УДК 343.234:343.34

Об особенностях учёта обстоятельств, предусмотренных п. «и» ч. 1 ст. 61 УК РФ, при назначении наказания за использование вычислительных мощностей ЭВМ для майнинга криптовалюты*

Мкртчян С.М.
Кандидат юридических наук,
доцент кафедры уголовного права
Волгоградского государственного университета

Статья посвящена изучению практики применения п. «и» ч. 1 ст. 61 УК РФ и учёта перечисленных в его тексте смягчающих обстоятельств при назначении наказания за несанкционированное использование вычислительных мощностей ЭВМ для майнинга криптовалюты. Установлено, что суды и другие правоприменители в некоторых случаях не учитывают особенности названной преступной деятельности и свойства личности преступников, её осуществляющих, при установлении соответствующих вариантов позитивного посткриминального поведения подсудимых. Проанализированы наиболее распространённые правоприменительные ошибки, выявлены общие черты, характеризующие соответствующие преступные деяния и совершающих их лиц, которые должны быть учтены при принятии решений о применении положений статей 61 и 62 УК РФ.

Ключевые слова: блокчейн, криптовалюты, майнинг, вредоносные компьютерные программы, несанкционированный доступ к компьютерной информации, позитивное посткриминальное поведение

Несмотря на то что ни представители научного сообщества [1-4], ни правоприменители[1] до сих пор не определились относительно статуса криптовалюты как предмета некоторых преступлений и возможности применения положений действующего российского уголовного закона к лицам, совершающим преступления в отношении неё, исследование судебной практики за период с 2016 г. по настоящее время позволяет судить о том, что в условиях отсутствия федерального законодательства, способного пролить свет на сущность криптовалюты и чётко регламентировать порядок её оборота на территории Российской Федерации, суды вынуждены были самостоятельно выработать некоторые правила квалификации преступных деяний, совершаемых в сфере функционирования блокчейн и оборота криптовалют, и назначения наказания за них. Указанное справедливо, в том числе для оценки судебных решений по уголовным делам о несанкционированном использовании вычислительных или энергетических мощностей компьютеров или энергоблоков для обеспечения процесса майнинга криптовалюты. Названная преступная схема получила распространение сначала в мире, а затем и в России ввиду высокой затратности соответствующего процесса в условиях необходимости практически непрерывного расходования интернет-трафика и электроэнергии в течение длительного периода времени в процессе генерирования криптовалюты, заключающемся в осуществлении математических вычислений в целях получения новых структур, добавления их

[1] См., например: Апелляционное определение судебной коллегии по уголовным делам Санкт-Петербургского городского суда от 23 ноября 2020 г. по делу № 22-5295/2020. – URL: https://sankt-peterburgsky--spb.sudrf.ru/modules.php?name=sud_delo&srv_num=1&name_op=doc&number=43236760&delo_id=4&new=4&text_number=1 (дата обращения: 23.07.2021); Апелляционное определение судебной коллегии по уголовным делам Верховного Суда Республики Татарстан от 18 октября 2019 г. по делу № 22-7705/2019. – URL: https://vs--tat.sudrf.ru/modules.php?name=sud_delo&name_op=case&_id=17504894&_uid=d39a9e4e-007f-4b37-bfae-063b41a38eaf&_deloId=1540006&_caseType=0&_new=4&_doc=1&srv_num=1 (дата обращения: 23.07.2021).

* Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 20-011-00823.

в блокчейн и верификации их системой. Изучение особенностей учёта смягчающих обстоятельств, отражающих позитивное посткриминальное поведение виновного лица, варианты которого упоминаются в п. «и» ч. 1 ст. 61 УК РФ, при назначении наказания за подобные виды преступной активности представляется значимым по нескольким причинам. Во-первых, суды весьма часто ссылаются при назначении наказания за рассматриваемые преступления на некоторые из указанных обстоятельств, в частности, на явку с повинной и активное способствование раскрытию и расследованию преступлений, а также на их разновидности («признание вины», «дача признательных показаний», «согласие с обвинением в полном объёме» и т.п.). Во-вторых, на необходимость установления указанных обстоятельств в рамках каждого уголовного дела по факту несанкционированного майнинга или покушения на него правоохранителей ориентирует сущность соответствующих преступных деяний.

Несанкционированное использование вычислительных мощностей ЭВМ для майнинга криптовалюты обычно осуществляется посредством использования специальных вредоносных компьютерных программ (далее – ВКП) или их совокупности[2], а также специальных навыков в области программирования[3] для получения удалённого доступа к 1) ЭВМ неопределённого числа пользователей сети Интернет или 2) компьютерам, функционирующим на серверах, принадлежащих коммерческим организациям или государственным органам и предприятиям. Соответствующие преступные деяния и лица, их совершающие, характеризуются несколькими общими чертами: 1) использование ВКП чрезвычайно упрощает совершение соответствующих преступлений в отношении обычных граждан – пользователей сети Интернет, однако не всегда увенчается успехом (то есть доходит до этапа непосредственного майнинга криптовалюты и даже до этапа получения удалённого доступа), если виновные пытаются внедриться на серверы государственных органов или предприятий, так как подобные действия моментально или по прошествии незначительного промежутка времени пресекаются собственными службами безопасности таких предприятий или сотрудниками ФСБ РФ, обеспечивающими кибербезопасность соответствующих виртуальных ресурсов или локальных сетей; 2) наличие налаженного ботнета (сеть заражённых компьютеров) или успешного несанкционированного доступа к серверам организаций позволяет длительное время, скрытно и весьма успешно осуществлять майнинг криптовалюты и прочие незаконные действия, поэтому чаще всего преступники самостоятельно не завершают преступную деятельность – она фактически продолжается до момента обнаружения незаконного присутствия; 3) соответствующие вредоносные программы предназначены для поражения неопределённого круга IP-адресов и серверов, то есть их использование с высокой долей вероятности свидетельствует о стремлении их неоднократного и продолжительного применения; 4) преступники чаще всего руководствуются корыстными целями и мотивами, более того – они рассчитывают на получение имущественной выгоды в особо крупных размерах с учётом стоимости криптовалют; 5) виновные практически во всех изученных случаях используют вредоносные программы, на специальных площадках в сети Интернет созданные и распространённые иными лицами, которые в некоторых случаях не только снабжают виновных соответствующими программами, их составляющими и модулями, обеспечивающими их функциональность, но и инструкциями по применению такого программного обеспечения, а также по сокрытию следов его применения; 6) в целях большего охвата неосведомлённых пользователей и серверов организаций преступники нередко действуют в составе группы – подобные преступные схемы наиболее успешны и устойчивы; 7) негативные последствия соответствующих преступных действий весьма трудно исчислимы: не во всех случаях удаётся установить всех пользователей, чьи компьютеры были заражены; кроме того, при атаке на серверы организаций могут возникать ситуации причинения вреда пользователям виртуальных ресурсов таких организаций, например, при утечке персональных данных или сведений, составляющих банковскую, коммерческую, государственную тайну[4] и т.п., то есть имеется возможность возникновения дополнительных (побочных, латентных) негативных последствий.

С учётом указанных особенностей (особая скрытность соответствующей преступной деятельности и наличие возможностей для её осуществления в течение длительного периода времени) неудивитель-

[2] См.: Приговор Набережночелнинского городского суда Республики Татарстан от 21 февраля 2019 г. по делу № 1-368/19. – URL: http://naberezhno-chelninsky.tat.sudrf.ru/modules.php?name=sdp2_cases#id=3_e82d8173d359e447ec45916fc58a6c01&shard=r16&from=p&r={%22dateValue%22:%2221.02.2019%22} (дата обращения: 18.08.2021).

[3] См., например: Приговор Советского районного суда г. Орла от 13 июня 2019 г. по делу № 1-43/2019. – URL: https://sovetsky--orl.sudrf.ru/modules.php?name=sud_delo&srv_num=1&name_op=doc&number=2593957&delo_id=1540006&new=&text_number=1 (дата обращения: 18.08.2021).

[4] См., например: Приговор Саровского городского суда Нижегородской области от 16 октября 2019 г. по делу № 1-166/2019. – URL: https://sarovsky--nnov.sudrf.ru/modules.php?name=sud_delo&srv_num=1&name_op=doc&number=42125707&delo_id=1540006&new=&text_number=1 (дата обращения: 18.08.2021); Приговор Саровского городского суда Нижегородской области от 24 октября 2019 г. по делу № 1-167/2019. – URL: https://sarovsky--nnov.sudrf.ru/modules.php?name=sud_delo&srv_num=1&name_op=doc&number=63695263&delo_id=1540006&new=&text_number=1 (дата обращения: 18.08.2021).

но, что суды и иные правоприменители уделяют такое пристальное внимание поведению виновных, свидетельствующему об их готовности способствовать изобличению собственных преступных действий, раскрытию деталей преступной активности, а также поиску иных лиц, задействованных в её реализации, и применяют к ним меры поощрения, предусмотренные п. «и» ч. 1 ст. 61 и ч. 1 ст. 62 УК РФ. И, напротив, вызывает сомнения практика применения соответствующих мер к лицам, поведение которых, внешне их напоминая, ничего общего не имеет с явкой с повинной, активным способствованием раскрытию и расследованию преступлений и изобличением соучастников. Приведём пример.

С.С.В., признанный виновным в использовании ВКП из корыстной заинтересованности (ч. 2 ст. 273 УК РФ), скопировал с сайтов сети Интернет компьютерные программы, предназначенные для нейтрализации средств защиты компьютерной информации и скрытого майнинга криптовалюты. Посредством запуска указанных программ он осуществил воздействие на сервер, принадлежащий ПАО «…», получил логин и пароль, необходимые для доступа к названному серверу, осуществил удаленный вход на него и скопировал на указанный сервер ВКП, предназначенную для скрытого майнинга криптовалюты за счёт использования вычислительных мощностей компьютеров ПАО «…», но не смог довести данные действия до конца в связи с пресечением противоправной деятельности сотрудниками ФСБ России. При назначении наказания суд учёл в качестве смягчающих обстоятельств в соответствие с п. «и» ч. 1 ст. 61 УК РФ активное способствование раскрытию и расследованию преступлений, а также согласно ч. 2 ст. 61 УК РФ – признание подсудимым своей вины и раскаяние в содеянном. Кроме того, уголовное дело было рассмотрено в особом порядке по ходатайству подсудимого, который «полностью признал себя виновным в совершении инкриминируемого ему преступления, в содеянном раскаялся». На основании изложенного суд пришёл к выводу о возможности назначения подсудимому С.С.В. наказания с учётом положений ч.ч. 1 и 5 ст. 62 УК РФ[5].

Как представляется, в приведённом выше примере суд излишне при применении ч.ч. 1 и 2 ст. 61 и ч.ч. 1 и 5 ст. 62 учёл в качестве основания для смягчения наказания одно и то же обстоятельство – признательные показания подсудимого, данные им после того, как его действия уже были пресечены сотрудниками правоохранительных органов. Несмотря на позицию Пленума Верховного Суда РФ, содержащуюся в абз. 2 п. 29 Постановления от 22.12.2015 г. № 58[6], признательные показания могут считаться активным способствованием раскрытию и расследованию преступления только в том случае, если согласно п. 30 того же Постановления, такое поведение заключается в предоставлении информации, имеющей значение для раскрытия и расследования соответствующего преступления. В описанных выше условиях указанное просто невозможно, так как сотрудники ФСБ на момент пресечения действий С.С.В. уже располагали информацией о: 1) личности и местонахождении преступника (его действия наверняка были засечены через принадлежащий ему *IP*-адрес, так как С.С.В. запускал программу с принадлежащего ему персонального компьютера); 2) способе и средствах совершения преступления (сотрудники ФСБ отреагировали именно на вредоносную активность на сервере охраняемой организации, то есть имели данные относительно того, что это за программа, для чего она и как её негативное воздействие пресечь и нейтрализовать); 3) времени и месте совершения преступления. В подобных условиях сами по себе признательные показания С.С.В., а точнее даже факт того, что он не отказывался признать себя виновным, нельзя считать значимым для расследования преступления.

Ещё большие сомнения вызывает практика признания наличия явки с повинной в условиях, когда преступник не достиг желаемого результата, так как его попытки несанкционированного доступа к компьютерной информации в целях начала майнинга криптовалюты были пресечены. М.В.А., осуждённый за использование вредоносной компьютерной программы из корыстной заинтересованности (ч. 2 ст. 273 УК РФ), загрузил с неустановленного ресурса, а затем «использовал вредоносные компьютерные программы <…>, совершив незаконные действия, направленные на получение несанкционированного удаленного доступа путем подбора авторизационных данных (логина и пароля) к серверным ЭВМ, имеющим IP-адреса <…>, функционирующим в диапазоне Государственной интегрированной системы телекоммуникаций Республики Татарстан, в целях нейтрализации средств защиты содержащейся на них компьютерной информации и ее последующей несанкционированной модификации путем установки программы-майнера и использования вычислительных мощностей этих ЭВМ при осуществлении майнинга». В качестве смягчающих обстоятельств при назначении наказания в соответствии с п. «и» ч. 1 ст. 61 УК РФ были учтены «явка с повинной, зафиксированная в его письменном опросе, активное способствование расследова-

[5] См.: Приговор Солнечногорского городского суда Московской области от 07 октября 2020 г. по делу № 1-227/2020. – URL: https://solnechnogorsk--mo.sudrf.ru/modules.php?name=sud_delo&srv_num=1&name_op=doc&number=237592748&delo_id=1540006&new=&text_number=1 (дата обращения: 18.08.2021).

[6] См.: Постановление Плеунма Верховного Суда Российской Федерации от 22 декабря 2015 № 58 «О практике назначения судами Российской Федерации уголовного наказания» (с изменениями, внесенными постановлениями Пленума от 29 ноября 2016 г. № 56, от 18 декабря 2018 г. № 43). – URL: http://www.supcourt.ru/documents/own/8470/ (дата обращения: 23.08.2021).

нию преступления», а в соответствии с ч. 2 ст. 61 УК РФ – в том числе, признание вины[7]. Для описания действий М.В.А. здесь неслучайно приведена полная цитата из текста приговора – дело в том, что подобные формулировки свидетельствуют о том, что М.В.А. лишь попытался получить соответствующий доступ путем подбора идентификационных данных с использованием соответствующей ВКП, но, что весьма вероятно, соответствующая попытка успехом не увенчалась благодаря действиям сотрудников правоохранительных органов (информации об этом в тексте судебного решения не содержится – на возможность подобного развития событий указывают приведённые формулировки обвинительного приговора и тот факт, что было осуществлено посягательство на сервер государственного органа). Очевидно, что в полном соответствии с абз. 2 п. 29 Постановления Пленума Верховного Суда РФ от 22.12.2015 г. № 58 в данном и подобных ему случаях признанию наличия явки с повинной препятствует тот факт, что действия преступника были пресечены, и он был задержан сотрудниками правоохранительных органов.

В целом следует согласиться с позицией Пленума Верховного Суда Российской Федерации, вытекающей из системного понимания положений абз. 2 п. 29 и абз. 1 п. 30 Постановления от 22.12.2015 г. № 58: в случае, если признательные показания будут являться значимыми для раскрытия и расследования уголовного дела, они должны быть учтены в качестве активного способствования расследованию, следовательно, при назначении наказания должны быть применены положения ч. 1 ст. 62 УК РФ. В иных случаях их применение не отвечает целям уголовного судопроизводства и противоречит положениям ч. 1 ст. 6 и ч. 1 ст. 7 УК РФ, так как может привести к неоправданному снижению объёма уголовной ответственности. Подобная ситуация может возникнуть ещё и потому, что сам по себе факт признания вины, согласно действующей позиции Пленума Верховного Суда и содержанию положений ч.ч. 1, 2 ст. 61 и ч.ч. 1, 5 ст. 62 УК РФ, признаётся и (или) может быть признан сущностной характеристикой сразу нескольких оснований смягчения наказания.

С.С.А., осуждённый за использование вредоносных компьютерных программ из корыстной заинтересованности (ч. 2 ст. 273 УК РФ), загрузил с неустановленного ресурса сети Интернет и установил на свой персональный компьютер ВКП, а затем с их помощью предпринял попытку получения несанкционированного удаленного доступа путем подбора авторизационных данных (логина и пароля) к серверным компьютерам других пользователей сети Интернет в целях нейтрализации средств защиты содержащейся на них компьютерной информации и ее последующей несанкционированной модификации путем установки программы-майнера и использования вычислительных мощностей этих компьютеров при осуществлении майнинга. Согласно тексту приговора, в качестве смягчающего обстоятельства, предусмотренного п. «и» ч. 1 ст. 61 УК РФ, суд учёл в том числе «признание вины, раскаяние в содеянном, активное способствование расследованию преступления (дача последовательных признательных показаний) (п.п. «г, и» ч. 1 ст. 61 УК РФ)», а при определении размера наказания сослался на положения ч.ч. 1 и 5 ст. 62 УК РФ, так как, наряду с установлением названных выше смягчающих обстоятельств, усмотрел возможность удовлетворения ходатайства С.С.А. о постановлении приговора без проведения судебного разбирательства. Причем последнее из упомянутых решений предваряет указание в тексте приговора на то, что «С.С.А. свою вину в совершении инкриминируемого ему преступления признал полностью и в полном объеме согласился с предъявленным обвинением, пояснив, что действительно при указанных в обвинительном заключении обстоятельствах совершил преступление»[8]. Таким образом, сам по себе факт признания С.С.А. своей вины одновременно трижды был учтён судом (ч. 2 ст. 61, ч. 1 ст. 62 и ч. 5 ст. 62 УК РФ) и в итоге повлиял на назначение подсудимому наказания в условиях, когда такое признание не имело значения для расследования уголовного дела, так как С.С.А. не удалось не только начать процесс создания криптовалюты (конечный желаемый результат), но и в принципе получить доступ к компьютерной информации (промежуточный необходимый результат) – очевидно, его действия были пресечены сотрудниками правоохранительных органов. Следует отметить, что подобные ситуации неоправданного множественного учёта признания вины в качестве основания смягчения наказания распространены в рамках рассматриваемой категории уголовных дел, так как подавляющее их большинство рассматривается с применением особого порядка судопроизводства (из числа изученных судебных решений лишь в одном случае подсудимый своей вины не признал и не согласился с обвинением).

Как уже неоднократно отмечалось выше, с учётом специфики анализируемой преступной схемы стремление преступника сотрудничать со следствием и способствовать расследованию чрезвычайно важно в подобных случаях, поэтому, безусловно, может и должно признаваться особо смягчающим

[7] См.: Приговор Муромского городского суда Владимирской области от 05 декабря 2018 г. по делу № 1-294/2018. – URL: https://muromsky--wld.sudrf.ru/modules.php?name=sud_delo&srv_num=1&name_op=doc&number=6080853&delo_id=1540006&new=&text_number=1 (дата обращения: 18.08.2021).

[8] См.: Приговор Собинского городского суда Владимирской области от 14 декабря 2017 г. по делу № 1-1-276/2017. – URL: https://sobinsky--wld.sudrf.ru/modules.php?name=sud_delo&srv_num=1&name_op=doc&number=1070159&delo_id=1540006&new=&text_number=1 (дата обращения: 18.08.2021).

обстоятельством и поощряться государством посредством смягчения наказания на основании положений ст. 62 УК РФ. Однако в качестве вариантов реализации такого стремления, наряду с простым признанием вины, должно учитываться предоставление сведений о соучастниках преступления, средствах и орудиях его совершения. К примеру, в рамках всех приведённых в данной статье примеров не были установлены источники приобретения виновными соответствующих вредоносных программ, на что указывалось непосредственно в приговоре. В современном мире подобные программы распространяются на специальных хакерских сайтах и теневых виртуальных площадках, администраторов и создателей (владельцев), которых практически невозможно привлечь к уголовной ответственности, а свидетельские показания пользователей вредоносного программного обеспечения могут помочь изобличить таких преступников. Если преступный замысел был доведён до конца, то способствовать расследованию также может предоставление сведений относительно возможных потерпевших (предоставление сведений о заражённых серверах или персональных компьютерах, если атаки были точечными и не были направлены на неопределённый круг пользователей сети Интернет). Во всех подобных случаях требования ст.ст. 6 и 7 УК РФ будут в полной мере соблюдены, так как объём смягчения наказания будет соответствовать уровню снижения степени общественной опасности виновного, доказавшего готовность осудить собственное преступное поведение и ступить на путь исправления.

Литература:

1. Архипов А.В. Цифровые объекты как предмет хищения // Уголовное право. – 2020. – № 6. – С. 16-23.
2. Быкова Е.Г., Казаков А.А. О правовой оценке противоправного безвозмездного изъятия криптовалюты // Уголовное право. – 2018. – № 2. – С. 16-19.
3. Долгиева М.М. Криптовалюта в вопросах судебной практики // Современное право. – 2018. – № 12. – С. 103-108.
4. Ильяшенко Е.А. О перспективах привлечения к уголовной ответственности за использование криптовалют в преступных целях // Российский следователь. – 2018. – № 8. – С. 51-54.

About Special Aspects of the Application Section "i" Part 1 Article 61 of the RF's Criminal Code in the Process of the Criminal Sentencing for the Unauthorized Use of Computing Capacity for Crypto-Mining

Mkrtchian S.M.
Volgograd State University

The article deals with the study of the practice of the application section "i" Part 1 Article 61 of the Criminal Code of the Russian Federation with regard to the mitigating circumstances, listed in its text, in the process of the criminal sentencing for unauthorized use of computing capacity for crypto-mining. It has been established that the courts and other law enforcement officials in some cases do not take into account the special aspects of the mentioned crimes and the personality of the criminals committing it, in the process of determining of the corresponding options of the positive post-offense conduct. The most common law enforcement errors were analyzed; common features were identified that characterize the corresponding criminal acts and their perpetrators, which should be taken into account in deciding the question of the application of the Articles 61 and 62 of the Criminal Code.

Key words: blockchain, cryptocurrencies, mining, malware, unauthorized access to the computer information, positive post-offense conduct