометрическим данным);
- Анализ естественного языка методами ИИ (моделирования всех уровней естественного языка (фонетика, морфология, синтаксис, семантика, прагматика) и его модальностей (текст, речь) с помощью вычислительных систем и методов ИИ.

Отраслевые центры:

- ИИ для промышленности;
- ИИ для робототехники и управления беспилотными системами;
- ИИ для медицины;
- ИИ для «Умного города» и транспорта;
- ИИ для решений по углеродному следу;

[17] Указ Президента Российской Федерации от 30.03.2022 № 166 «О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации»: http://publication.pravo.gov.ru/Document/View/0001202203300001

[18] Постановление Правительства Российской Федерации от 28.08.2021 № 1428: http://publication.pravo.gov.ru/Document/View/0001202108310009

- ИИ для решения задач развития ТЭК и энергетики;
- ИИ в сельском хозяйстве и производстве продуктов питания;
- ИИ в биотехнологиях и генной инженерии;
- Межотраслевые технологии ИИ и ИИ для иных приоритетных отраслей экономики и социальной сферы.

Научная технологическая инициатива

Внесены изменения в дорожные карты инициатив, объединенных в «Национальную технологическую инициативу»[19]:

Все изменения в нижеуказанные «дорожные карты» направлены на совершенствование законодательства и удаление административных барьеров для осуществления технологических инициатив.

1. Изменения в дорожную карту Национальной технологической инициативы «Аэронет»[20].
2. Изменения в дорожную карту Национальной технологической инициативы «Нейронет»[21].
3. Изменения в дорожную карту Национальной технологической инициативы «Маринет»[22].

Президиумом Правительственной комиссии по цифровому развитию, использованию информационных технологий утверждена **дорожная карта «Новые производственные технологии»**[23] в рамках национальной программы «Цифровая экономика». Картой предусмотрено также **создание центров тестирования российского промышленного ПО**. Ответственные за реализацию дорожной карты — государственные корпорации «Росатом» и «Ростех».

Центр НТИ по сквозной технологии «Технологии доверенного взаимодействия»

Согласно протоколу конкурсной комиссии по отбору получателей грантов на государственную поддержку центров национальной технологической инициативы на базе образовательных организаций высшего образования и научных организаций от 18.11.2021 г. в Томском государственном университете систем управления и радиоэлектроники будет создан центр НТИ по сквозной технологии «Технологии доверенного взаимодействия».

---

[19] Национальная технологическая инициатива: https://nti2035.ru/
[20] Распоряжение Правительства Российской Федерации от 16.09.2021 № 2587-р: http://publication.pravo.gov.ru/Document/View/0001202109230011
[21] Распоряжение Правительства Российской Федерации от 24.12.2021 № 3842-р: http://publication.pravo.gov.ru/Document/View/0001202112280037
[22] Распоряжение Правительства Российской Федерации от 24.12.2021 № 3836-р: http://publication.pravo.gov.ru/Document/View/0001202112280028

[23] «Минцифры России будет координировать развитие новых производственных и коммуникационных технологий»: https://digital.gov.ru/ru/events/41196/

В программе стратегического развития ТУСУРа проект «ИТ, безопасная цифровая среда и киберфизические системы» является одним из ключевых. Создание центра НТИ по сквозной технологии доверенного взаимодействия позволит проводить исследования, готовить кадры и вести практические разработки по новому направлению привлечением коллег и партнёров из ведущих университетов и компаний.

Программа государственной поддержки центров компетенций НТИ стартовала в 2017 году (Постановление Правительства РФ от 16.10.2017 N 1251 (ред. от 29.10.2021) «Об утверждении Правил предоставления субсидии из федерального бюджета на оказание государственной поддержки центров Национальной технологической инициативы на базе образовательных организаций высшего образования и научных организаций и Положения о проведении конкурсного отбора на предоставление грантов на государственную поддержку центров Национальной технологической инициативы на базе образовательных организаций высшего образования и научных организаций»). Конкурс проводится Фондом поддержки проектов НТИ в соответствии с поручением Минобрнауки России. Центры ведут исследовательскую и образовательную деятельность в консорциуме с крупнейшими технологическими компаниями и научными организациями, выступая платформой для развития кооперации университетского, научного и бизнес-сообщества для преодоления технологических барьеров и укрепления позиций российских компаний на глобальных рынках НТИ.

Центры компетенций НТИ — сеть инженерно-образовательных консорциумов на базе российских университетов и научных организаций, которые занимаются развитием «сквозных» технологий НТИ. Центры ведут исследовательскую и образовательную деятельность в партнерстве с крупнейшими технологическими компаниями. Участники консорциума определяют конкретные направления деятельности Центров, а также набор реализуемых проектов с учетом перспектив их коммерциализации.

Постановлением Правительства Российской Федерации от 27.09.2021 № 1626 «О внесении изменений в Положение о федеральной **государственной информационной системе координации информатизации**»[24] (ФГИС КИ[25]) была исключена система «Электронный регион», а также введена организация информационно-технологического взаимодействия ФГИС КИ с единой межведомственной информационно-статистической системой и иными информационными системами в целях сбора и обработки информации для формирования официальной статистических данных по показателям цифровой зрелости, предусмотренным указом президента от 21.07.2020 РФ № 474 «О национальных целях развития Российской Федерации на период до 2030 года».

Функции ФГИС КИ направлены на реализацию ведомственных программ цифровой трансформации, которые включают планирование закупок оборудования и ИТ-решений в соответствии с едиными стандартами цифровизации госорганов.

---

[24] Постановление Правительства Российской Федерации от 27.09.2021 № 1626 «О внесении изменений в Положение о федеральной государственной информационной системе координации информатизации»: http://publication.pravo.gov.ru/Document/View/0001202109290012

[25] ФГИС КИ: https://portal.eskigov.ru/

Продолжается и перевод ФГИС КИ в государственную единую облачную платформу (ГосОблако), которая является одним из сервисов «ГосТеха».

Постановление Правительства Российской Федерации от 20.10.2021 № 1795[26] «О внесении изменений в Положение **о проведении эксперимента по переводу информационных систем и информационных ресурсов федеральных органов исполнительной власти**, Центральной избирательной комиссии Российской Федерации и государственных внебюджетных фондов **в государственную единую облачную платформу**, а также по обеспечению федеральных органов исполнительной власти и государственных внебюджетных фондов автоматизированными рабочими местами и программным обеспечением».

Согласно постановлению, вдобавок к 20 ведомствам, уже участвующим в эксперименте по переходу в ГосОблако, добавятся:

- Министерство просвещения РФ;
- Министерство спорта РФ;
- Министерство РФ по делам гражданской обороны, чрезвычайных ситуаций и ликвидации стихийных бедствий;
- Федеральная служба по гидрометеорологии и мониторингу окружающей среды;
- Федеральная антимонопольная служба;
- Федеральное медико-биологическое агентство.

Эксперимент показал положительное влияние использования ГосОблака в деятельности федеральных органов исполнительной власти и государственных внебюджетных фондов, в частности:

- повысилась надежность, отказоустойчивость и катастрофоустойчивость в работе государственных информационных систем, появилась возможность долгосрочного планирования и оптимизации бюджетных эксплуатационных затрат;
- отмечается эффективность и достижимость импортозамещения при обеспечении ведомств информационной инфраструктурой и необходимым программным обеспечением;
- повышается готовность ведомств к цифровой трансформации и уменьшаются риски при переходе на сервисную модель, а также снижается совокупная стоимость владения государственными информационными системами.

[26] Постановление Правительства Российской Федерации от 20.10.2021 № 1795 «О внесении изменений в Положение о проведении эксперимента по переводу информационных систем и информационных ресурсов федеральных органов исполнительной власти, Центральной избирательной комиссии Российской Федерации и государственных внебюджетных фондов в государственную единую облачную платформу, а также по обеспечению федеральных органов исполнительной власти и государственных внебюджетных фондов автоматизированными рабочими местами и программным обеспечением»: http://publication.pravo.gov.ru/Document/View/0001202110220032

Эксперимент будет продолжаться до конца 2022 года. В постановлении Правительства РФ от 28 августа 2019 г. N 1114 об эксперименте уделено внимание информационной безопасности.

Для проведения эксперимента Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации по согласованию с Федеральной службой безопасности Российской Федерации и Федеральной службой по техническому и экспортному контролю утверждает требования:

- к центрам обработки данных, присоединяемым в рамках эксперимента к государственной единой облачной платформе;
- **к обеспечению информационной безопасности в государственной единой облачной платформе;**

Выпущено распоряжение об инициативах по социально-экономическому развитию до 2030 г., содержат **мероприятия по цифровой трансформации, включающие инициативы Минцифры России[27]:**

- «Доступ в Интернет»
- «Цифровой профиль гражданина»
- «Госуслуги онлайн»
- «Электронный документооборот»
- «Подготовка кадров для ИТ»

Выпущено постановление Правительства РФ «Об изменениях, которые вносятся в Правила организации деятельности многофункциональных центров предоставления государственных и муниципальных услуг[28]. Согласно постановлению, **при предоставлении государственных и муниципальных услуг при наличии технической возможности возможна идентификация личности с помощью единой биометрической системы**.

Также по решению высшего исполнительного органа государственной власти центры могут быть оснащены программно-техническими комплексами, позволяющим осуществлять размещение или обновление биометрических персональных данных в единой биометрической системе.

Государственные информационные системы

Внесены изменения в Положение о системе управления общественными финансами **«Электронный бюджет»**[29].

---

[27] Распоряжение Правительства Российской Федерации от 06.10.2021 № 2816-р http://publication.pravo.gov.ru/Document/View/0001202110070028

[28] Постановление Правительства Российской Федерации от 19.10.2021 № 1775 «О внесении изменении в Правила организации деятельности многофункциональных центров предоставления государственных и муниципальных услуг»: http://publication.pravo.gov.ru/Document/View/0001202110200045

[29] Постановление Правительства Российской Федерации от 15.07.2021 № 1214 «О внесении изменений в Положение о государственной интегрированной информационной системе управления общественными финансами «Электронный бюджет»: http://publication.pravo.gov.ru/Document/View/0001202107190003

Изменения подразумевают, что Министерство финансов Российской Федерации вправе приобретать программно-технические средства, необходимые для выполнения работ за счет бюджетных ассигнований, предусмотренных в федеральном бюджете Министерству финансов Российской Федерации, и передавать такие программно-технические средства в безвозмездное временное пользование субъектам системы «Электронный бюджет».

ФГИС «Электронный бюджет» предназначена для обеспечения прозрачности, открытости и подотчетности деятельности государственных органов и органов управления государственными внебюджетными фондами, органов местного самоуправления, государственных и муниципальных учреждений, а также для повышения качества их финансового менеджмента за счет формирования единого информационного пространства и применения информационных и телекоммуникационных технологий в сфере управления государственными и муниципальными (общественными) финансами. Введена в эксплуатацию в 2015 г.

Утверждена государственная программа Российской Федерации **«Национальная система пространственных данных»** (постановление Правительства от 1 декабря 2021 года №2148)[30]

Государственная программа направлена на достижение национальных целей развития страны «Цифровая трансформация» и «Комфортная и безопасная среда для жизни», определенных Указом Президента РФ от 21 июля 2020 г. № 474 «О национальных целях развития Российской Федерации на период до 2030 года».

К 2030 году планируется создание единой цифровой платформы пространственных данных и единую электронную картографическую основу, которые будут включать в себя сведения об объектах недвижимости, зарегистрированных правах на недвижимое имущество и государственной кадастровой оценке.

Их внедрение и функционирование позволит повысить качество государственных услуг в части осуществления государственного кадастрового учета недвижимого имущества или государственной регистрации прав на него.

Про обеспечение информационной безопасности системы в документе не говорится.

Информационная безопасность

По данной теме за 2021 год было принято 45 нормативных правовых актов (16% от всех принятых в исследуемой сфере актов).

Сокращение субсидий на ИБ. Минцифры РФ отменило субсидии из федерального бюджета на поддержку экспорта отечественных разработок и технологий в области информационной безопасности[31].

---

[30] Государственная программа Российской Федерации «Национальная система пространственных данных»: http://publication.pravo.gov.ru/Document/View/0001202112070014

[31] Постановление Правительства Российской Федерации от 08.02.2021 № 136 «О признании утратившим силу постановления Правительства Российской Федерации от 29 октября 2019 г. № 1382»: http://publication.pravo.gov.ru/Document/View/0001202102110022

Изначально целью субсидий было продвижение за рубежом отечественных решений в области информационной безопасности, а также оказание поддержки российским производителям по патентованию своих продуктов и услуг.

В связи с исключением финансирования соответствующих целей, средства на них не были предусмотрены в федеральном бюджете на 2021 г. и на плановый период 2022-2023 гг.

Однако стоит отметить, что ситуация стала стремительно меняться в феврале-марте 2022 года, когда был подписан указ о льготах для российской ИТ-индустрии, а также расширены грантовые фонды.

Киберполигоны. Продолжается курс в области создания киберполигонов. В 2021 году внесены уточняющие изменения в положение о субсидиях на их создание[32]. В том числе уточнены требования к организации, участвующей в конкурсе на получение субсидий. Указано, что все соглашения и дополнительные соглашения заключаются в ГИИС «Электронный бюджет» **с соблюдением требований о защите государственной тайны**.

Результатом предоставления субсидии является результат федерального проекта «введен в эксплуатацию и обеспечено функционирование киберполигона для обучения и тренировки специалистов и экспертов разного профиля, руководителей в области информационной безопасности и информационных технологий современным практикам обеспечения информационной безопасности». Срок предоставления результата — 15 ноября 2024 г.

Показателями, необходимыми для достижения результата предоставления субсидии, являются:

- создан и введен в эксплуатацию 1 сегмент киберполигона для не менее чем 2 информационных технологических инфраструктур, эмулирующих **корпоративные сети организаций банковской системы Российской Федерации («ИТ-киберполигон»)**;
- создан и введен в эксплуатацию 1 сегмент киберполигона для не менее чем 1 индустриальной инфраструктуры **(автоматизированной системы управления технологическим процессом**) энергетического сектора **(«Индустриальный киберполигон»**);
- создан и введен в эксплуатацию 1 **сегмент киберполигона нефтегазового комплекса**;

[32] Постановление Правительства Российской Федерации от 27.02.2021 № 288 «О внесении изменений в постановление Правительства Российской Федерации от 12 октября 2019 г. № 1320»: http://publication.pravo.gov.ru/Document/View/0001202103050011
Постановление Правительства Российской Федерации от 28.12.2021 № 2500 «О внесении изменений в Правила предоставления субсидий из федерального бюджета на введение в эксплуатацию и обеспечение функционирования киберполигона для обучения и тренировки специалистов и экспертов разного профиля, руководителей в области информационной безопасности и информационных технологий современным практикам обеспечения безопасности»: http://publication.pravo.gov.ru/Document/View/0001202112300034

- создан и введен в эксплуатацию 1 сегмент **киберполигона транспортной сферы**;
- создан и введен в эксплуатацию 1 сегмент **киберполигона отрасли связи**;
- создан и введен в эксплуатацию 1 сегмент **киберполигона горнодобывающей и металлургической промышленностей**;
- обеспечено кросс-отраслевое взаимодействие созданных инфраструктур сегментов киберполигона для проведения межотраслевых киберучений;
- обеспечено создание условий по использованию **киберполигона для** отработки практических навыков специалистов и экспертов разного профиля, **руководителей в области обеспечения информационной безопасности** и информационных технологий на территории федерального государственного автономного образовательного учреждения высшего образования «Дальневосточный федеральный университет».

Утверждены требования к **автоматизированным информационным системам оформления воздушных перевозок**[33] (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.

Федеральный закон от 01.07.2021 № 237-ФЗ «О ратификации Соглашения о сотрудничестве государств-участников Содружества Независимых Государств в борьбе с преступлениями в сфере информационных технологий»[34]. **Согласно закону, Российская Федерация оставляет за собой право признавать деяния, предусмотренные пунктами Соглашения, как в качестве уголовно наказуемых в соответствии с УК РФ, так и в качестве административно наказуемых в соответствии с КоАП РФ.**

В соответствии с требованиями 236-ФЗ **иностранные IT-компании, работающие в российском сегменте сети «Интернет»** и обладающие аудиторией более 500 тыс. человек в сутки, с 1 января 2022 года **обязаны создать свой филиал, открыть представительство или учредить российское юридическое лицо на территории РФ, а также зарегистрировать личный кабинет на сайте Роскомнадзора для взаимодействия с органами власти и установить на информационном ресурсе рекомендованный счетчик посещаемости**[35]**.**

---

[33] Постановление Правительства Российской Федерации от 30.04.2021 № 685 «О внесении изменения в постановление Правительства Российской Федерации от 24 июля 2019 г. № 955»: http://publication.pravo.gov.ru/Document/View/0001202105060001

[34] Федеральный закон от 01.07.2021 № 237-ФЗ «О ратификации Соглашения о сотрудничестве государств - участников Содружества Независимых Государств в борьбе с преступлениями в сфере информационных технологий»: http://publication.pravo.gov.ru/Document/View/0001202107010016

[35] Федеральный закон от 01.07.2021 № 236-ФЗ «О деятельности иностранных лиц в информационно-телекоммуникационной сети «Интернет» на территории Российской Федерации»: http://publication.pravo.gov.ru/Document/View/0001202107010014

Список опубликован на официальном сайте Роскомнадзора, в который вошли 13 иностранных компаний, которые владеют 22 информационными ресурсами[36].

В реестр включены компании:

1. Google (Google Play, YouTube, YouTube Music, Google Chat, Gmail).
2. Apple (iCloud, App Store, Apple Music).
3. Meta Platforms (Facebook, Instagram, WhatsApp), которая с 28.03.2022 признана экстремистской организацией и запрещена на территории РФ.
4. Twitter.
5. TikTok.
6. Telegram.
7. Zoom Video Communications.
8. Viber.
9. Spotify.
10. Likeme Pte. Ltd. (Likee).
11. Discord.
12. Pinterest.
13. Twitch.

Какие компании выполнили требования Роскомнадзора (по состоянию на 16 февраля 2022 года):

Полностью обязательства выполнили только Apple и Spotify (по состоянию на 16 февраля 2022 года).

Частично выполнили требования: Viber, TikTok, Likee, Twitter (открыл личный кабинет) и Zoom.

Не выполнили требования: Google, Meta Platforms (признана экстремистской организацией и запрещена на территории РФ), Discord, Pinterest, Twitch и Telegram.

Комментарий: Meta Platforms (признана экстремистской организацией и запрещена на территории РФ) только направила заявление о регистрации личного кабинета на официальном сайте Роскомнадзора.

Компания Zoom Video Communications зарегистрировала личный кабинет на официальном сайте Роскомнадзора. Компания также сообщила, что ведется работа над созданием формы обратной связи и рассматривается вопрос открытия представительства на территории РФ.

Роскомнадзор создал Реестр социальных сетей[37], в который внесены сервисы, в которых контент распространяется с персональных страниц пользователей. Также

[36] Перечень иностранных лиц, осуществляющих деятельность в сети «Интернет» на территории Российской Федерации: https://236-fz.rkn.gov.ru/agents/list

посещаемость соцсети должна превышать 500 тыс. человек в сутки. Участники реестра обязаны самостоятельно удалять всю противоправную информацию. Закон вступил в силу 1 февраля 2021 года.

В перечень вошли **Twitter, TikTok, YouTube «ВКонтакте», «Одноклассники», Likee, Instagram и Facebook** (оба ресурса принадлежат корпорации Meta, которая по состоянию на март 2022 года внесена в перечень общественных объединений и религиозных организаций, в отношении которых судом принято вступившее в законную силу решение о ликвидации или запрете деятельности по основаниям, предусмотренным Федеральным законом от 25.07.2002 № 114-ФЗ «О противодействии экстремистской деятельности»). В данный список не попали мессенджеры. Вышло также постановление Правительства Российской Федерации от 01.11.2021 № 1894 «Об утверждении Правил создания, формирования и ведения реестра информационных ресурсов, объем аудитории которых подлежит исследованию»[38].

Вышел приказ Федеральной службы безопасности Российской Федерации от 29.11.2021 № 472 «**О внесении изменений** в приказ ФСБ России от 11 декабря 2013 г. № 747 «**Об утверждении Перечня должностных лиц органов федеральной службы безопасности, уполномоченных составлять протоколы об административных правонарушениях**, и о реализации отдельных положений Кодекса Российской Федерации об административных правонарушениях в органах федеральной службы безопасности» и утвержденный этим приказом Перечень»[39].

Согласно документу, перечень должностных лиц органов федеральной службы безопасности дополнен пунктами:

«6.1. **Руководители служб, департаментов, их заместители, начальники управлений, центров, инспекций, служб, отделов, направлений, лабораторий, отделений и их заместители, начальники групп.**

Научные консультанты, ведущие оперативные сотрудники, ведущие научные сотрудники, старшие инспекторы, инспекторы, ученые консультанты, старшие консультанты, старшие оперативные сотрудники, старшие оперуполномоченные по особо важным делам, ведущие сотрудники, старшие научные сотрудники, консультанты, старшие оперуполномоченные, старшие офицеры, старшие референты, старшие следователи, старшие сотрудники, оперуполномоченные, офицеры, сотрудники, референты, младшие оперуполномоченные, младшие референты.

---

[37] Реестр социальных сетей: https://530-fz.rkn.gov.ru/

[38] Постановление Правительства Российской Федерации от 01.11.2021 № 1894 «Об утверждении Правил создания, формирования и ведения реестра информационных ресурсов, объем аудитории которых подлежит исследованию»: http://publication.pravo.gov.ru/Document/View/0001202111030033

[39] Приказ Федеральной службы безопасности Российской Федерации от 29.11.2021 № 472 «О внесении изменений в приказ ФСБ России от 11 декабря 2013 г. № 747 «Об утверждении Перечня должностных лиц органов федеральной службы безопасности, уполномоченных составлять протоколы об административных правонарушениях, и о реализации отдельных положений Кодекса Российской Федерации об административных правонарушениях в органах федеральной службы безопасности» и утвержденный этим приказом Перечень»: http://publication.pravo.gov.ru/Document/View/0001202111300061

«Указанные должностные лица с учетом осуществляемых должностных полномочий в пределах компетенции и по линиям работы уполномочены составлять протоколы об административных правонарушениях, перечисленных в части 1 статьи 23.91 Кодекса».

«9.1. **Начальники территориальных органов безопасности и органов безопасности в войсках, их заместители.**

Начальники структурных подразделений территориальных органов безопасности и органов безопасности в войсках (служб, инспекций, отделов, отделений, направлений) и их заместители, начальники групп.

Старшие инспекторы, инспекторы, старшие консультанты, старшие оперативные сотрудники, старшие оперуполномоченные по особо важным делам, консультанты, старшие оперуполномоченные, старшие офицеры, старшие референты, старшие инженеры, оперуполномоченные, офицеры, референты, инженеры, младшие оперуполномоченные, младшие референты».

Импортозамещение

По данному разделу за 2021 год было принято 18 нормативных правовых актов (6% от общего количества принятых актов в исследуемой сфере).

В августе 2021 года был введен запрет на госзакупки импортных планшетов, ноутбуков, портативных компьютеров, серверов и интегральных микросхем[40].

Согласно постановлению №1432 от 28.08.2021, в их отношении «устанавливается запрет на допуск для целей осуществления закупок для государственных и муниципальных нужд, предусмотренный приложением к постановлению Правительства РФ от 30.04.2020 № 616 «Об установлении запрета на допуск промышленных товаров, происходящих из иностранных государств, для целей осуществления закупок для государственных и муниципальных нужд, а также промышленных товаров, происходящих из иностранных государств, работ (услуг), выполняемых (оказываемых) иностранными лицами, для целей осуществления закупок для нужд обороны страны и безопасности государства».

Также «при осуществлении закупок радиоэлектронной продукции, включенной в перечень, заказчик отклоняет все заявки, содержащие предложения о поставке радиоэлектронной продукции, происходящей из иностранных государств (за исключением государств-членов Евразийского экономического союза), при условии, что на участие в закупке подана 1 (или более) удовлетворяющая требованиям извещения об осуществлении закупки и (или) документации о закупке заявка, содержащая предложение о поставке радиоэлектронной продукции, произведенной на территориях государств-членов Евразийского экономического союза.

Подтверждением производства радиоэлектронной продукции является:

[40] Постановление Правительства Российской Федерации от 28.08.2021 № 1432 «О внесении изменений в некоторые акты Правительства Российской Федерации»: http://publication.pravo.gov.ru/Document/View/0001202108310011

- на территории Российской Федерации — наличие сведений о такой продукции в реестре;
- на территории государства-члена Евразийского экономического союза — наличие сведений о такой продукции в евразийском реестре промышленных товаров государств-членов Евразийского экономического союза, формирование и ведение которого устанавливаются правом Евразийского экономического союза.

При этом согласно пункту 3 постановления №616 «**запрет** на допуск промышленных товаров, происходящих из иностранных государств **не применяется** в случае наличия разрешения на закупку происходящего из иностранного государства промышленного товара, выдаваемого с использованием государственной информационной системы промышленности в порядке, установленном Министерством промышленности и торговли Российской Федерации; **в случае закупки одной единицы товара, стоимость которой не превышает 100 тыс. рублей, и закупки совокупности таких товаров, суммарная стоимость которых составляет менее 1 млн. рублей** (за исключением закупок товаров, указанных в пунктах 1 - 7, 123, 125 - 127 перечня промышленных товаров); в случае необходимости обеспечения взаимодействия товаров с товарами, используемыми заказчиком, ввиду их несовместимости с товарами, имеющими другие товарные знаки (за исключением закупок товаров, указанных в пунктах 67 - 71 перечня промышленных товаров); в случае закупки запасных частей и расходных материалов к машинам и оборудованию, используемым заказчиком в соответствии с технической документацией на указанные машины и оборудование (в случае закупки товаров, указанных в пунктах 25(3) - 25(7) и 47 - 51 перечня промышленных товаров)».

В сентябре 2021 года утверждён **план мероприятий («дорожная карта») «Создание дополнительных условий для развития отрасли информационных технологий»**[41]

Согласно плану мероприятий, в сфере информационной безопасности планируются следующие решения:

1. Обеспечение в рамках исполнения **федерального проекта «Информационная безопасность»** национальной программы «Цифровая экономика Российской Федерации» ввода в эксплуатацию 3-х сегментов киберполигона для обучения и тренировки специалистов и экспертов разного профиля, руководителей в области информационной безопасности и информационных технологий современным практикам обеспечения безопасности (про киберполигоны написали выше).
2. Внесение изменений в нормативные правовые акты, предусматривающих **включение в ВПЦТ раздела по информационной безопасности в качестве обязательного условия согласования ВПЦТ**, с учетом применения отечественных передовых решений в сфере информационной безопасности

[41] План мероприятий («дорожная карта») «Создание дополнительных условий для развития отрасли информационных технологий» (утв. Правительством РФ 9 сентября 2021 г.): http://www.garant.ru/hotlaw/federal/1484752/#review

3. **Внесение изменений в федеральный проект «Информационная безопасность»** национальной программы «Цифровая экономика Российской Федерации» с целью включения результатов, предусматривающих:
    - проведение обучения ключевых руководителей и специалистов по информационной безопасности зарубежных стран с участием российских компаний-вендоров программного обеспечения по информационной безопасности за счет средств федерального бюджета;
    - обучение иностранных студентов решениям в сфере информационной безопасности в ВУЗах Российской Федерации совместно с российскими компаниями-вендорами (профессиональное образование, дополнительное образование).
4. **Обеспечение для ИТ-компаний сферы информационной безопасности приоритетного права доступа к мерам государственной поддержки**, предусмотренным в федеральном проекте «Цифровые технологии» национальной программы «Цифровая экономика Российской Федерации»

Отметим, что начиная с марта 2022 года, сформированы дополнительные меры поддержки ИТ-отрасли:

Президент РФ подписал Указ от 02.03.2022 № 83[42], направленный на поддержку ИТ-отрасли. Меры распространяются на аккредитованные организации, осуществляющие деятельность в области информационных технологий (аккредитованные ИТ-компании).

В соответствии с Указом Правительству РФ поручено для аккредитованных ИТ-компаний:

- обеспечить выделение ежегодно из федерального бюджета бюджетных ассигнований на **осуществление грантовой поддержки перспективных разработок отечественных решений в области информационных технологий**;
- предусмотреть выделение финансовых средств аккредитованным организациям, осуществляющим деятельность в области ИТ, на улучшение жилищных условий работников этих организаций и обеспечение повышения уровня их заработной платы;
- **обеспечить предоставление льготных кредитов по ставке, не превышающей 3 процентов**, на обеспечение текущей деятельности аккредитованных организаций и реализацию новых проектов;

Поручено также принять меры, направленные:

- на установление до 31 декабря 2024 г. для аккредитованных организаций налоговой ставки по **налогу на прибыль организаций в размере 0 процентов**;

[42] Указ Президента Российской Федерации от 02.03.2022 № 83 «О мерах по обеспечению ускоренного развития отрасли информационных технологий в Российской Федерации»: http://publication.pravo.gov.ru/Document/View/0001202203020001

- на упрощение процедур трудоустройства иностранных граждан и получения этими гражданами вида на жительство;
- на установление налоговых льгот и преференций для аккредитованных организаций, получающих доходы от распространения рекламы или оказания дополнительных услуг с использованием приложений и онлайн-сервисов этих организаций либо доходы, связанные с реализацией, установкой, тестированием и сопровождением отечественных решений в области информационных технологий;
- на освобождение аккредитованных организаций от налогового контроля, валютного контроля и других видов государственного контроля (надзора) и муниципального контроля на срок до трех лет;
- на обеспечение консолидации и стимулирования закупок критически важных отечественных разработок в области информационных технологий, проводимых для обеспечения государственных и муниципальных нужд или проводимых
- отдельными видами юридических лиц, а также на упрощение порядка проведения таких закупок.

Работникам аккредитованных ИТ-компаний будет предоставляться отсрочка от призыва на военную службу до достижения возраста 27 лет.

В сентябре 2021 года вышло постановление Правительства РФ о создании инновационного научно-технологического центра «Интеллектуальная электроника – Валдай»[43] (на базе Новгородского государственного университета имени Ярослава Мудрого),

Направления научно-технологической деятельности, осуществляемой на территории Центра:

- разработка и создание высокотехнологичной электронно-компонентной базы, профессиональной и потребительской электроники;
- разработка и создание квантовых сенсоров, устройств
- с использованием квантовых технологий;
- разработка и создание новых, в том числе портативных, источников энергии;
- разработка биомедицинских клеточных технологий;
- разработка и создание мобильной сети связи 5-го поколения;
- разработка и создание интернета вещей (приборы, устройства, системы, программные платформы).

Также одобрен **проект концепции научно-технической программы Союзного государства «Разработка интеллектуальных, высокотехнологичных цифровых и электронных компонентов и систем для автотранспортных средств специального**

[43] Постановление Правительства Российской Федерации от 30.09.2021 № 1649 «О создании инновационного научно-технологического центра «Интеллектуальная электроника - Валдай»: http://publication.pravo.gov.ru/Document/View/0001202110010002

и двойного назначения»[44] («Интелавто»), в котором государственным заказчиком-координатором выступит Минпромторг России.

Внесены изменения в Положение о Минцифры России[45], которое теперь дополнено словами **о выработке** государственного **политики по стимулированию спроса на отечественную радиоэлектронную продукцию гражданского назначение, а также государственной политики в сфере развития и поддержки российской электронной продукции и программного обеспечения**, в том числе при реализации мер поддержки проектов разработки, внедрения и использования информационно-телекоммуникационных решений.

Таким образом, мы видим большое число мер, направленных на поддержку ИТ-отрасли, в том числе ряда вопросов обеспечения ИБ, которые усилены в 2022 году.

Другие нормативные правовые акты

Национальная безопасность

Указом Президента Российской Федерации от 02.07.2021 г. № 400 была **утверждена Стратегия национальной безопасности Российской Федерации**[46]**.** Предыдущая действовала с 31 декабря 2015 г. согласно Указу Президента Российской Федерации № 683 «О Стратегии национальной безопасности Российской Федерации» (Собрание законодательства Российской Федерации, 2016, № 1, ст. 212).

Помимо того, что в этом документе уделено внимание информационной безопасности, и она теперь выступает одним из национальных приоритетов, в нем также упоминается и политика в области международной информационной безопасности.

В Стратегии определено, что информационное пространство выступает новой сферой ведения военных действий. Согласно документу, Российская Федерация также стремится к повышению эффективности многостороннего сотрудничества на важных для мирового сообщества направлениях, в числе которых международная информационная безопасность.

Также выпущен указ Президента Российской Федерации от 17.01.2022 № 15 «О внесении изменений в Положение о Министерстве обороны Российской Федерации, утвержденное Указом Президента Российской Федерации от 16 августа 2004 г. № 1082, и Положение о Генеральном штабе Вооруженных Сил Российской Федерации, утвержденное Указом Президента Российской Федерации от 23 июля 2013 г. № 631», согласно которому теперь **Минобороны уполномочено определять политику в области международной информационной безопасности.**

---

[44] Распоряжение Правительства Российской Федерации от 22.10.2021 № 2981-р: http://publication.pravo.gov.ru/Document/View/0001202110260009

[45] Постановление Правительства Российской Федерации от 17.12.2021 № 2344 «О внесении изменений в Положение о Министерстве цифрового развития, связи и массовых коммуникаций Российской Федерации»: http://publication.pravo.gov.ru/Document/View/0001202112220034

[46] Указ Президента Российской Федерации от 02.07.2021 № 400 «О Стратегии национальной безопасности Российской Федерации»: http://publication.pravo.gov.ru/Document/View/0001202107030001

Немного ранее такими же полномочиями было наделено и Минцифры России[47].

Утверждены «**Основы государственной политики Российской Федерации в области международной информационной безопасности**»[48] (Указ Президента Российской Федерации от 12.04.2021 № 213). Согласно документу, целью государственной политики в области международной информационной безопасности является содействие установлению международно-правового режима, при котором создаются условия для предотвращения (урегулирования) межгосударственных конфликтов в глобальном информационном пространстве, а также для формирования с учетом национальных интересов Российской Федерации системы обеспечения международной информационной безопасности.

Биометрия и ПДн

Единая биометрическая система

В конце 2021 года согласно подписанному Президентом РФ закону[49], **Единая биометрическая система получила статус государственной** информационной системы (ГИС). Поскольку система получила такой статус, на нее теперь распространяется и приказ ФСТЭК №17 от 11.02.2013 г. «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»[50]. Подробнее о нормативных актах, регулирующих обработку биометрических данных в информационных системах, включая ЕБС, раскрыто в дайджестах на сайте InfoWatch[51].

Нормативные правовые акты в отношении безопасности критической информационной инфраструктуры (КИИ) РФ

Безопасность КИИ РФ стала наиболее актуальна в феврале-марте 2022 года, и в будущем мы посвятим изменениям отдельный обзор. Перечень актуальных документов по безопасности критической информационной инфраструктуры (КИИ) доступен на сайте InfoWatch[52].

Одним из ключевых изменений в отношении безопасности КИИ за 2021 год стало введение **административной ответственности** за нарушение законодательства в

---

[47] Указ Президента Российской Федерации от 17.01.2022 № 15 «О внесении изменений в Положение о Министерстве обороны Российской Федерации, утвержденное Указом Президента Российской Федерации от 16 августа 2004 г. № 1082, и Положение о Генеральном штабе Вооруженных Сил Российской Федерации, утвержденное Указом Президента Российской Федерации от 23 июля 2013 г. № 631: http://publication.pravo.gov.ru/Document/View/0001202201170005

[48] Указ Президента Российской Федерации от 12.04.2021 № 213 «Об утверждении Основ государственной политики Российской Федерации в области международной информационной безопасности»: http://publication.pravo.gov.ru/Document/View/0001202104120050

[49] Федеральный закон от 30.12.2021 № 441-ФЗ «О внесении изменений в статью 15-3 Федерального закона «Об информации, информационных технологиях и о защите информации» и статьи 3 и 5 Федерального закона «О внесении изменений в отдельные законодательные акты Российской Федерации»: http://publication.pravo.gov.ru/Document/View/0001202112300008

[50] Приказ ФСТЭК №17 от 11.02.2013 г.: https://fstec.ru/normotvorcheskaya/akty/53-prikazy/702-prikaz-fstek-rossii-ot-11-fevralya-2013-g-n-17?highlight

[51] Минцифры установило правила работы с биометрическими данными: https://www.infowatch.ru/analytics/daydzhesty-i-obzory/mintsifry-ustanovilo-pravila-raboty-s-biometricheskimi-dannymi
Изменения, коснувшиеся Единой биометрической системы в 2022 году: https://www.infowatch.ru/analytics/daydzhesty-i-obzory/izmeneniya-kosnuvshiesya-edinoy-biometricheskoy-sistemy-v-2022-godu

[52] Актуальная документация по безопасности КИИ: https://www.infowatch.ru/analytics/daydzhesty-i-obzory/aktualnaya-dokumentatsiya-po-bezopasnosti-kii

области обеспечения безопасности критической информационной инфраструктуры Российской Федерации.

Штрафы были введены после принятия Федерального закона от 26 мая 2021 года № 141-ФЗ «О внесении изменений в Кодекс Российской Федерации об административных правонарушениях» [53].

В КоАП РФ появились следующие статьи:

- 13.12.1. Нарушение требований в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации.
- 19.7.15. Непредставление сведений, предусмотренных законодательством в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации.
- 23.90. Федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации.
- 23.91. Федеральный орган исполнительной власти, уполномоченный в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации.

Закон вступил в силу с 6 июня 2021 года, кроме части 1 статьи 13.12.1:

«Нарушение требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования либо требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации, установленных федеральными законами и принятыми в соответствии с ними иными нормативными правовыми актами Российской Федерации, если такие действия (бездействие) не содержат признаков уголовно наказуемого деяния,

- влечет наложение административного штрафа на должностных лиц в размере от десяти тысяч до пятидесяти тысяч рублей; на юридических лиц - от пятидесяти тысяч до ста тысяч рублей», которая вступила в силу с 01.09.2021 г.

Таким образом, ФСТЭК России и ФСБ России получили право штрафовать за непредоставление сведений (нарушение порядка и сроков информирования и т.п.) уже с 6 июня 2021 года.

[53] Федеральный закон от 26.05.2021 № 141-ФЗ «О внесении изменений в Кодекс Российской Федерации об административных правонарушениях» http://publication.pravo.gov.ru/Document/View/0001202105260038

Проекты нормативных правовых актов

За 2021 год всего было внесено на обсуждение 217 проектов.

Разбивку по месяцам можно увидеть в таблице ниже.

Таблица 5

Итоги:	
I квартал 2021	19
II квартал 2021	46
III квартал 2021	97
IV квартал 2021	55
Итого внесенных проектов НПА за 2021	**217**

Ситуация складывается немного иным образом по сравнению с принятыми нормативными правовыми актами: пик нормотворческой активности пришелся на 3 квартал 2021 года, тогда было внесено на обсуждение 97 актов, в то время как в 4 квартале почти вдвое меньше — 55.

Примечания

- Особенность портала проектов нормативных правовых актов https://regulation.gov.ru/ в том, что по итогам рассмотрения проекта не ставится отметок о принятии нормативного правового акта, в том числе о номере и дате, а также о названии итогового документа, в связи с чем не всегда есть возможность отследить судьбу проекта нормативного правового акта. Кроме того, у ряда проектов еще не истёк срок общественного обсуждения (вплоть до следующего года), некоторые принятые документы находятся на регистрации в Министерстве юстиции. Таким образом, однозначно сопоставить перечень проектов с принятыми актами не представляется возможным.
- Количество принятых актов превышает количество проектов НПА примерно на треть (287 принятых, 217 опубликованных для обсуждения), не все проекты НПА из приведенных выше списков приняты. На общественные обсуждения, антикоррупционную экспертизу и завершение стадии разработки уходят месяцы, поэтому сроки принятия могут выходить за рамки анализируемого периода. Например, в 2021 году также принимались проекты, которые были внесены еще в 2020.
- Иногда в процессе рассмотрения инициаторы отказываются от разработки некоторых проектов, но затем снова вносят их на обсуждение.

Рассмотрим подробнее структуру внесенных проектов нормативных правовых актов в разрезе их тем:

Таблица 6. Проекты нормативных правовых актов в области информационной безопасности и цифровой экономики, по темам

Тема проекта нормативного правового акта	Количество внесенных проектов по теме	Доля от общего количества, %
Цифровая экономика	70	32%
Информационная безопасность (ЗИ, ТЗИ), без учета актов в области КИИ	62	29%
Биометрия и персональные данные	41	19%
Лицензирование деятельности по ТЗИ и УНСИ	16	7%
Импортозамещение	11	5%
Безопасность критической информационной инфраструктуры (КИИ)	9	4%
Сертификация СЗИ и СКЗИ, аттестация объектов информатизации	2	1%
Аккредитация и экспертиза в сфере ИБ и ИТ	2	1%
Государственная тайна (перечни, поправки в законодательство и т.д.)	2	1%
Национальная безопасность	2	1%
Общий итог	**217**	**100%**

Распределение по темам проектов наглядно представлено и на рисунке ниже:

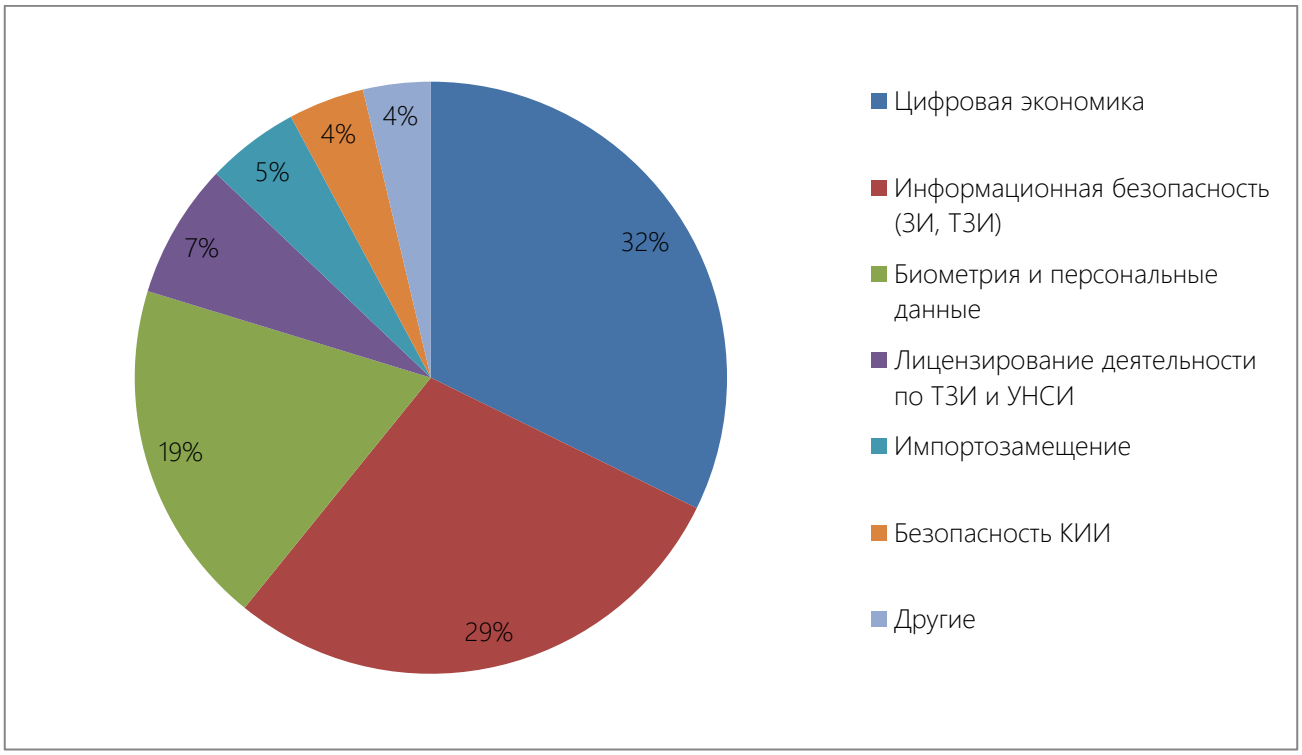

Рисунок 3. Проекты нормативных правовых актов в области информационной безопасности и цифровой экономики, по темам

Две области, **«Цифровая экономика»** и **«Информационная безопасность»** (защита информации, техническая защита информации) поделили между собой большую часть внесенных проектов нормативных правовых актов и составили почти равные доли – **32%** и **29%** соответственно. На третьем месте проекты актов в сфере **биометрии и персональных данных**, их доля составила **19%** от общего числа проектов исследуемой нами области.

Проекты в области **лицензирования деятельности по ТЗИ и УНСИ** составили **7%**, **импортозамещению** – **5%**, по **безопасности критической информационной инфраструктуры** – **4%**.

Рассмотрим, какие из министерств и ведомств были самыми активными в нормотворческой деятельности по итогам рассматриваемого периода (в части проектов НПА).

Таблица 7. Проекты нормативных правовых актов в области информационной безопасности и цифровой экономики

Министерство/ведомство	Количество внесенных на обсуждением проектов актов	Доля от общего количества, %
Минцифры России	161	74%
ФСТЭК России	21	10%
ФСБ России	15	7%
Роскомнадзор	11	5%
Минздрав России	4	2%
Минобороны России	2	1%
Другие	3	1%
Общий итог	**217**	**100%**

Распределение по министерствам и ведомствам представлено на рисунке ниже:

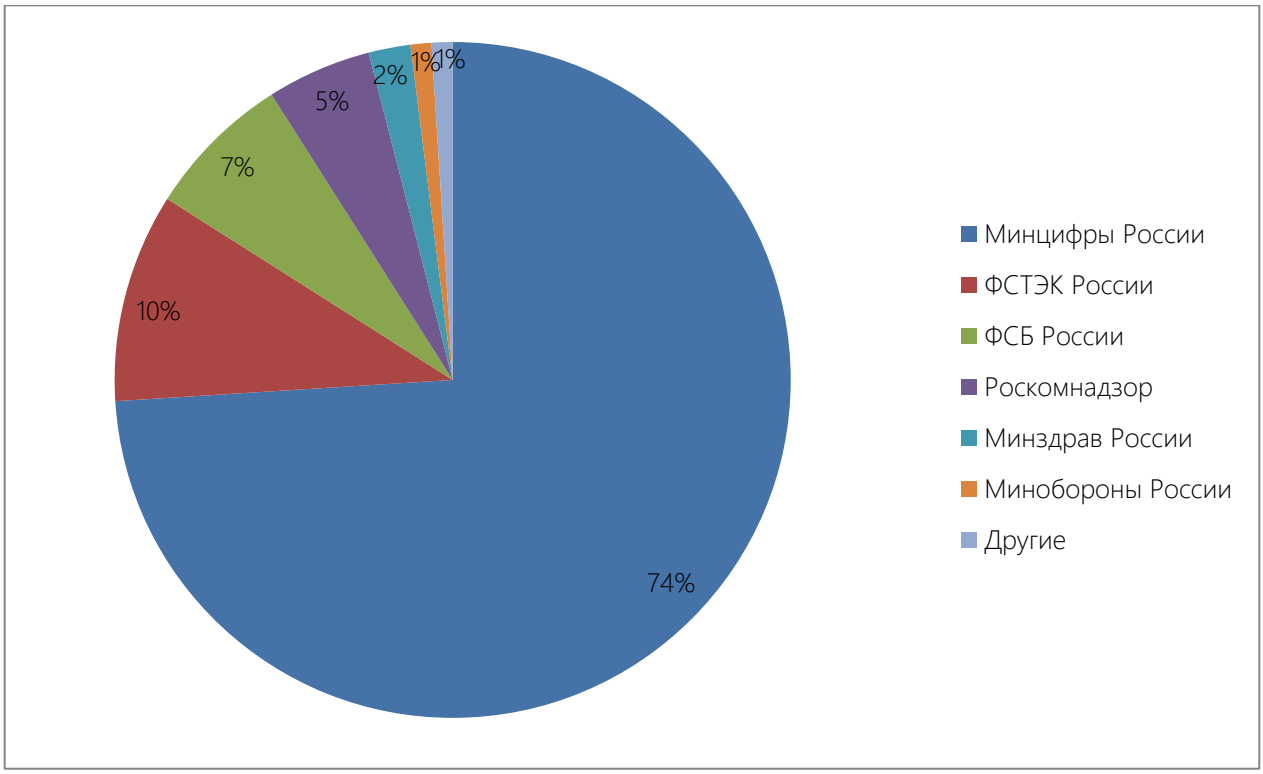

Рисунок 4. Проекты нормативных правовых актов в области информационной безопасности и цифровой экономики

Как видно, подавляющее **большинство инициатив принадлежит Министерству цифрового развития, связи и массовых коммуникаций Российской Федерации** и составляет **74%** от общего числа выдвинутых к обсуждению проектов.

Следующим по объему инициатив располагается **ФСТЭК России**, пусть и с большим отрывом, по итогам 2021 года его доля составила **10%.** Третье место занял **Роскомнадзор** с долей **7%**.

В таблице ниже можно также увидеть, по какой теме какое ведомство выступило с наибольшим количеством инициатив.

Таблица 8. Проекты нормативных правовых актов

Тема проекта нормативного правового акта и внесший его орган	Доля от общего количества проектов актов, %
Цифровая экономика	**32%**
Минцифры России	30%
Минздрав России	2%
Информационная безопасность (ЗИ, ТЗИ)	**29%**
Минцифры России	19%
Роскомнадзор	4%
ФСБ России	3%
ФСТЭК России	1%
Центральный банк России	1%
Генпрокуратура России	1%
Биометрия и персональные данные	**19%**
Минцифры России	17%
ФСБ России	1%
Другие	1%
Лицензирование деятельности по ТЗИ и УНСИ	**7%**
ФСТЭК России	6%
ФСБ России	1%
Импортозамещение	**5%**
Минцифры России	5%
Безопасность КИИ	**4%**
Минцифры России	2%
ФСТЭК России	1%
ФСБ России	1%
Сертификация СЗИ и СКЗИ, аттестация объектов информатизации	**1%**
ФСТЭК России	1%
Аккредитация и экспертиза в сфере ИБ и ИТ	**1%**
Минцифры России	1%
Государственная тайна	**1%**
ФСБ России	1%
Национальная безопасность	**1%**
Минобороны России	1%
Общий итог	**100%**

Как видно, и по каждой теме **Минцифры России** принадлежит большинство инициатив. Исключения составили только **«Лицензирование деятельности по ТЗИ»**, **«Сертификация СЗИ»,** в данных сегментах **основным инициатором выступил ФСТЭК России**, а в проектах, связанных с государственной тайной, представлена только **ФСБ России**.

По аналогии с разделом о принятых нормативных правовых актах, рассмотрим ключевые проекты по итогам 2021 года в трех сегментах: цифровая экономика, информационная безопасность и импортозамещение.

Цифровая экономика

По теме цифровой экономики на обсуждение внесена почти треть всех проектов 2021 года — 32%. В целом, большинство проектов актов по этой теме связаны с функционированием портала «Госуслуги», а также с внесением незначительных изменений в уже существующие нормативные акты.

1. В 2021 году был внесен Проект постановления Правительства Российской Федерации о внесении изменений в Положение о Министерстве цифрового развития, связи и массовых коммуникаций Российской Федерации, утвержденное постановлением Правительства Российской Федерации от 02.06.2002 № 418[54].

Проект постановления предусматривает **наделение Минцифры России полномочиями для определения требований к технологиям взаимодействия средств информатизации, реализующих российские криптографические алгоритмы с иными средствами информатизации.** По мнению авторов проекта, наделение Минцифры России данными полномочиями позволит обеспечить реализацию поэтапного перехода на использование российских криптографических алгоритмов и средств шифрования.

Проект **постановления** также **предусматривает внесение в Положение изменений, определяющих участие Минцифры России в пределах своей компетенции в разработке и реализации основных направлений государственной политики Российской Федерации в области международной информационной безопасности.**

Основанием для внесения указанного изменения являются пункт 5 протокола заседания Совета Безопасности Российской Федерации от 26 марта 2021 г. и Основы государственной политики Российской Федерации в области международной информационной безопасности, утвержденные Указом Президента Российской Федерации от 12 апреля 2021 № 213.

На портале отсутствует информация о результатах рассмотрения данного проекта, однако в конце года вышло Постановление Правительства от 31.12.2021, определяющее участие Минцифры России в реализации государственной политики в области международной информационной безопасности.

2. Проект постановления «О государственной информационной системе «**Типовое облачное решение системы электронного документооборота»**[55]

ГИС **создается в целях обеспечения** посредством использования информационно-телекоммуникационных технологий **процессов делопроизводства и**

[54] О внесении изменений в Положение о Министерстве цифрового развития, связи и массовых коммуникаций Российской Федерации: https://regulation.gov.ru/projects/List/AdvancedSearch#npa=115344

[55] О государственной информационной системе «Типовое облачное решение системы электронного документооборота»: https://regulation.gov.ru/projects/List/AdvancedSearch#npa=116601

документооборота при осуществлении полномочий государственными органами, органами местного самоуправления, государственными и муниципальными учреждениями, некоммерческими организациями, созданными для выполнения задач, поставленных перед Правительством Российской Федерации, **не имеющими собственных систем электронного документооборота либо обладающими системами электронного документооборота, нуждающимися в развитии**.

Оператор обеспечивает:

г) **соблюдение требований информационной безопасности**, в том числе защиту данных, размещенных в государственной информационной системе.

Для обеспечения защиты информации в ходе создания, эксплуатации и развития государственной информационной системы осуществляются:

а) формирование требований к защите информации, содержащейся в государственной информационной системе;

б) применение сертифицированных по требованиям безопасности информации средств защиты информации;

в) защита информации при ее передаче по информационно-телекоммуникационным сетям.

При создании и развитии государственной информационной системы должны использоваться программно-технические средства, приобретенные с учетом требований и особенностей нормативных правовых актов, направленных на применение национального режима при осуществлении закупок.

Технические средства, используемые при эксплуатации государственной информационной системы, **должны размещаться на территории Российской Федерации.**

Технические и программные средства государственной информационной системы обеспечивают:

а) **защиту информации**, содержащейся в государственной информационной системе, в том числе от копирования, распространения, уничтожения, модификации и блокирования доступа к ней, а также от иных неправомерных действий;

б) **применение усиленной квалифицированной электронной подписи** при подписании электронных документов, а также возможность проверки такой электронной подписи на протяжении всего срока хранения документов средствами государственной информационной системы;

в) возможность использования усиленной неквалифицированной электронной подписи, сертификат ключа проверки которой создан и используется в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме, в установленном Правительством Российской Федерации порядке.

г) идентификацию, аутентификацию и авторизацию пользователей, осуществляющих формирование, размещение, изменение и удаление информации, содержащейся в государственной информационной системе;

д) ведение электронных журналов учета операций, выполненных с помощью технических и программных средств, позволяющих обеспечивать учет всех действий по размещению, изменению и удалению информации, фиксировать точное время, содержание изменений и сведения о лицах, осуществивших изменения;

е) ежедневное копирование информации и электронных журналов учета операций на резервный материальный носитель, обеспечивающий возможность восстановления указанной информации;

ж) хранение резервных копий информации и электронных журналов учета операций, полученных в результате ежедневного копирования, в течение 30 календарных дней.

Пользователи государственной информационной системы (ГИС) самостоятельно обеспечивают соответствие автоматизированных рабочих мест, с которых происходит подключение к ГИС, и информационных систем, в состав которых входят указанные автоматизированные рабочие места, требованиям, установленным законодательством Российской Федерации о защите информации, в зависимости от классификации информационных систем и автоматизированных рабочих мест по требованиям безопасности информации.

Для обеспечения защиты информации при ее передаче между автоматизированными рабочими местами и государственной информационной системой на автоматизированных рабочих местах должны применяться программные средства криптографической защиты информации, совместимые со средствами криптографической защиты информации из состава государственной информационной системы и поддерживающие протокол защиты транспортного уровня с использованием российских криптографических алгоритмов.

Для обеспечения возможности формирования и проверки квалифицированной электронной подписи при использовании государственной информационной системы на автоматизированных рабочих местах должны применяться средства электронной подписи, соответствующие требованиям приказа Федеральной службы безопасности Российской Федерации от 27 декабря 2011 г. № 796 «Об утверждении Требований к средствам электронной подписи и Требований к средствам удостоверяющего центра», совместимые с государственной информационной системой и сертифицированные в установленном порядке в системе сертификации Федеральной службы безопасности Российской Федерации.

Общественное обсуждение и антикоррупционная экспертиза проекта должны были закончиться в июне 2021 года, больше обновлений по нему пока не публиковалось, аналогов среди принятых нормативных правовых актов не обнаружено.

3. Проект «Об утверждении **Порядка ведения перечня отечественных социально значимых информационных ресурсов** и о внесении изменений в

Постановление Правительства Российской Федерации от 28 мая 2020 г. № 770»[56].

В связи с событиями февраля-марта 2022 года, уделяется особое внимание безопасности к обеспечению доступа к публичным и социально значимым ресурсам, о чем выпущена соответствующая правительственная телеграмма.

Предлагаемый документ определяет порядок ведения перечня отечественных социально значимых информационных ресурсов, при доступе к которым услуги связи по передаче данных и по предоставлению доступа к информационно-телекоммуникационной сети «Интернет» могут оказываться абоненту-гражданину Российской Федерации без взимания платы;

В Перечень включаются следующие информационные ресурсы:

- официальные сайты государственных органов и органов местного самоуправления, размещенные в российском государственном сегменте информационно-телекоммуникационной сети «Интернет»;
- официальные сайты государственных внебюджетных фондов Российской Федерации в информационно-телекоммуникационной сети «Интернет»;
- порталы государственных и муниципальных услуг;
- иные информационные ресурсы, имеющие социальную значимость, в том числе направленные на духовно-нравственное воспитание молодого поколения и формирование культуры безопасного пользования информационно-телекоммуникационной сетью «Интернет».

Информационные ресурсы включаются в Перечень при условии соответствия одного из следующих критериев:

- **технические и программные средства**, используемые для размещения и обеспечения функционирования информационного ресурса, **располагаются на территории Российской Федерации;**

Информационная безопасность

По данной теме в 2021 году опубликовано 29% от всех внесенных на обсуждение инициатив (проектов НПА). Множество проектов связанно с электронными подписями, а также с иностранными лицами, действующими на территории Российской Федерации.

Например, подобный проект закона опубликовала ФСБ России, согласно которому иностранным юридическим лицам запрещено осуществлять отдельные виды деятельности в области информационной безопасности, отнесенные к компетенциям ФСБ России и ФСТЭК России. Подробнее о нем было рассмотрено в обзоре на сайте

[56] Об утверждении Порядка ведения перечня отечественных социально значимых информационных ресурсов и о внесении изменений в Постановление Правительства Российской Федерации от 28 мая 2020 г. № 770: https://regulation.gov.ru/projects/List/AdvancedSearch#npa=122114

InfoWatch[57]. В результате с 1 марта 2022 года все иностранные физические лица не могут вести деятельность в сфере ИБ, лицензируемые ФСБ России и ФСТЭК России[58].

1. ФСТЭК России опубликовала проект о внесении изменений в статью 16 Федерального закона об информации, информационных технологиях и о защите информации. Законопроект направлен на **установление требований о защите информации, обладателями которой являются государственные органы, вне зависимости от места ее хранения или обработки[59].**

На текущий момент государственные органы поручают обработку информации, обладателями которой они являются, подведомственным организациям, коммерческим организациям, информационные системы которых не относятся к государственным.

Создание подобных информационных систем осуществляется без учета требований о защите информации, установленных в соответствии с частью 5 статьи 16 Закона № 149-ФЗ, что приводит к снижению уровня защищенности информации, являющейся государственным информационным ресурсом.

Предлагаемыми изменениями устанавливается обязанность соблюдения требований о защите информации, обладателями которой являются государственные органы, вне зависимости от места ее хранения или обработки, а также требований к организации и управлению системой защиты информации.

Документ получил положительное заключение по итогам процедуры ОРВ, однако нет ссылок и отметок, что был принят.

2. **Закрепление в законодательстве понятия «ГосОблако».** Опубликован проект[60] Федерального закона «О внесении изменений в Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» разработан в целях закрепления в законодательстве понятия государственной единой облачной платформы (ГосОблако).

Авторы проекта предлагают ввести в правовое поле определение «ГосОблако», и это позволит обеспечить совершенствование правового и технологического регулирования, в том числе направленного на повышение уровня защиты и доступности данных.

ГосОблако является основным проектом «ГосТеха», поэтому для дополнительной информации см. материалы по «Гостеху».

---

[57] Иностранные компании в сфере ИБ останутся без лицензий: https://www.infowatch.ru/analytics/novosti-ib/inostrannye-kompanii-v-sfere-ib-ostanutsya-bez-litsenziy

[58] Постановление Правительства Российской Федерации от 28.12.2021 № 2518 «О внесении изменений в некоторые акты Правительства Российской Федерации по вопросам лицензирования отдельных видов деятельности и признании утратившим силу отдельного положения акта Правительства Российской Федерации»: http://publication.pravo.gov.ru/Document/View/0001202112300215

[59] Проект о внесении изменений в статью 16 Федерального закона об информации, информационных технологиях и о защите информации: https://regulation.gov.ru/projects/List/AdvancedSearch#npa=120094

[60] Проект Федерального закона «О внесении изменений в Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»: https://regulation.gov.ru/projects/List/AdvancedSearch#npa=122604

3. **Кибергигиена.** Опубликован проект постановления Правительства РФ «Об утверждении Правил предоставления субсидий из федерального бюджета российскому юридическому лицу на разработку и реализацию на регулярной основе программы кибергигиены и повышения грамотности широких слоев населения по вопросам информационной безопасности».

Субсидия предоставляется в рамках реализации федерального проекта «Информационная безопасность» национальной программы «Цифровая экономика Российской Федерации».

Субсидия предоставляется для реализации следующих мероприятий:

1) разработка и актуализация программы кибергигиены;

2) разработка информационных (аудиовизуальных и иных) материалов для повышения осведомленности широких слоев населения в рамках программы кибергигиены;

3) разработка, реализация и поддержание функционирования сервиса повышения уровня знаний в области кибергигиены и грамотности по вопросам информационной безопасности в формате web-портала и его функциональных элементов;

4) разработка плана и проведение информационной кампании (в том числе новостные публикации, промо-компании на социально значимых ресурсах, информационные материалы для формирования на внутренних порталах и ресурсах государственных органов, познавательно-развлекательный контент в различных формах (игровых, практико-обучающих сервисов, видеороликов), проведение круглых столов и вебинаров для государственных гражданских служащих);

5) разработка и актуализация методологии мониторинга уровня знаний в области кибергигиены и грамотности по вопросам информационной безопасности, проведение мониторинга.

Документ был принят 04.02.2022.

Импортозамещение

В области импортозамещения опубликовано 5% от всех внесенных на обсуждение законодательных инициатив.

Разработаны проекты изменений в постановления Правительства РФ:

1. Проект изменений в постановление Правительства РФ **«О предоставлении субсидий из федерального бюджета Российскому фонду развития информационных технологий на поддержку проектов по разработке и внедрению российских решений** в сфере информационных технологий, утвержденные постановлением Правительства Российской Федерации от 3 мая 2019 г. № 550 «Об утверждении Правил предоставления субсидии из федерального бюджета Российскому фонду развития информационных технологий на поддержку проектов по разработке и внедрению российских решений в сфере информационных технологий» (Собрание законодательства

Российской Федерации, 2019, № 19, ст. 2306; 2019, № 37, ст. 5171; 2021, № 18, ст. 3153)[61].

2. Проект изменений в постановление Правительства РФ **«О Центре компетенций по импортозамещению в сфере информационно-коммуникационных технологий»**[62].

Авторами предлагается создать при участии Государственной корпорации по содействию разработке, производству и экспорту высокотехнологичной промышленной продукции «Ростех» и Государственной корпорации по атомной энергии «Росатом» Центр компетенций по новым производственным технологиям, к полномочиям которого относятся:

- разработка актуальной системы целевых показателей и методики их расчета в соответствии с планом мероприятий дорожной карты по развитию высокотехнологичной области «Новые производственные технологии» (далее – ДК НПТ) в целях развития российского промышленного программного обеспечения (ППО), на основе анализа российского и зарубежного рынков, включая расчет интегрального показателя, отражающего уровень развития технологий промышленного ПО (НПТ) - индекс технологической независимости в области промышленного ПО;
- разработка предложений по новым механизмам поддержки проектов внедрения и сопровождения отечественного ППО, на основе передового зарубежного опыта;
- разработка перечня технологий ППО высокой степени готовности и актуализация перечня ключевых технологических задач;
- реализация организационно-методологических функций по развитию высокотехнологичной области «Новые производственные технологии» и выполнению мероприятий ДК НПТ».

3. Проект изменений в постановление Правительства Российской Федерации от 3 декабря 2020 г. № 2014 **«О минимальной обязательной доле закупок российских товаров и ее достижении заказчиком»**[63] (Собрание законодательства Российской Федерации, 2020, № 50, ст. 8220) касательно закупки радиоэлектронной продукции иностранного происхождения при закупках работ и услуг.

---

[61] Проект постановления Правительства РФ «О предоставлении субсидий из федерального бюджета Российскому фонду развития информационных технологий на поддержку проектов по разработке и внедрению российских решений в сфере информационных технологий, утвержденные постановлением Правительства Российской Федерации от 3 мая 2019 г. № 550 «Об утверждении Правил предоставления субсидии из федерального бюджета Российскому фонду развития информационных технологий на поддержку проектов по разработке и внедрению российских решений в сфере информационных технологий»: https://regulation.gov.ru/projects/List/AdvancedSearch#npa=122289

[62] Проект изменений в постановление Правительства РФ «О Центре компетенций по импортозамещению в сфере информационно-коммуникационных технологий: https://regulation.gov.ru/projects/List/AdvancedSearch#npa=121104

[63] Проект изменений в постановление Правительства Российской Федерации от 3 декабря 2020 г. № 2014 «О минимальной обязательной доле закупок российских товаров и ее достижении заказчиком»: https://regulation.gov.ru/projects/List/AdvancedSearch#npa=117562

Постановление предлагается дополнить пунктами следующего содержания:

«2 (1). Для целей настоящего постановления в части радиоэлектронной продукции, используемой при выполнении работ, оказании услуг, под контрактами понимаются:

а) контракты на оказание услуг или выполнение работ, в результате исполнения которых заказчику передается на любой срок право владения и пользования радиоэлектронной продукцией;

б) контракты на оказание услуг или выполнение работ, в результате исполнения которых право владения на радиоэлектронную продукцию заказчику не передаются, но исполнение которых технологически может быть осуществлено только при условии передачи заказчику права пользования этой радиоэлектронной продукции.

2 (2). Контракты, указанные в подпункте «а» пункта 2(1), включают в себя:

а) контракты на разработку и (или) изготовление, а также модернизацию радиоэлектронной продукции обособленно или в составе сложных вещей (программно-аппаратного комплекса, автоматизированной системы управления, сетевой или иной инфраструктуры информационно-коммуникационных технологий заказчика);

б) контракты по предоставлению радиоэлектронной продукции обособленно или в составе сложных вещей в аренду, лизинг, в пользование, в том числе контракты на оказание услуг по изготовлению твердых копий электронных документов (сервис-печати).

Можно ожидать, что данный проект должен быть также гармонизирован с Указом Президента РФ от 30.03.2022 года.

4. Проект постановления Правительства Российской Федерации «О внесении изменений в акты Правительства Российской Федерации» в **целях содействия развитию в Российской Федерации радиоэлектронной отрасли и связанной с ней отрасли создания и внедрения программного обеспечения[64].**

Для обеспечения единообразия регулирования и в целях содействия разработчикам **нормативных правовых актов** при формулировании ими положений, **регулирующих вопросы рынка радиоэлектронной продукции и программного обеспечения**, проектом постановления Правительства Российской Федерации предусматривается обязательность направления таких проектов нормативных правовых актов на согласование в Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации и Министерство промышленности и торговли Российской Федерации.

Для предотвращения затягивания процедуры согласования проектов актов Правительства Российской Федерации, которыми предусматриваются основания и порядок предоставления субсидий из средств федерального бюджета, проектом

[64] Проект «О внесении изменений в акты Правительства Российской Федерации»: https://regulation.gov.ru/projects/List/AdvancedSearch#npa=116860

постановления Правительства Российской Федерации предусматривается сокращенный пятидневный срок представления по ним позиции, а при непредставлении позиции в указанный срок проект нормативного правового акта считается согласованным.

5. **Проект постановления Правительства РФ о создании Реестра секретов производства (ноу-хау), непосредственно связанные с обеспечением обороны и безопасности**, подлежат учету в Реестре результатов интеллектуальной деятельности, **непосредственно связанных с обеспечением обороны и безопасности**[65].

Как пишут авторы проекта, в настоящее время в Российской Федерации учет и регистрация секретов производства (ноу-хау) не предусмотрены.

Организация учета секретов производства (ноу-хау) позволит подтвердить исключительные права Российской Федерации на секреты производства (ноу-хау).

Объектами учета в Реестре являются секреты производства (ноу-хау), непосредственно связанные с обеспечением обороны и безопасности, а именно:

- полученные в рамках государственных программ или при выполнении государственного оборонного заказа, осуществление которых обеспечивает федеральный орган исполнительной власти, уполномоченный в области обороны;
- являющиеся собственными разработками уполномоченного органа или подведомственных ему государственных учреждений;
- приобретенные уполномоченным органом или подведомственными учреждениями по договорам отчуждения.

Реестр будет являться федеральной информационной системой и должен будет обеспечивать возможность формирования и выдачу информации по запросу заинтересованных лиц для использования ее в целях обеспечения деятельности исполнителей при выполнении государственных контрактов, государственных заказчиков государственного оборонного заказа, обеспечения возможности передачи прав Российской Федерации предприятиям оборонно-промышленного комплекса, в том числе и на безвозмездной основе по решению Президента Российской Федерации.

Другие проекты нормативных правовых актов

Генеральная прокуратура 28.07.2021 внесла в ООН проект конвенции о противодействии использования информационно-коммуникационных технологий в преступных целях. Предложено дополнить законы новыми составами преступлений, таким образом, их станет 23 вместо 9, в том числе инициатива включила несанкционированный доступ к персональным данным, неправомерный

[65] Проект постановления Правительства РФ о создании Реестра секретов производства (ноу-хау), непосредственно связанные с обеспечением обороны и безопасности: https://regulation.gov.ru/projects/List/AdvancedSearch#npa=119513

доступ, воздействие и перехват цифровой информации, неправомерное воздействие на критическую информационную инфраструктуру, создание и использование цифровой информации для введения пользователя в заблуждение.

В предлагаемом варианте конвенции также предлагается порядок взаимодействия государств в вопросах выдачи киберпреступников и оказания правовой помощи по уголовным делам. Россия также предлагает создать новый механизм под эгидой ООН - Международную техническую комиссию.

Документ находится на стадии обсуждения и пока планируется к принятию в 2023 году.

Проекты с отрицательными заключениями

1. Проект «О внесении изменений в Правила установки, эксплуатации и о модернизации в сети связи оператора связи технических средств **противодействия угрозам устойчивости, безопасности и целостности функционирования** на территории российской федерации информационно-телекоммуникационной сети «Интернет» и сети связи общего пользования, утвержденные постановлением Правительства Российской Федерации от 12 февраля 2020 года № 126[66].

Согласно проекту, предлагается обязать операторов связи ежегодно не позднее 4 квартала текущего года для формировать план мероприятий по установке, эксплуатации и модернизации технических средств противодействия угрозам (ТСПУ) направлять в адрес радиочастотной службы планы на следующий год по модернизации, реконструкции сети связи, ликвидации фрагмента сети связи, где установлены или планируется установка ТСПУ.

Предлагалось также конкретизировать, что обеспечение доступа радиочастотной службы к ТСПУ должно быть своевременным и беспрепятственным.

Документ получил отрицательное заключение по итогам процедуры ОРВ (оценки регулирующего воздействия), однако будем следить, какой документ появится в свете последних событий.

2. Проект в области импортозамещения «О внесении изменений в постановление Правительства Российской Федерации от 18.11.2020 № 1867»[67].

Проектом постановления предусматриваются следующие изменения:

- конкретизируются положения, в соответствии с которыми правообладатели программ из государств – членов Евразийского экономического союза могут участвовать в отборе программ для включения в перечень программ, которые должны быть предварительно установлены на отдельные виды технически сложных товаров (далее – перечень программ);

[66] https://regulation.gov.ru/projects/List/AdvancedSearch#npa=116428
[67] https://regulation.gov.ru/projects/List/AdvancedSearch#npa=115423

- устанавливаются требования к поисковой системе, страной происхождения которой является Российская Федерация или другие государства - члены Евразийского экономического союза, которая должна использоваться по умолчанию;
- устанавливается порядок определения такой поисковой системы, а также порядок реализации возможности использования поисковой системы по умолчанию;
- уточнены наименования классов программ, которые могут быть предварительно установлены на технически сложные товары, а также предусмотрен новый класс – «программы, обеспечивающие доступ к электронным книгам»;
- дополняется информация, которая должна быть указана в перечне программ (должны указываться ссылки в сети «Интернет» и в магазинах приложений на установочные файлы программ, а также операционная система технически сложного товара, на который должна осуществляется предварительная установка программы);
- уточнено требование о наличии программы в магазине приложений (данное требование будет обязательным только для программ, которые устанавливаются на смартфоны, планшеты и телевизоры с цифровым блоком управления);
- уточнены требования правил предварительной установки программ на технически сложные товары в части недискриминационного отображения на экране устройств по отношению к иным установленным программам.

По итогам процедуры ОРВ было также выпущено отрицательное заключение.

Выводы

1. За 2021 год было исследовано более 10 000 нормативных правовых актов и их проектов, и отобрано более 500 актов, которые относятся к области информационной безопасности, средств защиты информации, персональных данных, импортозамещения в сфере ИТ, цифровой экономики в целом.
2. За 2021 год в исследуемой сфере было принято 287 нормативных правовых актов и внесено на обсуждение 217 проектов НПА.
3. Нормотворческая активность в течение года шла по нарастающей, и самый активный период пришелся на 4 квартал 2021 года.
4. Почти половина принятых нормативных правовых актов касается цифровой экономики – 44% от общего числа. По теме информационной безопасности (защиты информации, технической защиты информации), без учета актов в области безопасности КИИ – 16%, по теме биометрии и персональных данных – 18%. В области импортозамещения и безопасности критической информационной инфраструктуры количество принятых нормативных правовых актов составило 6% и 3% соответственно.
5. Подавляющее число принятых нормативных правовых актов относится на долю Правительства РФ и составляет 65%.
6. Сферы «Информационная безопасность» (защита информации, техническая защита информации) и «Цифровая экономика» поделили между собой большую часть внесенных проектов нормативных правовых актов и составили почти равные доли – 32% и 29% соответственно. На тему биометрии и персональных данных пришлось 19% от всех предложенных инициатив. Проекты в области безопасности критической информационной инфраструктуры составили 4%, импортозамещения – 5%, лицензирования деятельности по ТЗИ и УНСИ – по 7%.
7. Количество принятых актов превышает количество проектов НПА примерно на треть (287 принятых, 217 опубликованных для обсуждения), не все проекты НПА из приведенных выше списков приняты. На общественные обсуждения, антикоррупционную экспертизу и завершение стадии разработки уходят месяцы, а регистрация нормативного правового акта в Минюсте может длиться до 6 месяцев, поэтому сроки принятия могут выходить за рамки анализируемого периода. Например, в 2021 году также принимались проекты, которые были внесены еще в 2020.
8. Деление на группы «Цифровая экономика», «Импортозамещение» или «Информационная безопасность» достаточно условны. Исследование показало, даже если законодательные акты относятся к цифровизации отраслей, все они так или иначе тесно связаны с процессами импортозамещения и учитывают (или должны учитывать) вопросы информационной безопасности, поскольку все новые системы являются и новыми объектами защиты. Ту же самую тенденцию мы видим и в проектах нормативных актов.
9. В течение и, особенно, к концу 2021 года было принято порядка десяти актов в области цифровой трансформации отраслей. С одной стороны, документы имеют схожую структуру в части описания решаемых проблем и целей цифровизации. С

другой стороны, каждый из них составлен по-разному, и в каждом по-своему формулируются и учитываются меры по информационной безопасности и импортозамещению. Однако одно можно сказать точно - в большинстве стратегий и концепциях уделено внимание импортозамещению и ИБ, а также признаны их неоспоримые приоритеты при реализации стратегий и концепций цифровизации.

10. Несмотря на то, что принятых актов и инициатив по импортозамещению, на первый взгляд, не так много, все акты и их проекты носят все более жесткий характер. Даже при возможности все еще закупать, например, иностранное программное обеспечение (при условии, что альтернатив отечественного ПО нет), каждый новый принятый законодательный акт заметно сужает данные возможности. В свете принятых нормативных правовых актов 2022 года перевод полностью на российское ПО значимых объектов критической информационной инфраструктуры должен завершиться к 2025 году.
11. Параллельно выходят акты и проекты НПА о поощрении разработки отечественных решений и продуктов (например, гранты в рамках Российского фонда развития ИТ).
12. Ужесточается контроль деятельности иностранных компаний на территории Российской Федерации. Например, вышли законодательные акты для регламентирования работы социальных сетей, принятые для контроля распространяемой в них информации и удаления той, которая нарушает законы РФ. Также запрещена деятельность иностранных компаний в тех лицензируемых областях информационной безопасности, которые относятся к ведению ФСБ России и ФСТЭК России.
13. События февраля-марта 2022 уже дали толчок для введения новых стимулирующих мер для развития ИТ-отрасли и поставили ребром вопрос обеспечения безопасности и независимости страны в сфере ИТ (особенно в части обеспечения безопасности КИИ, где фактически делают обязательным переход на отечественное ПО).

Мониторинг утечек на сайте InfoWatch

На сайте Экспертно-аналитического центра InfoWatch регулярно публикуются отчеты по утечкам информации и самые громкие инциденты с комментариями экспертов InfoWatch.

Следите за новостями утечек, новыми отчетами, аналитическими и популярными статьями на наших каналах:

- Почтовая рассылка
- VK
- Telegram

Экспертно-аналитический центр InfoWatch

www.infowatch.ru/analytics

© InfoWatch

Полное воспроизведение, опубликование материалов запрещено.

Цитирование возможно только при указании ссылки на источник.