Мониторинг международных трендов правового регулирования для развития законодательства в сфере цифровой экономики в России

ЕС против крупных платформ, регулирование деятельности брокеров данных, постквантовая криптография для кибербезопасности

Мониторинг № 8 (Август 2024)

Monitoring was prepared by a team of experts of the Gaidar Institute for Economic Policy (the Gaidar Institute):
Antonina Levashenko, Senior Researcher, International Best Practices Analysis Department, Gaidar Institute.
Maria Girich, Researcher, International Best Practices Analysis Department, Gaidar Institute.
Ivan Ermokhin, Researcher, International Best Practices Analysis Department, Gaidar Institute.
O. Magomedova, Researcher, International Best Practices Analysis Department, Gaidar Institute.
Tatiana Malinina, Senior Researcher, International Best Practices Analysis Department, Gaidar Institute

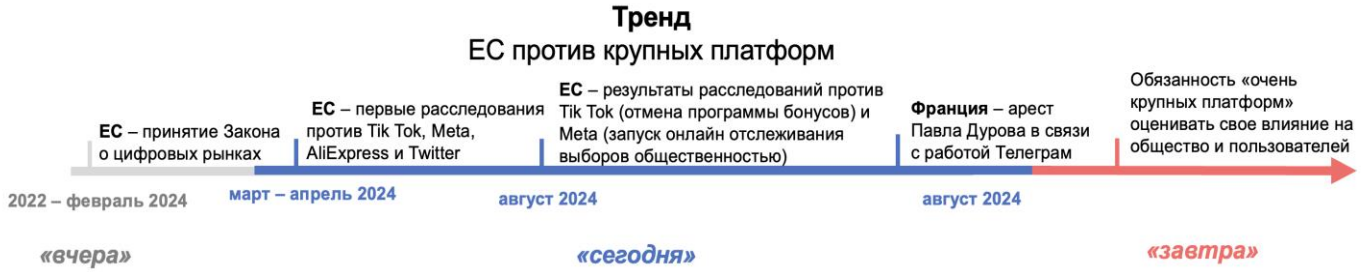
«Август плодовит во всех отношениях».

А. Чехов

В августе 2024 г. можно выделить 3 события, которые определяют тренды развития регулирования цифровой экономики в мире.

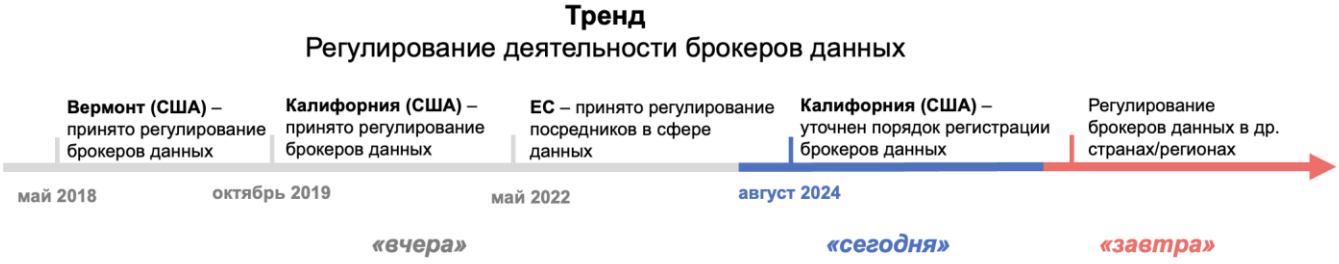
Тренд № 1. ЕС против крупных платформ

В августе 2024 г. Еврокомиссия опубликовала некоторые результаты расследования против «очень крупных платформ» Meta[1] и TikTok в части нарушения Закона ЕС о цифровых рынках (DSA). Кроме того, во Франции был арестован Павел Дуров – основатель Телеграм – по обвинению в создании социальной сети для незаконных целей. Многие обвинения коррелируют с нормами, установленными для платформ в законодательстве ЕС. При этом Телеграм, работая в пространстве ЕС, пока еще не подпадает под регулирование «очень крупных платформ», однако рост числа пользователей заставит Телеграм выполнять эти нормы в ближайшее время.



Тренд №2. Регулирование деятельности брокеров данных

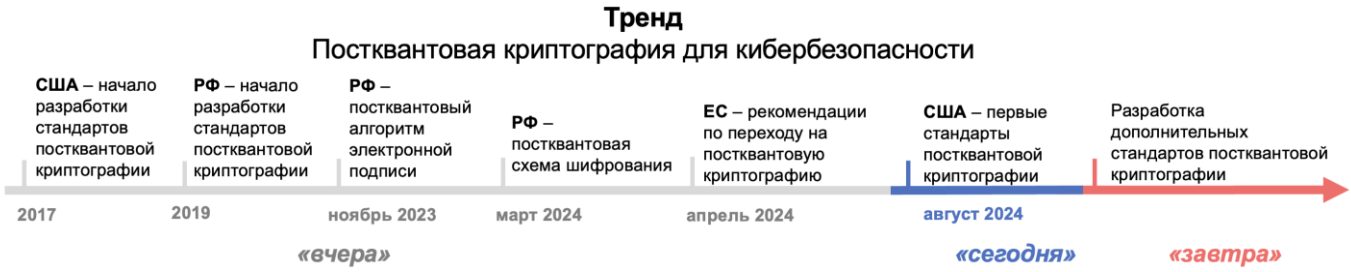
В августе 2024 г. в Калифорнии (США) подготовлены разъяснения по уточнению критериев признания компании брокером данных: например, если компания продает данные своих работников, полученные не напрямую от них. В цифровой экономике брокеры данных, выполняя посреднические функции между держателями и пользователями данных, способствуют росту их оборота, снижая издержки и повышая доверие участников рынка. В последние годы регулирование брокеров данных принято в ЕС и ряде штатов США. В России такое регулирование брокеров отсутствует, что тормозит развитие рынка данных.



Тренд №3. Постквантовая криптография для кибербезопасности

В августе 2024 г. в США вступили в силу 3 стандарта, определяющие схемы установления ключей для шифрования информации и цифровой подписи, разработанные для противостояния будущим атакам квантовых компьютеров. Считается, что текущие стандарты криптографии (шифрования) могут оказаться бессильными. В России с 2019 г. также разрабатываются, но пока не утверждены стандарты постквантовой криптографии. Страны ЕС пока полагаются на стандарты постквантовой криптографии, разработанные в 2024 г. в США.

[1] Компания Meta, запрещенная на территории Российской Федерации, включена в Перечень организаций и физических лиц, в отношении которых имеются сведения об их причастности к экстремистской деятельности или терроризму.



В августе 2024 г. в России произошло 2 значимых события:

1. Регулирование майнинга криптовалют

В августе 2024 г. был принят Федеральный закон, направленный на создание правовых основ регулирования деятельности, связанной с майнингом, который вступает в силу 1 ноября 2024 г.[2] Майнинг – это деятельность по проведению математических вычислений путем эксплуатации оборудования средств для внесения записей в информационную систему, использующую технологии распределенного реестра как блокчейн, для выпуска криптовалют и получения дохода в криптовалюте за подтверждение записей в информационной системе.

Предложено следующее регулирование майнинга:

1) майнингом могут заниматься ИП и юридические лица при регистрации в реестре лиц, осуществляющих майнинг цифровой валюты, а также физические лица – без необходимости включения в реестр, но при соблюдении лимитов энергопотребления. Возможно создание майнинг-пула, т.е. объединения майнинговых мощностей нескольких майнеров;.

2) майнеры, включенные в реестр, должны будут соблюдать законодательство о противодействии отмыванию денег и финансированию терроризма (например, об идентификации клиентов), в противном случае майнер исключается из реестра;

3) майнеры обязаны отчитываться о всей цифровой валюте, полученной в результате майнинга – указывать адрес-идентификатор[3], на который зачислена такая валюта;

4) правительство может ограничивать майнинг в отдельных субъектах Федерации или на отдельных территориях России. Это, с одной стороны, позволит сокращать риски энергодефицита в некоторых регионах (например, на Дальнем Востоке), с другой – может наносить ущерб майнерам, которые понесут затраты на перенос деятельности в другие регионы.

Таким образом, закон создает правовой режим для осуществления майнинга, не устанавливая значимых ограничений.

Кроме того, принято еще 2 важных обновлений:

1) запрет любого предложения о покупке цифровых валют неограниченному кругу лиц. Фактически усилен запрет на продажу криптовалют (ранее запрет действовал только в отношении покупки товаров или услуг за криптовалюту);

2) допуск иностранных ЦФА (цифровые финансовые активы) и иностранных участников рынка ЦФА в Россию:

- введена категория иностранных цифровых прав, что фактически дает доступ на российский рынок ЦФА, выпущенных за рубежом. Однако установлено ограничение на покупку иностранных ЦФА российскими физическими лицами – покупать могут только ИП или юридические лица. Доступ на российских рынок иностранных ЦФА обеспечивается через операторов выпуска ЦФА, которые должны квалифицировать иностранный актив в качестве ЦФА;

[2] https://sozd.duma.gov.ru/bill/237585-8

[3] Уникальная последовательность символов, предназначенная для учета в информационной системе приходных и расходных операций с цифровой валютой.

- возможность зачисления российских ЦФА иностранными покупателями в соответствии с их правом, а не российским. Это фактически позволяет передавать российские ЦФА на хранение за рубеж, при этом держатели таких ЦФА могут выполнять все действия, связанные с ЦФА в интересах своих клиентов. Иностранные участники могут покупать, хранить и далее продавать за рубежом выпущенные в России ЦФА.

Создана возможность как для продажи российских ЦФА за рубежом, так и для торговли иностранными ЦФА в России.

2. Усиление надзора за онлайн-контентом

В августе 2024 г. были приняты поправки в ФЗ «Об информации»[4] с целью противодействия распространению деструктивного контента:

1) социальные сети должны осуществлять мониторинг в отношении нового вида запрещенной информации, оскорбляющей «общественную нравственность и выражающей явное неуважение к обществу, содержащей изображение противоправных действий» и распространяемой «из хулиганских, корыстных или иных низменных побуждений». Однако по каким критериям искать такую информацию в потоке онлайн-контента в соцсетях не ясно – как выглядит «безнравственный и оскорбительный контент»? Непонятно как оценивать «низменные побуждения» для квалификации контента как противоправного?

2) доступ к информации может ограничиваться не только федеральными законами, но и актами президента России, что упрощает введение новых запретов на информацию. Указанные выше типы информации также подпадают под внесудебную блокировку сайта (по инициативе Роскомнадзора);

3) Роскомнадзор наделяется новыми полномочиями по управлению сетями связи через специальные технические средства, которые операторы связи обязуются установить. Роскомнадзор получает возможность прямого контроля за информацией, проходящей через сеть, и принимать меры (например, блокировать страницы с незаконным контентом). Такие полномочия возникают при обращении генпрокурора по факту выявления массового или неоднократного распространения противоправной информации в сети.

Новое регулирование поддерживает заданный тренд на ужесточение регулирования в сфере информации в двух аспектах. Во-первых, в расширении спектра сведений, в отношении которых требуется принимать меры по блокировке информации. Для бизнеса в сфере информации такие нововведения всегда вызывают вопросы со стороны исполнителей из-за неясности критериев квалификации нового вида ограничиваемой информации. Во-вторых, ужесточение выражается в ограничении компетенций операторов связи в отношении собственных сетей, поскольку в случае установления управления Роскомнадзором в сети решение о мерах реагирования на незаконный контент принимает уже не оператор сети, а госорган.

[4] https://www.consultant.ru/document/cons_doc_LAW_482411/
https://www.consultant.ru/law/review/fed/fd2024-08-09.html

Ключевые аспекты

1. ЕС против крупных платформ

Опыт ЕС

В августе 2024 г. подведены результаты расследований ЕС в отношении TikTok и Meta по нарушению требований вступившего в силу в феврале 2024 г. Закона о цифровых рынках[5] (далее – DSA), который установил ряд обязанностей для платформ, работающих с незаконным контентом.

DSA выделяет специальную категорию «очень крупных платформ» – более 45 млн пользователей из ЕС в месяц. В настоящее время в эту категорию попадают 19 платформ[6]. Для них установлены специальные требования, несоблюдение которых вызвало расследования со стороны Еврокомиссии против AliExpress, Meta и Instagram[7], TikTok и Twitter.

В ЕС также работает платформа Телеграм, против основателя которой – Павла Дурова было начато расследование в августе 2024 г. Обвинения в нарушении французского законодательства во многом коррелируют с нормами, заложенными DSA.

Рассмотрим процесс расследований против Meta и TikTok, а также может ли Telegram быть признан «очень крупной платформы», и к каким последствиям это приведет?

Прежде всего статус «очень крупной онлайн-платформы» влечет ряд обязанностей:

- оценивать не реже 1 раза в год «системные риски» (ст. 34) в отношении своих сервисов, в том числе систем модерации контента, дизайна рекомендательных систем, рекламных сервисов и пр. К системным рискам относится распространение нелегального контента, оскорбление человеческого достоинства, нарушение прав на защиту персональных данных, свободу слова и информации, недискриминацию, защиту прав ребенка и потребителей и пр.;
- снижать системные риски (ст. 35), включая адаптацию дизайна и интерфейсов, функций сервисов, модерации контента (например, скорость реагирования на жалобы о незаконном контенте, оперативность удаления такого контента), алгоритмических систем, в том числе рекомендательных систем, внедрение инструментов защиты детей (проверка возраста и родительский контроль), маркировку дипфейков и пр.;
- внедрять механизм кризисного реагирования (ст. 36) на угрозы безопасности;
- проводить независимый аудит на реже 1 раза в год (ст. 37) и иметь независимый механизм комплаенса для соблюдения требований DSA (ст. 41);
- иметь рекламный репозиторий – хранилище информации о размещаемой рекламе;
- предоставлять в своих рекомендательных системах опцию, которая не основана на профилировании пользователей.

В августе 2024 г. завершилось расследование Комиссии против TikTok в связи с работой «Программы задач и вознаграждений» TikTok Lite, которая позволяет пользователям зарабатывать баллы, выполняя определенные «задачи», такие как просмотр видео, лайкинг контента, приглашение друзей присоединиться к TikTok и пр. Баллы можно обменять на ваучеры Amazon, подарочные карты PayPal, валюту TikTok coin и пр. По мнению Еврокомиссии, Программа была запущена без предварительной оценки системных рисков, например, риска «эффекта привыкания к платформе» пользователей, не приняты меры снижения таких рисков,

[5] https://eur-lex.europa.eu/eli/reg/2022/2065/oj

[6] Alibaba AliExpress, Amazon Store, Apple AppStore, Booking.com, Facebook, Google Play, Google Maps, Google Shopping, Instagram, LinkedIn, Pinterest, Snapchat, TikTok, Twitter, Wikipedia, YouTube, Zalando, Bing, Google Search.

[7] Компания Meta, запрещенная на территории Российской Федерации организация, включенная в Перечень организаций и физических лиц, в отношении которых имеются сведения об их причастности к экстремистской деятельности или терроризму.

особенно в отношении детей и их психического здоровья, стимулируя аддиктивное поведение. В итоге сначала Программа TikTok Lite была приостановлена (в апреле 2024 г.), а с учетом того, что TikTok не смог провести оценку рисков – с августа Комиссия приняла решение о запрете в ЕС Программы.

Также в августе получило развитие расследование в отношении Meta[8]. Само расследование началось еще в апреле 2024 г. в связи с тем, что Meta:

- нарушает требования к механизму пометки нелегального контента – механизм не является легкодоступным и удобным для пользователя, отсутствует внутренняя система обработки жалоб на решения по модерации контента;
- не предоставляет инструменты для гражданского дискурса и мониторинга выборов в режиме реального времени в преддверии выборов. Meta планирует прекратить поддержку «CrowdTangle» – инструмента для сбора информации общественностью с целью мониторинга выборов в режиме реального времени. По мнению Комиссии, прекращение поддержки CrowdTangle создает риски, для гражданского дискурса и избирательных процессов в ЕС – потребители не смогут отслеживать случаи дезинформации, вмешательства в выборы и обеспечивать общую прозрачность в реальном времени путем предоставления фактов журналистам и другим заинтересованным сторонам.

В преддверии выборов в мае 2024 г. Meta включила новые функции в CrowdTangle – 27 общедоступных панелей мониторинга (по 1 на каждое государство ЕС). На данный момент работа функций прекращена, в связи с чем в августе 2024 г. Комиссия потребовала предоставить информацию о работе таких функций для дальнейшего расследования.

Событием августа 2024 г. также стал арест основателя Телеграм Павла Дурова[9], обвиняемого в соучастии создания онлайн-платформы для осуществления незаконных транзакций, отказа предоставлять по запросу компетентных органов информацию о хранении порнографических изображений несовершеннолетних, продажи оборудования, программ получения доступа к автоматизированной системе обработки данных с целью нарушения ее функционирования, мошенничестве, предоставлении криптологических услуг и импорт криптологических инструментов без декларирования.

Однако обвинения преимущественно основаны на нарушении французского законодательства. Например, декларирование в государственных органах криптологических инструментов, оборудования, программ предусмотрено Законом о доверии в цифровой экономике[10].

Некоторые обвинения коррелируют с нормами, закреплёнными DSA, как обязанность предоставлять уполномоченным органам информацию (ст. 10), обязанность защищать несовершеннолетних (ст. 28) и пр.

Важно отметить, что на данный момент Телеграм не признается «очень крупной платформой» в рамках DSA, так как имеет менее 45 млн пользователей из ЕС в месяц. Кроме того, во исполнение DSA Телеграм назначил законного представителя в Бельгии. Поэтому на данный момент в отношении Телеграм пока не могут проводиться расследования, аналогичные расследованиям против Meta и TikTok за нарушение DSA. Тем не менее в ближайшее время аудитория Телеграм может достигнуть более 45 млн человек – после этого сама Еврокомиссия должна определить Телеграм в качестве «очень крупной онлайн-платформы». В таком случае в течение 4 месяцев Телеграм должна будет обеспечить полное соответствие DSA, иначе это повлечет расследование уже Комиссии.

Опыт России

В России на данный момент отсутствует схожее с ЕС регулирование, однако действует регулирование с точки зрения мониторинга и удаления с платформ информации, признанной незаконной. При

[8] https://digital-strategy.ec.europa.eu/en/news/commission-sends-request-information-meta-under-digital-services-act-2

[9] https://www.tribunal-de-paris.justice.fr/sites/default/files/2024-08/2024-08-26%20-%20CP%20TELEGRAM%20.pdf

[10] https://www.legifrance.gouv.fr/codes/section_lc/JORFTEXT000000801164/LEGISCTA000006117690/2020-01-01

это в России основной метод борьбы – блокировка, причем в некоторых случая, например, при распространении информации с нарушением закона (призывы к массовым беспорядкам, экстремистской деятельности, ложные сообщения об актах терроризма) Роскомнадзор вправе заблокировать информационный ресурс без предупреждения. В остальных случаях Роскомнадзор отправляет предварительное требование удалить контент, и если контент не удален, то только тогда у Роскомнадзора появляется право блокировки.

Кроме того, существуют специальные обязанности для социальных сетей – принимать меры для предотвращения распространения информации, содержащей призывы к совершению уголовно наказуемых деяний, к террористической деятельности, экстремизму, материалы, пропагандирующие жестокость, насилие и др. Для этого социальная сеть должна обеспечить канал связи для получения сообщений о запрещенной информации, установить пользовательские правила в отношении ограничения распространения такой информации, а также обеспечить ежегодную публичную отчетность о результатах мониторинга.

2. Регулирование деятельности брокеров данных

Специальное регулирование для брокеров данных появилось с середины 2010-х годов. В цифровой экономике брокеры данных (посредники между продавцами и покупателями данных) способствуют сокращению трансакционных издержек (например, на поиск подходящего набора данных и его продавца), повышению доверия между участниками рынка (например, за счет прозрачности своей деятельности) и тем самым развивают рынок данных. В то же время при появлении посредника между владельцами и пользователями данных создаются дополнительные риски для безопасности данных при их передаче, например, риски утечки данных. Регулирование может усилить преимущества работы таких лиц (например, за счет открытого реестра брокеров данных) и сократить риски их деятельности (например, за счет мер ответственности, в том числе штрафов за нарушения информационной безопасности).

Опыт США (Вермонт, Калифорния)

В августе 2024 г. в Калифорнии подготовлены разъяснения по регистрации брокеров данных, в том числе уточнены критерии признания компании брокером данных: в частности, таким критерием служит отсутствие «прямых отношений» (инвестор – компания, работник – работодатель и т.п.) между компанией и субъектами данных.

Среди штатов США регулирование брокеров данных принято в Вермонте (2018 г.)[11] и Калифорнии (2019 г.)[12]. В этих штатах брокеры данных – это профучастники, функция которых состоит в законном сборе персональных данных из разных источников (например, веб-сайты, бизнес), их преобразовании под потребности рынка и продаже/ передаче по лицензии. В Вермонте, чтобы компания признавалась брокером данных, данные должны быть в электронном и подготовленном для распространения третьим лицам виде. При этом в обоих штатах не признаются брокерами данных компании, реализующие данные своих покупателей, работников, инвесторов и пр., например, приложение, продающее данные своих пользователей[13].

В обоих штатах брокеры данных обязаны ежегодно регистрироваться. Регистрация производится в следующем за деятельностью периоде, т.е., по сути, содержит элемент отчетности. Предоставляемые сведения немного различаются: например, в Вермонте требуется число нарушений безопасности данных (при хранении, передаче и т.д.), в

[11] https://legislature.vermont.gov/bill/status/2018/H.764
[12] https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201920200AB1202. Сейчас действует редакция 2023 г.: https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=202320240SB362, разъяснения к которой были выпущены в 2024 г.: https://cppa.ca.gov/regulations/pdf/data_broker_reg_prop_text.pdf

[13] https://ago.vermont.gov/sites/ago/files/wp-content/uploads/2018/12/2018-12-11-VT-Data-Broker-Regulation-Guidance.pdf, https://cppa.ca.gov/regulations/pdf/data_broker_reg_prop_text.pdf,

Калифорнии – число запросов от субъектов на осуществление своих прав (удаление данных и т.п.) и срок ответа на них.

В Вермонте существует также требование к брокерам данных о комплексной информационной безопасности, включающей, в том числе оценку рисков, регулярный пересмотр мер безопасности и контроль доступа к данным.

Опыт ЕС

В ЕС Закон об управлении данными, устанавливающий требования к услугам по посредничеству в сфере данных, принят в 2022 г.[14] Брокеры оказывают посреднические услуги между держателями и пользователями данных (п. «а» ст. 10).

В отличие от рассмотренных штатов США, в ЕС регистрация брокеров данных проводится однократно и до начала деятельности, при этом, так же как в США, имеет уведомительный характер и сведения о брокере, включая описание его услуг, публикуются в едином реестре.

В остальном подход ЕС жестче, чем в США:

1) оказание услуг через отдельное юрлицо: даже если компания уже работает в сфере данных, деятельность по оказанию посреднических услуг должна быть строго отделена от прочей деятельности как юридически, так и экономически[15];

2) обмен данными, как правило, должен происходить в формате, в котором они получены от держателя. Сопутствующие услуги, например, обезличивание, – только по явному запросу/одобрению держателя данных. Иначе говоря, в ЕС ограничиваются функции, которые в рассмотренных штатах США входят в основные функции брокеров данных;

3) обязательные процедуры против мошенничества и злоупотреблений – в Вермонте проверка добросовестности приобретателей данных относится к лучшей практике, но обязательной не является.

Опыт России

В России специальное регулирование для брокеров данных отсутствует. Это может дестимулировать оборот данных в экономике, повышая издержки на поиск контрагентов и заключение договоров и не способствуя развитию доверия на рынке данных. Например, это усложняет привлечение к ответственности профучастников рынка данных: при делегировании обработки данных их приобретателю ответственность за исполнение обязательств оператора несет приобретатель данных. В связи с этим целесообразно определить права, обязанности и ответственность профучастников рынка данных в законах о персональных данных и об информации.

3. Постквантовая криптография для кибербезопасности

В Мониторинге № 2 мы уже рассматривали тренд на стандартизацию в сфере квантовых технологий в отдельных странах (США, Великобритания) с прицелом на аспекты безопасности таких технологий.

В цифровой экономике криптография имеет важное значение, защищая хранимую и передаваемую в электронном виде информацию, например, сообщения электронной почты, медицинские записи и платежные данные. Криптография основана на математических задачах, которые обычным компьютерам слишком сложно или невозможно решить. Но с появлением квантовых компьютеров, отличающихся мощностью и скоростью вычислений, многие такие задачи становятся решаемыми, что ставит под угрозу как конфиденциальность частной информации, так и безопасность критической инфраструктуры, например, электроснабжения. В связи с этим актуальны разработка и внедрение стандартов постквантовой криптографии, т.е. базирующихся на задачах, которые не под силу ни обычным, ни квантовым компьютерам, – такой задачей, например,

[14] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R0868

[15] Micheli M., Farrell E. et al. Mapping the landscape of data intermediaries. Emerging models for more inclusive data governance. JRC Science for Policy Report. European Commission, 2023, с. 23.

считается задача обучения с ошибками (LWE).

Опыт США

В августе 2024 г. в США приняты первые 3 стандарта постквантовой криптографии: 1 по инкапсуляции ключей[16] для передаваемой по сетям информации и 2 (основной и резервный, базирующийся на другом математическом подходе) для цифровых подписей[17].

Национальный институт стандартов и технологий (NIST)[18] начал разработку стандартов постквантовой криптографии в 2017 г. и проводил отбор вариантов в 3 этапа, в том числе на основе оценки безопасности и сравнительного анализа производительности.

Содержащиеся в стандартах технические решения считаются устойчивыми к атакам квантовых компьютеров. Например, в стандарте по инкапсуляции ключей[19] решение для установления секретного ключа, который затем может использоваться для шифрования и аутентификации, основано на вычислительной сложности задачи обучения с ошибками (LWE).

Несмотря на то что речь идет, по сути, о подготовке к будущим угрозам, в США еще в 2023 г., до принятия указанных стандартов, призывали все организации начать планирование перехода на стандарты постквантовой криптографии[20].

Опыт стран ЕС

В отличие от США в ЕС в настоящее время обсуждаются более общие параметры: в апреле 2024 г. приняты рекомендации Еврокомиссии для перехода к постквантовой криптографии, призванные определить цели, этапы и сроки формирования совместной дорожной карты[21].

Вместе с тем на уровне стран-членов союза (например, Германии, Франции, Нидерландов и Швеции[22]) ведомства, отвечающие за защиту информации, призывают компании уже сейчас предпринять шаги к квантово-устойчивому шифрованию. По мнению ведомств этих стран внимание должно быть сосредоточено на доступной на существующем оборудовании постквантовой криптографии, в том числе с использованием стандартов, разработанных NIST США.

Опыт России

В России разработкой национальных стандартов постквантовой криптографической защиты информации с 2019 г. занимается рабочая группа 2.5 «Постквантовые криптографические механизмы» Технического комитета по стандартизации «Криптографическая защита информации» (ТК 26)[23]. ТК 26 работает под руководством Росстандарта и ФСБ России[24].

В 2023 г. в рамках ТК 26 разработан постквантовый алгоритм электронной подписи «Шиповник», основанный на задаче декодирования случайного линейного кода[25], а в марте 2024 г. – постквантовая схема инкапсуляции ключа «Кодиеум» для защиты информации, передаваемой в сетях, в том числе связи, основанная на том же классе математических задач[26]. Готовится проект стандарта с использованием этой схемы.

---

[16] Схема, которая может использоваться для установления секретного ключа между двумя сторонами, взаимодействующими по общедоступному каналу.
[17] https://www.federalregister.gov/documents/2024/08/14/2024-17956/announcing-issuance-of-federal-information-processing-standards-fips-fips-203-module-lattice-based; https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards
[18] Относится к Министерству торговли (*Department of Commerce*).
[19] https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.203.pdf
[20] https://www.cisa.gov/news-events/news/cisa-nsa-and-nist-publish-new-resource-migrating-post-quantum-cryptography
[21] https://digital-strategy.ec.europa.eu/en/library/recommendation-coordinated-implementation-roadmap-transition-post-quantum-cryptography
[22] https://www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2024/240126_QKD-Positionspapier.html; https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Crypto/Quantum_Positionspapier.pdf?__blob=publicationFile&v=4
[23] https://tc26.ru/about/structure/
[24] https://tc26.ru/about/
[25] https://kryptonite.ru/news/postkvantovyi-algoritm-shipovnik-realisatsiya/
[26] https://habr.com/ru/companies/kryptonite/articles/802121/; https://tc26.ru/news/novosti-kriptografii/v-rossii-razrabotan-kriptograficheskiy-mekhanizm-sposobnyy-vyderzhivat-ataki-kvantovykh-kompyuterov.html?sphrase_id=77397