Форензика в расследовании антимонопольных нарушений

Аннотация. *Представлены анализ и оценка ряда цифровых доказательств, используемых антимонопольным органом при расследовании дел о заключении антиконкурентных соглашений, включая электронные письма участников соглашений, документы на электронных носителях, совпадение IP-адресов или MAC-адресов, а также данные параметрической программы «Большой цифровой кот».*

В статье дается также описание возможных оснований и способов формирования контраргументов на собираемые антимонопольным органом цифровые доказательства в целях подтверждения добросовестности действий компаний.

Ключевые слова: *форензика, цифровые доказательства, картель, антиконкурентные соглашения, антимонопольное законодательство, параметрическая программа «Большой цифровой кот».*

DOI: 10.17803/2311-5998.2022.95.7.119-131

Андрей Евгеньевич ШАСТИТКО,
доктор экономических наук, профессор, заведующий кафедрой конкурентной и промышленной политики экономического факультета МГУ имени М. В. Ломоносова, директор Центра исследований конкуренции и экономического регулирования РАНХиГС при Президенте РФ
aes@ranepa.ru
119571, Россия, г. Москва, просп. Вернадского, д. 82

Елизавета Николаевна САВИНА,
адвокат, руководитель направления антимонопольного комплаенса компании Kulik & Partners Law. Economics
e.savina@kple.ru *119017, Россия, г. Москва, 1-й Казачий пер., д. 5/2, стр. 1, оф. 1*

ANDREY E. SHASTITKO,
Dr. Sci. (Economics), Professor, Head of the Chair of competition and industrial policy, Economic department at the Lomonosov Moscow State University, Director of the Center for Competition and Economic Regulation Studies, Russian Presidential Academy of National Economy and Public Administration
aes@ranepa.ru
82, Vernadskogo prosp., Moscow, Russia, 119571

ELIZAVETA N. SAVINA,
Advocate, Head of Antitrust compliance in Kulik & Partners Law.Economics
e.savina@kple.ru
of. 1, str. 1, 5/2, 1st Kazachiy per., Moscow, Russia, 119017

Forensics in Investigation of Antitrust Violations

Abstract. *This article contains an analysis and assessment of digital evidences used by the Federal Antimonopoly Service of the Russian Federation in anticompetitive agreement cases, such as an e-mails of the parties of agreements, electronic documents, equal IP or MAC address, and data from the Big Digital Cat parametric program.*

This article also contains description of the possible methods and arguments in order to confirm the good faith of companies' actions against digital evidence collected by the Federal Antimonopoly Service of the Russian Federation.

Keywords: *data forensics, digital evidence, cartel, anticompetitive agreements, antitrust law, the "Big digital cat" parametric program.*

В числе антимонопольных нарушений наиболее опасными по праву признаются антиконкурентные соглашения, в том числе на товарных рынках и торгах.

Антиконкурентное соглашение — форма монополистического объединения хозяйствующих субъектов, результатом которого является их противоестественное взаимовыгодное сотрудничество вместо ожидаемого потребителями соперничества между ними[1].

Вот почему лица, уличенные в указанных нарушениях, подлежат наказанию в виде высоких штрафных санкций в соответствии со ст. 14.32 Кодекса РФ об административных правонарушениях[2], а при соответствии составу нарушения — даже лишению свободы в рамках положений Уголовного кодекса РФ[3] (в первую очередь — ст. 178).

Однако для предъявления обвинения и применения наказаний необходимо получение достаточных доказательств. Нарушение данного принципа — источник ошибок первого рода в правоприменении, ослабляющих сдерживающие свойства правовой системы[4].

Современная экономика проходит фазу фундаментальной цифровой трансформации, когда на применении цифровых технологий основаны бизнес-процессы как в рамках одной компании, так и между компаниями. Цифровизация бизнес-процессов позволяет ускорить и упростить выполнение бизнес-задач, но вместе с тем и предоставляет возможность совершать правонарушения и преступления с помощью цифровых средств.

В настоящее время значительная часть коммуникации между правонарушителями организована с применением электронной переписки, электронного документооборота, а также технических средств, предполагающих использование компьютерных технологий. Соответственно, нарушение законодательства с применением цифровых средств оставляет за собой цифровые следы.

В последние несколько лет цифровизация бизнес-процессов все чаще вынуждает антимонопольный орган прибегать к сбору и оценке цифровых доказательств, содержащихся на различных электронных носителях. В качестве

---

1 *Кинёв А. Ю.* Картели и другие антиконкурентные соглашения. С. 1 // СПС «КонсультантПлюс».

2 Кодекс РФ об административных правонарушениях от 30.12.2001 № 195-ФЗ // СЗ РФ. 2002. № 1 (ч. I). Ст. 1.

3 Уголовный кодекс РФ от 13.06.1996 № 63-ФЗ // СЗ РФ. 1996. № 25. Ст. 2954.

4 *Шаститко А. Е.* Ошибки I и II рода в экономических обменах с участием третьей стороны — гаранта // Журнал новой экономической ассоциации. № 10. С. 125—148.

доказательств нарушения в антимонопольных делах нередко выступают электронная переписка, электронные документы, IP-адреса и MAC-адреса участников торгов, цифровой анализ поведения компаний на различных электронных площадках и т.д.

Результативность правовой системы по сдерживанию преступлений, связанных с ограничением конкуренции в форме антиконкурентных соглашений, зависит от того, каким образом применяются результаты исследований в форензике — отрасли знания о раскрытии преступлений с применением цифровых технологий, об исследовании цифровых доказательств, о методах поиска, получения и закрепления таких доказательств.

Основная задача данной работы — раскрыть отдельные аспекты применения форензики в рамках формирования доказательной базы для раскрытия правонарушений в форме антиконкурентных соглашений на торгах и на товарных рынках. Остановимся на двух блоках вопросов, касающихся передаваемого контента, в котором содержится информация, оцениваемая на предмет проверки гипотезы о наличии антиконкурентных соглашений.

С этой целью рассмотрим проблематику формирования доказательств в сфере электронной переписки, а также электронных документов в различных форматах (Word, Excel, PDF и т.п.). Далее будет исследован вопрос об однозначности идентификации устройств, с помощью которых компании участвуют в торгах. Наконец, в третьей (завершающей) части будет рассмотрен комплексный вопрос об автоматизации контроля деятельности компаний на предмет соблюдения требований антимонопольного законодательства (в первую очередь в сфере торгов) через призму распределения рисков и трансакционных издержек между регулятором и участниками торгов.

Электронная коммуникация

Электронная коммуникация (переписка) является одним из наиболее часто используемых антимонопольным органом доказательств. Это может быть электронная переписка, например, между сотрудниками компаний-конкурентов, участниками и заказчиками торгов, продавцами и покупателями.

Антимонопольный орган получает доступ к электронной переписке проверяемых хозяйствующих субъектов путем проведения внеплановых выездных проверок, а также от заявителей, заинтересованных или иных лиц при предоставлении ими переписки (по инициативе таких лиц или в ответ на запрос антимонопольного органа).

Представление заявителями, заинтересованными или иными лицами электронной переписки в большинстве случаев происходит на бумажном носителе (в форме распечатанных электронных писем или скриншотов экрана компьютера с изображением таких писем), в связи с чем антимонопольный орган и стороны в рамках антимонопольного дела могут исследовать такие доказательства без применения цифровых средств.

Иным образом обстоят дела с исследованием электронной переписки, полученной в ходе внеплановой выездной проверки, когда антимонопольным органом

и привлеченными им IT-специалистами осуществляется посекторное копирование жестких дисков рабочих компьютеров сотрудников проверяемого хозяйствующего субъекта.

Под посекторным копированием понимается копирование данных, содержащихся на исходном жестком диске, в соответствии с занимаемыми ими секторами. При посекторном копировании жесткого диска получается точная копия (клон) исходного диска, содержащегося на рабочем компьютере сотрудника компании. При открытии посекторной копии жесткого диска на компьютерах сотрудников антимонопольного органа отображается точный образ исходного диска со всеми хранящимися на нем данными, с сохранением внутренней структуры рабочего компьютера проверяемого сотрудника.

Скопированный антимонопольным органом жесткий диск открывается с помощью специальной программы, где среди прочих файлов содержится история электронной переписки в формате *.ost.* Для открытия и изучения электронной переписки антимонопольный орган, как правило, осуществляет конвертацию файла в формате *.ost* в формат *.pst*, который позволяет изучать содержимое переписки в привычном для нас почтовом клиенте, например, в почтовом клиенте *Outlook*.

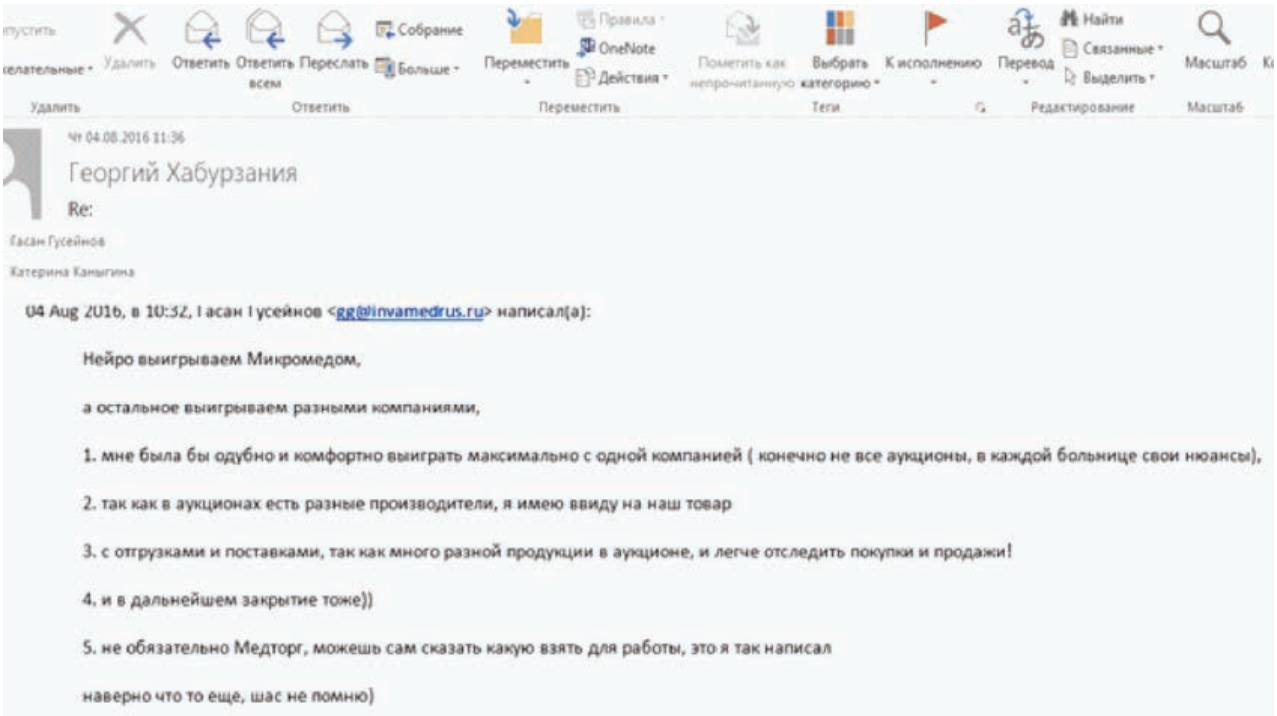
По итогам анализа электронной переписки, полученной в ходе внеплановой выездной проверки, сотрудник антимонопольного органа составляет отчет об исследовании доказательств в соответствии с положениями приказа ФАС России от 25.05.2012 № 340 «Об утверждении административного регламента по исполнению государственной функции по проведению проверок соблюдения требований антимонопольного законодательства Российской Федерации».

Данный отчет приобщается в качестве письменного доказательства к материалам антимонопольного дела. В отчете отражается в том числе и информация о времени, месте проведения осмотра, также помещается изображение электронной переписки (как правило, в форме распечатанных скриншотов компьютера сотрудника или распечатки сообщений электронной почты), содержащей, по мнению антимонопольного органа, признаки нарушения.

Согласно постановлению Президиума Высшего арбитражного суда РФ от 12.11.2013 по делу № А47-7950/2011 «распечатки сообщений электронной почты, информации с жестких дисков и иных носителей, заверенные антимонопольным органом, который получил эти материалы в ходе проведенной им проверки, являются надлежащими доказательствами по делам о нарушении антимонопольного законодательства».

Пример скриншота электронного письма, использованного ФАС России в качестве доказательства в одном из своих решений от 08.12.2017 по делу № 1-00-87/00-22-17, приведен ниже. Следует отметить, что использование антимонопольным органом подобного рода скриншотов, приложенных к отчетам об исследовании доказательств, является наиболее распространенным (изображение письма взято из решения ФАС России от 08.12.2017 по делу № 1-00-87/00-22-17 и содержит переписку между участниками торгов.).

Далее мы покажем, почему скриншоты электронных сообщений или электронные сообщения не являются неоспоримым или однозначно достоверным доказательством в рамках антимонопольных дел.



Представляемые заявителями, заинтересованными и иными лицами распечатанные электронные письма или скриншоты с изображением таких писем, а также исследуемые и распечатываемые сотрудниками антимонопольного органа файлы в формате *.pst* доступны для изменения и корректировки.

На практике встречаются случаи, когда представляемые в качестве доказательств электронные письма содержат следы изменений их содержания, времени и даты отправления, адресатов, количества и наименования приложений к письмам и т.д. В связи с этим первое, что рекомендуется делать при работе с доказательствами в форме распечатанной электронной переписки, — искать оригиналы таких писем (на компьютерах сотрудников компании, которые являлись отправителями или адресатами таких писем) и сравнивать их с содержащимися копиями в материалах антимонопольного дела на предмет наличия расхождений. Если расхождения будут выявлены, станет очевидным, что представленные в материалы дела электронные письма являются измененными и не могут выступать допустимым доказательством.

Для подтверждения внесения изменений в исходное электронное письмо и, как следствие, его недопустимости в качестве доказательства стороне необходимо представить оригинал (копию) письма (на электронном носителе или распечатку) в адрес антимонопольного органа или суда с ходатайством о признании имеющегося в материалах антимонопольного дела доказательства недопустимым. Такое ходатайство будет являться основанием для повторного изучения содержащихся в материалах дела документов в целях установления достоверности содержания письма.

Довод о внесения изменения в исходное электронное письмо можно дополнительно сопроводить нотариальным протоколом осмотра электронной почты сотрудника компании с прикрепленными к нему приложениями, где может содержаться скриншот исходного (оригинального) электронного письма.

Кроме того, лицо вправе представить заключение специалиста в сфере IT, в котором может содержаться конкретная информация о том, вносились ли, по мнению специалиста, в содержащиеся в материалах антимонопольного дела скриншоты электронных писем изменения (на основании анализа заголовков электронного письма, даты направления письма, наименования темы письма, свойств приложенных файлов и т.д.).

Самостоятельным направлением для изучения в рамках заключения специалиста в сфере IT может являться вопрос о наличии или отсутствии в электронном письме пересылаемого письма или приложений (вложений) к такому письму. Определить наличие или отсутствие пересылаемого письма и (или) приложений (вложений) в полученном письме в почтовом клиенте Outlook можно посредством:

1) анализа темы и содержания полученного письма;
2) исследования заголовков полученного письма.

Исключительно на основании анализа темы и содержания полученного электронного письма нельзя однозначно (достоверно) установить факт наличия в нем пересылаемого электронного письма или вложения, поскольку Microsoft Outlook позволяет редактировать тему[5], реквизиты и (или) текст[6] электронных писем с последующим сохранением.

Наиболее достоверным способом установления факта наличия пересылаемого письма в полученном электронном письме является анализ заголовков электронного письма (отображающихся в свойствах электронного письма).

Заголовки электронного письма — это техническая информация, описывающая электронное письмо. Они могут содержать данные о маршруте прохождения письма, идентификаторе письма и многом другом.

Заголовки представляют собой текст, состоящий из элементов в соответствии со стандартом RFC 5322[7]. Каждый заголовок обычно представляет собой пару «ключ, значение». Пример заголовка: «Message-ID: <b41095601e1f465a8695a9ca41e4dce9@gmail.com>».

Многие почтовые клиенты позволяют просмотреть заголовки электронного письма. В клиенте Microsoft Outlook они указаны в окне «свойства» электронного письма.

На основании анализа свойств и заголовков оригинала (исходного) электронного письма специалистом в сфере IT может быть сделан вывод о внесении изменений в электронные письма, содержащиеся в материалах антимонопольного дела.

---

[5] Изменение темы электронной почты // URL: https://support.office.com/ru-ru/article/08d60328-2a27-473e-8227-0b42a1ff2ce6 (дата обращения: 10.01.2022).

[6] How to Edit Received Emails in Outlook // URL: https://www.wikihow.com/edit-received-emails-in-outlook (дата обращения: 10.01.2022).

[7] RFC 5322. Internet Message Format // URL: https://datatracker.ietf.org/doc/html/rfc5322 (дата обращения: 10.01.2022).

Электронные документы в различных форматах

Еще одним часто используемым видом цифровых доказательств в антимонопольных делах являются документы в форматах Word, Excel, PDF, PowerPoint и др.

Как и в случае с электронными письмами, документы могут быть представлены в антимонопольный орган (например, на электронном носителе, жестком диске, CD-диске, USB-флеш-накопителе и т.д.) заявителями, заинтересованными или иными лицами, в том числе электронной площадкой, а также получены антимонопольным органом в ходе проведения внеплановых выездных проверок.

В электронные документы, как и в электронные письма, у третьих лиц существует возможность вносить изменения. В данном случае один из принципиальных вопросов — прослеживаемость указанных изменений.

В целях проверки представленных документов на предмет их достоверности потребуется исходный документ для сравнения, также допустимо изучение вкладки «*свойства*» представленного электронного документа.

Свойства документа (или метаданные) — это сведения о файле, которые его описывают или определяют. В число свойств документа входят его название, имя автора, тема и ключевые слова, указывающие на раздел или содержимое документа[8].

Вкладка «*свойства*» содержит в том числе и информацию о создателе документа, последнем изменившим его лице, количестве затраченного на создание документа времени, а также о дате и времени его создания. Данная информация будет полезной, например, при необходимости подтверждения факта самостоятельной подготовки заявок их участниками. В случае если авторы и лица, вносившие изменения в текст заявок разных участников, не совпадают, то говорить о согласовании текста заявок (при отсутствии иных доказательств) едва ли возможно.

Кроме того, существуют случаи, когда в материалах антимонопольного дела содержатся документы, подвергшиеся изменению после их создания со стороны третьих лиц. Для подтверждения данного факта в электронном документе, содержащемся в материалах антимонопольного дела, рационально будет изучить поле «*кем изменено*» во вкладке «*свойства*» раздела «*сведения*» рабочей книги Microsoft, в которой отображается информация об имени пользователя, который последним внес изменения в рабочую книгу с последующим ее сохранением[9].

Microsoft автоматически заполняет поле «*кем изменено*». Пользователь не может изменять вручную значение этого поля. При скачивании, копировании и сохранении электронного документа Microsoft на различных носителях без внесения в документ изменений значение поля «*кем изменено*» не обновляется, сохраняя прежнее значение. Следовательно, в случае внесения в текст изменений третьими лицами данный факт можно будет выявить и подтвердить. Вместе с тем объем внесенных изменений установить не удастся.

---

[8] Просмотр или изменение свойств файла Office // URL: https://support.office.com/ru-ru/article/21d604c2-481e-4379-8e54-1dd4622c6b75 (дата обращения: 10.01.2022).

[9] Изменение имени пользователя и инициалов // URL: https://support.office.com/ru-ru/article/cdd4b8ac-fbca-438d-a5b5-a99fb1c750e3 (дата обращения: 10.01.2022).

Иным образом обстоит дело с полем «*автор*», которое, в отличие от поля «*кем изменено*», доступно для редактирования любому пользователю. Информация о первоначальном авторе документа может быть изменена или полностью удалена любым пользователем в любое время, что может позволить исказить информацию о лице, создавшем документ, в том числе в недобросовестных целях[10].

Для подтверждения фактов неправомерного внесения изменений третьими лицами в исходные электронные документы целесообразно обратиться за заключением к специалисту в сфере IT.

Следует учитывать, что при подготовке заключения специалист в сфере IT в первую очередь будет анализировать представленные документы (оригинал / исходный электронный файл и содержащийся в материалах антимонопольного дела документ). Такие документы позволят изучить свойства электронных файлов, а также сделать выводы о наличии или отсутствии фактов внесения изменений в документы, содержащиеся в материалах антимонопольного дела. В заключении специалиста, как правило, подробно излагаются способы исследования электронных документов, а также с помощью скриншотов экрана компьютера демонстрируется, каким образом и почему специалист пришел к тем или иным выводам о внесении изменений в документ.

Совпадение IP- и MAC-адресов

Одной из последствий цифровизации системы закупок являлась проблема сговоров на торгах[11] с использованием цифровых средств.

Первым делом, в котором IP-адреса были использованы в качестве доказательства заключения антиконкурентного соглашения, стало решение ФАС России от 06.04.2012 по делу № 1 11/141-11 о нарушении антимонопольного законодательства[12].

На сегодняшний день практически в каждом деле о заключении антиконкурентного соглашения антимонопольный орган анализирует и использует в качестве доказательства недобросовестных действий компаний-конкурентов совпадение IP-адресов.

IP-адрес это уникальный адрес (числовой идентификатор) устройства (компьютера, планшета, смартфона), подключенного к локальной сети или сети Интернет, который задается провайдером. Совпадение IP-адресов участников торгов при подаче заявок на участие в торгах толкуется антимонопольным органом, как

---

[10] См.: Порядок внесения изменений в поле «автор» электронного документа на вкладке «Изменение имени автора документа» // URL: https://support.office.com/ru-ru/article/0ad23fe7-b82e-40c4-b9d9-391fec971a54 (дата обращения: 10.01.2022).

[11] Антимонопольное регулирование в цифровую эпоху: как защищать конкуренцию в условиях глобализации и четвертой промышленной революции : монография / под ред. А. Ю. Цариковского, А. Ю. Иванова и Е. А. Войниканис. М. : ИД Высшей школы экономики, 2018. С. 311.

[12] См.: Актуальные вопросы современного конкурентного права : сборник научных трудов. Вып. 3 / отв. ред. М. А. Егорова. М. : Юстицинформ, 2019. С. 65.

подача заявок конкурентами с одного компьютера (адреса), что свидетельствует о договоренности компаний об отказе от конкуренции.

Однако совпадение IP-адресов компаний-конкурентов при подаче заявок на торгах не всегда может считаться однозначным подтверждением подачи заявок с одного электронного устройства. Если значимость данного обстоятельства недооценена, то повышается риск совершения ошибки первого рода в правоприменении (неправильное определение субъекта правонарушения).

Судебная и административная практика знает примеры, когда совпадение IP-адресов не принималось в качестве доказательства заключения картельного соглашения[13].

Приведенная выше судебная практика исходит в том числе и из того, что IP-адрес, хотя и является уникальным адресом устройства, но при проведении Интернета многие провайдеры назначают внешние IP-адреса на базе блоков, привязанных к регионам, в связи с чем один IP-адрес может независимо использоваться несколькими компаниями. Например, при независимом осуществлении деятельности компаний в бизнес-центре (но на разных этажах). При подключении к единой локальной сети или беспроводной сети Wi-Fi у разных компаний также может отображаться одинаковый IP-адрес.

В рамках антимонопольных дел в целях подтверждения добросовестности своего поведения лица вправе представить техническое обоснование независимого использования одного IP-адреса. Один из вариантов обоснования — договор аренды помещений конкурентов в одном бизнес-центре. Однако зачастую этого недостаточно, поскольку сам по себе факт аренды офиса в одном бизнес-центре не гарантирует использование одного интернет-шлюза.

Для усиления своих доводов компания может представить в антимонопольный орган письмо от интернет-провайдера и (или) заключение специалиста в сфере IT, подтверждающих факт возможности автономного использования компаниями-конкурентами одного интернет-шлюза, которое приводит к совпадению IP-адресов, в том числе с учетом следующих обстоятельств:

1) возможность или невозможность установить однозначную привязку пользователя к IP-адресам;
2) наличие или отсутствие возможности работы нескольких пользователей с одинаковыми IP-адресами в сети Интернет (например, из-за использования интернет-провайдерами технологии NAT[14] для трансляции адресов из внутрисетевых во внешние);

[13] См., например: определение Верховного Суда РФ от 28.03.2018 по делу № А65-27996/2016, постановления Арбитражного суда Дальневосточного округа от 02.02.2021 по делу № А24-8534/2019, от 05.11.2019 по делу № А24-1720/2019, Арбитражного суда Волго-Вятского округа от 09.06.2020 по делу № А38-6825/2019, Арбитражного суда Центрального округа от 15.10.2018 по делу № А14-3561/2018, Арбитражного суда Поволжского округа от 25.09.2018 по делу № А65-21680/2017, Арбитражного суда Московского округа от 26.12.2016 по делу № А40-37651/16, решение Якутского УФАС России от 12.04.2019 по делу № 02-21/18А.

[14] NAT (Network Address Translation) — технология преобразования приватных сетевых адресов в общедоступные, что дает возможность многочисленным устройствам, каждое

3) возможность использования диапазона IP-адресов, присвоенного конечному оборудованию общества — маршрутизатору, который используется для выхода в сеть Интернет любыми лицами с любого устройства, подключенного к этому оборудованию как посредством локальной сети, так и с использованием сети беспроводного доступа (Wi-Fi) и т.д.

Таким образом, совпадение IP-адресов не всегда является следствием недобросовестных действий конкурентов и может быть обусловлено техническими особенностями используемого оборудования.

Сто́ит учитывать, что в последние несколько лет антимонопольный орган стремится устанавливать совпадение не только IP-адресов, но и MAC-адресов[15].

Информацию об IP-адресах и MAC-адресах, с которых были поданы заявки и ценовые предложения участников торгов, антимонопольный орган получает от электронных площадок, на которых проводились такие торги.

В отличие от IP-адреса, присваиваемого компьютерному устройству провайдером связи, MAC-адрес привязан к одному конкретному устройству (в большинстве случаев — к сетевой карте компьютера). Таким образом, по сути, MAC-адрес представляет собой уникальный идентификатор физического устройства в сети Интернет или локальной сети.

В связи с этим факт совпадения MAC-адресов участников картеля или иного антиконкурентного соглашения означает, что ими использовалось одно и то же компьютерное устройство[16].

Сайт государственных закупок настроен таким образом, что может запустить разные ЭВМ с одного IP-адреса, однако исключена возможность совпадения MAC-адресов компьютеров. На электронную площадку невозможно зайти на один и тот же аукцион, с одного и того же компьютера под разными паролями и с применением разных ключей, так как система безопасности распознает совпадения уже имеющегося MAC-адреса и введенного пароля, что не дает возможности повторного ввода другого ключа (пароля). Система пропишет ошибку и более не запустит данную ЭВМ на электронные торги до замены ключа (пароля)[17].

В последние годы совпадение MAC-адресов все чаще используется антимонопольным органом в качестве доказательства заключения антиконкурентного соглашения, в том числе при подаче заявок на участие в торгах. При этом антимонопольный орган стремится установить совпадение сразу IP-адресов и MAC-адресов.

из которых имеет собственный приватный адрес, использовать единый общедоступный адрес и повышает уровень безопасности и конфиденциальности сети.

[15] См. например: постановления Арбитражного суда Волго-Вятского округа от 02.07.2020 по делу № А38-2930/2019, Арбитражного суда Поволжского округа от 16.02.2021 по делу № А55-38691/2019, Девятого арбитражного апелляционного суда от 19.04.2018 по делу № А40-164963/17.

[16] См.: решение ФАС России от 20.08.2020 по делу № 1-11-13/00-22-19.

[17] См.: постановление Третьего арбитражного апелляционного суда от 16.10.2017 по делу № А33-26295/2015.

Параметрическая система «Большой цифровой кот»

Одной из последних крупных разработок, используемых российским антимонопольным органом в сборе доказательств с 2018 г., является параметрическая программа «Большой цифровой кот». Данная компьютерная программа позволяет исследовать большой объем данных об участии различных компаний на торгах (в общей сложности программа предусматривает возможность анализа нескольких десятков параметров). Сопоставление параметрических данных, а также выявление закономерностей при участии компаний в торгах позволяет довольно эффективно выявлять антиконкурентные соглашения, направленные на поддержание стоимости торгов.

В последние годы наметилась следующая тенденция: антимонопольный орган стремится выявлять признаки антиконкурентных соглашений в рамках не одной закупки, а в ряде закупок, объединяя несколько эпизодов (соглашений в ходе нескольких закупок) в одно дело на основании одинакового/сходного состава участников торгов (субъектного состава)[18].

Параметрическая программа «Большой цифровой кот» во многом способствует выявлению систематического поведения, обусловленного антиконкурентными соглашениями.

Согласно данным официального сайта ФАС России по состоянию на 2018 г. антимонопольным органом было выявлено более 90 картелей на торгах с использованием параметрической программы[19].

В настоящее время программа работает преимущественно с данными, представляемыми электронными площадками, банковскими системами, ГИС «Независимый регистратор». В анализируемых антимонопольным органом данных содержится в том числе следующая информация: количество и наименование участников с их юридическим адресом и адресом электронной почты, дата и время подачи заявок и ценовых предложений участников, размер ценовых предложений и процент снижения от начальной максимальной цены, IP-адреса участников, с которых производилась подача заявок и ценовых предложений. Вся данная информация загружается в программу и анализируется антимонопольным органом с помощью автоматизированной программы.

В будущем планируется дорабатывать и расширять функционал параметрической системы таким образом, чтобы она в автоматическом режиме автономно производила анализ информации, содержащейся на сайтах электронных площадок.

«Большой цифровой кот» — важный элемент в современной технологии применения российского антимонопольного законодательства. Программа позволяет значительно снизить прямые трансакционные издержки правоприменителя, поскольку делает излишней обработку большого массива информации вручную.

---

[18] *Савина Е. Н.* Изменение подходов антимонопольного органа к рассмотрению дел о картельных соглашениях на торгах // Российское конкурентное право и экономика. 2018. Вып. 3 (15). С. 33.

[19] Пресечение цифровых форм нарушений — новый вызов для антимонопольного регулирования // URL: https://fas.gov.ru/news/25854.

Следует отметить, что в любом случае компьютерная программа работает по определенному алгоритму, шаблону. Соответственно, в той мере, в какой действия компаний на торгах полно и адекватно описываются указанными шаблонами, можно говорить об отсутствии ошибок в идентификации признаков правонарушений. Соответственно, фиксация «аномалий» в поведении участников торгов могла бы рассматриваться сначала как признак правонарушения, а затем — как достаточное основание использования автоматизированной обработки данных как косвенных доказательств противоправного поведения.

Однако любые шаблоны работают на основе определенных допущений. И перечень указанных допущений может не охватывать все множество обстоятельств, учитываемых в принятии бизнес-решений, в том числе и на торгах[20]. Вот почему отказываться от предметной перепроверки полученных аномальных результатов вручную нет достаточных оснований.

Выводы

Использование антимонопольным органом цифровых доказательств требует от ответчиков представления симметричных цифровых доказательств, подтверждающих добросовестность действий компании.

Многие цифровые доказательства являются оспоримыми.

При анализе содержащихся в материалах антимонопольного дела цифровых доказательств следует выявлять первоисточник — исходные электронные документы и письма для установления их подлинности и отсутствия внесения в них изменений.

При доказывании добросовестности поведения компании в случае выявления антимонопольным органом совпадения IP-адресов или MAC-адресов компании надлежит выявить причины такого совпадения и представить антимонопольному органу или суду подтверждение возможности совпадения IP- или MAC-адресов по независящим от компании причинам.

Зачастую формирование цифровых доказательств добросовестности компании требует привлечения третьих лиц (нотариуса или специалистов в сфере IT).

Рассмотренная в статье параметрическая программа «Большой цифровой кот» способствует повышению эффективности выявления антиконкурентных соглашений на торгах, являясь эффективным инструментом не только для выявления картельных соглашений, но и для формирования доказательственной базы в делах о картельных соглашениях. Вместе с тем сто́ит учитывать, что параметрическая программа строится на выявлении аномалий в поведении компаний и не может исключать наличие объективных факторов, свидетельствующих о добросовестности поведения компаний.

---

[20] В частности, аналогичные проблемы удалось идентифицировать в сфере автоматического контроля уплаты налогов. См. об этом: *Шаститко А. Е.*, *Морозов А. Н.* Амбивалентность цифровой трансформации в налоговом администрировании // Закон. 2021. № 4. С. 34—42.

БИБЛИОГРАФИЯ

1. Актуальные вопросы современного конкурентного права : сборник научных трудов. — Вып. 3 / отв. ред. М. А. Егорова. — М. : Юстицинформ, 2019.
2. Антимонопольное регулирование в цифровую эпоху: как защищать конкуренцию в условиях глобализации и четвертой промышленной революции : монография / под ред. А. Ю. Цариковского, А. Ю. Иванова и Е. А. Войниканис. — М. : ИД Высшей школы экономики, 2018.
3. *Кинёв А. Ю.* Картели и другие антиконкурентные соглашения // СПС «КонсультантПлюс».
4. *Савина Е. Н.* Изменение подходов антимонопольного органа к рассмотрению дел о картельных соглашениях на торгах // Российское конкурентное право и экономика. — 2018. — № 3 (15). — С. 32—36.
5. *Шаститко А. Е.* Ошибки I и II рода в экономических обменах с участием третьей стороны — гаранта // Журнал новой экономической ассоциации. — № 10. — С. 125—148.
6. *Шаститко А. Е., Морозов А. Н.* Амбивалентность цифровой трансформации в налоговом администрировании // Закон. — 2021. — № 4. — С. 34—42.