



ВОПРОСЫ ОТЛИЧЕНИЯ ПРЕСТУПЛЕНИЙ ПРОТИВ ПРАВОСУДИЯ ОТ ДРУГИХ ПРЕСТУПЛЕНИЙ СХОДНОГО СОСТАВА В ПРОЦЕССЕ ЦИФРОВИЗАЦИИ

Юсупов Бехзоджон Фархадович

Ташкентский государственный
юридический университет

самостоятельный исследователь

<https://doi.org/10.5281/zenodo.21885071>

Аннотация: в статье рассматриваются вопросы отграничения преступлений против правосудия от сходных составов, предусмотренных иными главами уголовного закона, в условиях цифровизации. Основное внимание уделено непосредственному объекту посягательства, конкуренции общей и специальной норм, совокупности преступлений, процессуальному статусу предмета, режиму охраняемой информации, статусу субъекта и цели деяния.

Ключевые слова: преступления против правосудия, цифровизация, квалификация, смежные составы, непосредственный объект, конкуренция норм, совокупность преступлений, электронные доказательства.

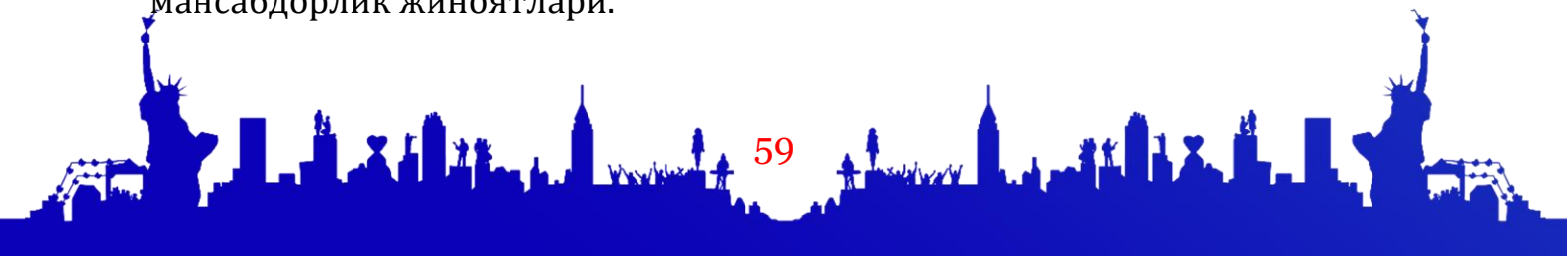
РАҚАМЛАШТИРИШ ЖАРАЁНИДА ОДИЛ СУДЛОВГА ҚАРШИ ЖИНОЯТЛАРНИ БОШҚА ЎХШАШ ТАРКИБЛИ ЖИНОЯТЛАРДАН ФАРҚЛАШ МАСАЛАЛАРИ

Юсупов Бехзоджон Фарҳодович

Тошкент давлат юридик университети
мустақил изланувчиси

Аннотация: мақолада рақамлаштириш шароитида одил судловга қарши жиноятларни Жиноят кодекси Махсус қисмининг бошқа бобларидаги ўхшаш таркиблардан ажратиш масалалари таҳлил қилинган. Фарқлашнинг асосий мезони сифатида қилмишнинг асосий бевосита объекти, шунингдек умумий ва махсус нормалар рақобати, жиноятлар мажмуаси, предметнинг процессуал мақоми, ахборотнинг муҳофаза режими, субъектнинг хизмат ва процессуал мақоми ҳамда қилмиш мақсади ёритилган.

Калит сўзлар: одил судловга қарши жиноятлар, рақамлаштириш, квалификация, ўхшаш таркиблар, асосий бевосита объект, нормалар рақобати, жиноятлар мажмуаси, электрон далил, ахборот тизими, мансабдорлик жиноятлари.





ISSUES OF DIFFERENCING CRIMES AGAINST JUSTICE FROM OTHER CRIMES OF A SIMILAR COMPOSITION IN THE PROCESS OF DIGITALIZATION

Bekhzodjon Farkhodovich Yusupov

Tashkent State University of Law
independent researcher

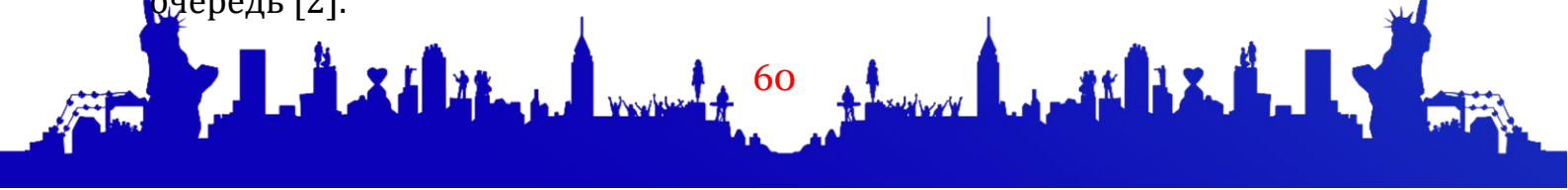
Abstract: the article examines the distinction between crimes against justice and similar offences contained in other chapters of criminal law in the context of digitalization. The analysis focuses on the primary direct object of encroachment, competition between general and special norms, concurrence of offences, the procedural status of an object, the legal regime of protected information, the status of the offender and the purpose of the act.

Keywords: crimes against justice, digitalization, legal qualification, similar offences, direct object, competition of norms, concurrence of crimes, electronic evidence, information system.

ВВЕДЕНИЕ

Точное отграничение преступлений против правосудия от иных смежных составов относится к числу наиболее сложных направлений уголовно-правовой квалификации. Во многих случаях указанные деяния по внешней форме, способу совершения либо субъекту сходны с преступлениями в сфере информационных технологий, должностными преступлениями, подделкой документов, разглашением охраняемой законом информации, преступлениями против личности или порядка управления, а также легализацией доходов, полученных преступным путем. Неправильное разграничение может повлечь необоснованное расширение либо сужение объема уголовной ответственности, утрату направленности деяния против правосудия и формирование неоднородных подходов в судебной практике [1].

В цифровой среде данная проблема приобретает еще большую остроту. Объекты, ранее обладавшие различной правовой природой, в электронной форме объединяются: электронный документ одновременно может являться официальным документом, компьютерной информацией и доказательством по конкретному делу. Поэтому разграничения, основанного лишь на внешних признаках, недостаточно; необходимо установить внутреннюю юридическую направленность деяния и определить, на какие общественные отношения оно посягает в первую очередь [2].





При отграничении смежных составов необходимо различать две правовые ситуации. В первой одно деяние формально соответствует признакам нескольких норм, однако между ними возникает конкуренция. В таком случае содеянное квалифицируется по норме, наиболее полно и специально охватывающей деяние. Во второй ситуации совершается несколько деяний, направленных на различные самостоятельные объекты, либо одним деянием причиняется самостоятельный вред нескольким объектам; в этом случае применяются правила о совокупности преступлений [3].

Основным критерием отграничения выступает основной непосредственный объект. Если первичная и преобладающая направленность деяния связана с общественными отношениями, обеспечивающими осуществление правосудия, производство расследования, достоверность доказательств, процессуальную тайну либо исполнение судебного акта, применяется норма Уголовного кодекса о преступлениях против правосудия. Если же основное посягательство направлено на безопасность компьютерной информации, государственную службу, экономический оборот, здоровье личности или порядок управления, приоритет имеет соответствующая иная норма. При причинении самостоятельного вреда обоим объектам возникает совокупность преступлений [4].

На практике данный подход может быть представлен в виде четырехэтапного алгоритма. Сначала определяется основной непосредственный объект. Затем устанавливается наличие специальной нормы, полностью охватывающей деяние. На третьем этапе оценивается самостоятельное юридическое значение вреда, причиненного иному объекту. Наконец, определяются статус субъекта, форма вины и цель деяния. Такая последовательность снижает степень субъективизма и способствует единообразной квалификации.

Отграничение от преступлений в сфере информационных технологий

В условиях цифровизации наиболее часто возникает пересечение с составами неправомерного доступа к компьютерной информации, ее модификации, компьютерного саботажа и использования вредоносных программ. Нормы о преступлениях в сфере информационных технологий охраняют целостность, конфиденциальность и доступность компьютерной информации. Нормы о преступлениях против правосудия, независимо от





технической природы электронного объекта, защищают его процессуальную функцию и роль в осуществлении правосудия.

Например, если посредством внесения изменений в электронный файл фальсифицировано доказательство по делу, в центре деяния находится посягательство на достоверность доказательства, и оно подлежит квалификации по статье 230¹ УК. Если такое изменение совершено путем неправомерного доступа к системе, принадлежащей другому лицу, и одновременно причинен самостоятельный вред информационной безопасности, возможна квалификация по совокупности с нормой о модификации компьютерной информации. Напротив, если уполномоченное лицо искажает электронное доказательство в пределах предоставленного ему законного доступа, состав компьютерного преступления отсутствует, а деяние квалифицируется только как фальсификация доказательств.

То же правило применимо к сокрытию преступления в электронном реестре, разглашению данных расследования через сеть, вмешательству в системы электронного судопроизводства или исполнения судебных актов. Доступ к компьютерной системе в таких случаях нередко является не самостоятельной целью, а способом совершения преступления против правосудия. Если этот способ не влечет самостоятельных общественно опасных последствий, он может охватываться составом основного преступления; при причинении отдельного вреда информационной системе применяются правила о совокупности.

Граница между компьютерным саботажем и вмешательством в процессуальную деятельность определяется на той же основе. Если основная цель вывода из строя судебной либо исполнительной системы состоит в воспрепятствовании процессуальному действию, приоритет имеет норма о вмешательстве в осуществление правосудия. Если вред работоспособности системы приобретает самостоятельное значение, деяние дополнительно квалифицируется как компьютерный саботаж.

Указанные пересечения можно подразделить на три вида: пересечение предметов, пересечение способов и пересечение последствий. При пересечении предметов один электронный объект одновременно является доказательством и компьютерной информацией. При пересечении способов компьютерное деяние выступает средством совершения преступления против правосудия. При пересечении последствий одно действие причиняет самостоятельный вред двум различным объектам.





Такая типология позволяет определить действительный уголовно-правовой объем цифрового деяния.

Отграничение от должностных преступлений

Фальсификация доказательств или результатов оперативно-розыскной деятельности, разглашение данных расследования и умышленное сокрытие преступления от учета нередко совершаются должностным лицом. Поэтому внешне они сходны со злоупотреблением должностными полномочиями, превышением власти или должностных полномочий, должностным подлогом и халатностью.

Решающим здесь является соотношение общей и специальной норм. Должностные преступления в общем виде охватывают нарушения закона в сфере служебной деятельности. Нормы о преступлениях против правосудия специально криминализуют конкретные действия должностного лица именно в сфере расследования, судебного разбирательства, доказательств, процессуальной тайны либо учета преступлений. Поэтому фальсификация доказательств следователем квалифицируется не как должностной подлог, а по статье 230¹ УК; умышленное неотражение преступления в учете — не как общее злоупотребление полномочиями, а по статье 241¹ УК.

Если должностное деяние в сфере правосудия не предусмотрено специальной нормой, может применяться общий состав должностного преступления. Следовательно, первым условием правильной квалификации является проверка наличия специальной нормы. Если специальная норма полностью охватывает содеянное, общая норма не применяется.

Форма вины также может служить критерием отграничения. Умышленное невнесение сведений о преступлении в электронный реестр охватывается статьей 241¹ УК, тогда как нерегистрация вследствие небрежности либо отсутствия надлежащего технического контроля может оцениваться в рамках нормы о халатности. Кроме того, если преступление против правосудия совершается за взятку, возникает совокупность получения взятки и преступления против правосудия, поскольку эти деяния посягают на различные объекты.

В цифровом делопроизводстве возможна и трехсторонняя конкуренция: должностное лицо злоупотребляет полномочиями в электронной системе, реализует специальный состав преступления против правосудия и причиняет вред информационной безопасности. В таком





случае прежде всего устанавливается специальная норма о преступлении против правосудия, затем, при наличии самостоятельных признаков компьютерного преступления, применяется совокупность; общая норма о должностном преступлении имеет значение лишь в части, не охваченной специальным составом.

Отграничение от подделки документов

Фальсификация доказательств и результатов оперативно-розыскной деятельности внешне сходна с подделкой документов, печатей, штампов и бланков. В обоих случаях создается объект с ложным содержанием либо изменяется существующий объект. Однако предмет и объект уголовно-правовой охраны этих преступлений различаются.

Предметом преступления, предусмотренного статьей 230¹ УК, является доказательство, подтверждающее либо опровергающее обстоятельство, имеющее значение в конкретном производстве. Предметом статьи 228 УК могут выступать официальный документ, печать, штамп или бланк вне рамок конкретного процесса. Поэтому основным критерием отграничения является наличие у подделанного объекта статуса доказательства по определенному делу. Если подложный документ изготовлен вне производства, а затем представлен в качестве доказательства, с момента приобретения им процессуального статуса содеянное оценивается в рамках состава преступления против правосудия.

Различие между материальным и интеллектуальным подлогом здесь имеет второстепенное значение. Изменение подписи, печати или даты документа представляет собой материальный подлог, а внесение ложных сведений в документ, формально составленный надлежащим образом, — интеллектуальный подлог. Фальсификация доказательств может охватывать обе формы; определяющим является использование объекта в качестве процессуального доказательства.

В электронных документах функцию внешних реквизитов выполняют электронная подпись, отметка времени и метаданные. Их искажение может одновременно содержать признаки подделки документа и воздействия на компьютерную информацию. Если подложный электронный документ представлен как доказательство по конкретному делу, применяется статья 230¹ УК; если это поддельная электронная справка или разрешение, предназначенные для общего оборота, — статья 228 УК. При введении в процесс созданных с помощью искусственного интеллекта дипфейк-аудио или видео решающим также является их процессуальный статус.





Отграничение от преступлений, связанных с разглашением охраняемой законом информации

Разглашение данных расследования или судебного разбирательства сходно с разглашением государственной, коммерческой или банковской тайны, а также персональных данных. Во всех случаях информация распространяется вопреки установленному законом режиму. Отграничение начинается с определения вида разглашенных сведений и правовой цели их охраны.

В статье 239 УК конфиденциальность информации устанавливается для обеспечения законного хода расследования и судебного разбирательства. Охрана государственной тайны служит интересам государственной безопасности, коммерческой и банковской тайны — экономической деятельности, персональных данных — неприкосновенности частной жизни. Если информация охраняется как составная часть материалов дела в интересах правосудия, ее разглашение прежде всего подлежит квалификации по статье 239 УК.

В цифровой среде единичная утечка данных может одновременно охватывать тайну следствия, персональные данные, коммерческую или государственную тайну. Если каждому самостоятельному режиму охраны информации причинен отдельный вред, возможна идеальная совокупность преступлений. Если же основным правовым режимом всех сведений является конфиденциальность в рамках конкретного расследования, по критерию основного объекта приоритет имеет статья 239 УК.

Важное значение имеет и правовая связь субъекта с информацией. Обязанность не разглашать данные расследования вытекает из процессуального предупреждения либо служебных обязанностей. При отсутствии такого условия содеянное может образовывать не преступление против правосудия, а иной состав разглашения охраняемой тайны. С учетом повышенной опасности распространения в электронной форме значительного объема данных предлагается предусмотреть такое обстоятельство в качестве квалифицирующего признака.

Отграничение от преступлений против личности и порядка управления

Вмешательство в расследование, судебное разбирательство или исполнение судебного акта нередко осуществляется путем угроз, запугивания либо насилия. Поэтому оно пересекается с преступлениями против жизни и здоровья личности, а также с преступлениями против





порядка управления, включая применение насилия в отношении представителя власти. При отграничении необходимо установить, к кому, в связи с чем и с какой целью применено насилие.

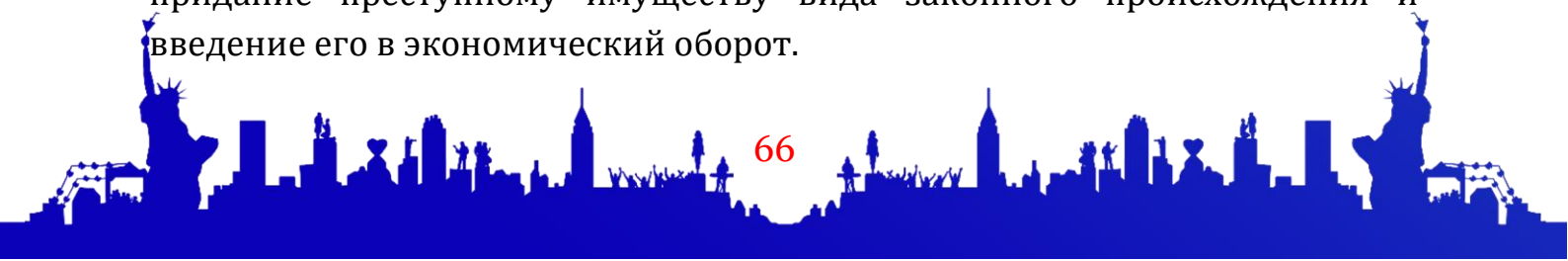
Если угроза или насилие применяются с целью принудить судью, следователя либо дознавателя к принятию определенного процессуального решения или воздействовать на объективность его деятельности, содеянное оценивается как вмешательство в осуществление правосудия. Если насилие влечет самостоятельные тяжкие последствия, в том числе причинение тяжкого телесного повреждения, применяется совокупность с соответствующим преступлением против личности. Угроза судье, обусловленная личным конфликтом, образует преступление против личности, тогда как угроза в связи с его судебной деятельностью подпадает под статью 236 УК.

Онлайн-угрозы оцениваются по тем же критериям. Уголовно-правовая природа давления, осуществленного посредством электронной почты, мессенджера или социальной сети, определяется не цифровой формой средства, а его направленностью на процессуальную деятельность. Поскольку использование информационно-коммуникационных систем повышает скрытность деяния и масштаб воздействия, оно может быть предусмотрено в качестве квалифицирующего признака.

При отграничении вмешательства в исполнение судебных актов от преступлений против порядка управления существенное значение имеет правовая природа исполняемого документа. Если воспрепятствование направлено на принудительное исполнение судебного акта, применяется статья 232¹ УК; если оно касается общей управленческой деятельности либо исполнения решения иного органа, применяется соответствующая норма о преступлении против порядка управления.

Отграничение от легализации доходов, полученных преступным путем

Соккрытие орудий, следов преступления либо имущества, полученного преступным путем, внешне близко к легализации преступных доходов. В обоих случаях лицо совершает действия с имуществом или иным объектом, возникшим в результате другого преступления. Однако цель укрывательства состоит в воспрепятствовании раскрытию преступления либо изобличению преступника, тогда как легализация направлена на придание преступному имуществу вида законного происхождения и введение его в экономический оборот.





Если лицо прячет имущество в месте, исключающем его обнаружение, либо уничтожает следы его происхождения, содеянное подпадает под статью 241 УК. Если же посредством фиктивных сделок, финансовых операций или иных способов имуществу придается законный вид, применяется статья 243 УК. Если укрывательство впоследствии перерастает в легализацию и два этапа причиняют вред различным общественным отношениям, возможна реальная совокупность преступлений.

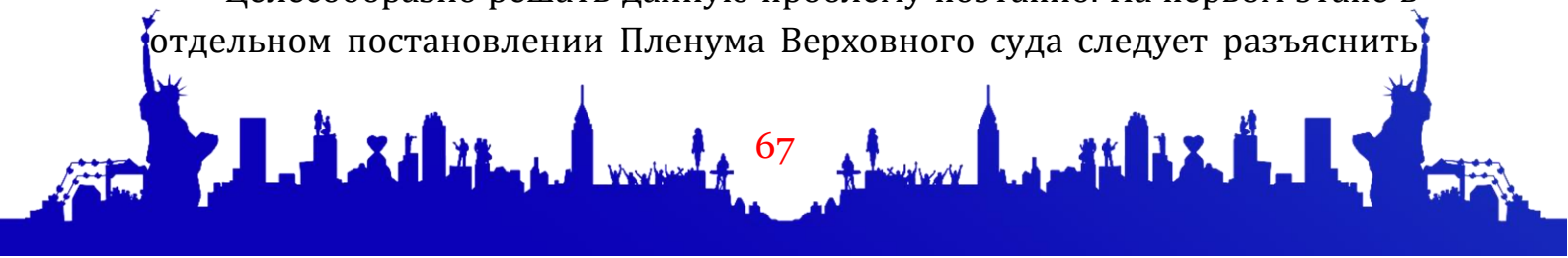
В цифровой экономике криптоактивы и электронные платежные средства размывают эту границу. Одна операция может одновременно служить сокрытию электронного следа и введению преступного имущества в экономический оборот. В таком случае устанавливается преобладающая цель: если на первом плане находится воспрепятствование раскрытию преступления, содеянное оценивается как укрывательство; если преобладает цель придания имуществу устойчивого законного вида — как легализация.

Сохраняется и граница между прикосновенностью к преступлению и соучастием. Обещание скрыть преступление или оказать содействие, данное до его совершения, образует соучастие, тогда как укрывательство, совершенное после преступления без заранее данного обещания, является самостоятельной формой прикосновенности. Использование цифровых средств не изменяет данный критерий; электронная переписка и следы транзакций имеют значение для установления времени и содержания обещания.

Направления совершенствования законодательства и правоприменения

Основная проблема отграничения цифровых деяний заключается в асимметрии между материальным уголовным и процессуальным законодательством. Несмотря на признание процессуальным законом электронных доказательств и цифровой информации, составы фальсификации, укрывательства и разглашения по-прежнему ограничены традиционными понятиями «документ», «предмет» и «сведения». Это создает риск необоснованного отнесения цифрового деяния к компьютерному преступлению или подделке документов либо, напротив, необоснованной квалификации одного деяния по совокупности.

Целесообразно решать данную проблему поэтапно. На первом этапе в отдельном постановлении Пленума Верховного суда следует разъяснить





критерии отграничения посягательств на электронные доказательства, электронные реестры и электронные системы от преступлений против правосудия и преступлений в сфере информационных технологий. В нем необходимо четко сформулировать правила определения основного непосредственного объекта, соотношения способа и цели, приоритета специальной нормы и совокупности преступлений.

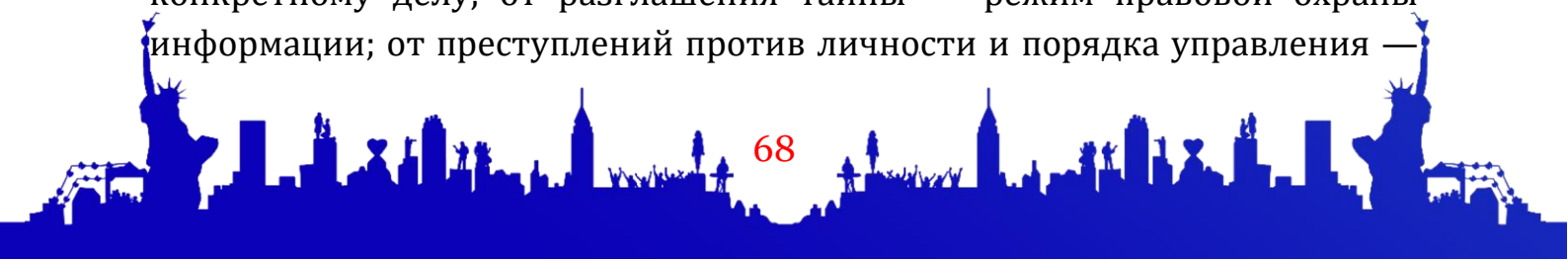
На втором этапе в предмет преступлений, предусмотренных статьями 230¹, 230² и 241¹ УК, необходимо прямо включить электронный документ, метаданные, запись электронного реестра и цифровой контент, созданный с использованием искусственного интеллекта. В статьях 236, 232¹ и 239 УК совершение деяния с использованием информационно-коммуникационных систем может быть предусмотрено в качестве квалифицирующего признака. Такие изменения позволят более четко отграничивать посягательства на цифровые объекты от компьютерных преступлений и подделки документов.

Правильность квалификации зависит не только от текста закона, но и от практики исследования электронных доказательств, сохранения цифровых следов и проведения судебно-технической экспертизы. Поэтому для правоприменительных органов необходимо разработать единые методические рекомендации, направленные на установление процессуального статуса электронного объекта, права доступа к информации, механизма внесения изменений и цели деяния.

ЗАКЛЮЧЕНИЕ

Цифровизация не отменяет традиционных критериев отграничения преступлений против правосудия от иных смежных составов. Напротив, основной непосредственный объект, соотношение общей и специальной норм, совокупность преступлений, статус субъекта, форма вины, процессуальная функция предмета и цель деяния приобретают в цифровой среде еще большее значение.

При отграничении от преступлений в сфере информационных технологий решающими являются процессуальная роль электронного объекта и то, выступает ли неправомерный доступ способом совершения преступления либо самостоятельным посягательством; от должностных преступлений — приоритет специальной нормы и форма вины; от подделки документов — статус объекта как доказательства по конкретному делу; от разглашения тайны — режим правовой охраны информации; от преступлений против личности и порядка управления —





процессуальная цель; от легализации — экономическая направленность деяния.

Пока не устранено цифровое несоответствие между материальным и процессуальным законодательством, сохраняется риск различной квалификации одинаковых деяний. Поэтому прямое закрепление электронных объектов в качестве предметов соответствующих составов преступлений, определение уголовно-правового значения использования информационных систем и утверждение на уровне Пленума Верховного суда единого алгоритма отграничения являются необходимыми условиями справедливого и стабильного правоприменения.

