Дата поступления рукописи в редакцию: 01.04.2025 г. DOI: 10.24412/2782-3830-2025-4-225-230
Дата принятия рукописи в печать: 13.05.2025 г.

ТАРНОВСКИЙ Александр Владимирович,
аспирант кафедры уголовного права ФГБОУ ВО
«Юго-Западный государственный университет»,
e-mail: ccpupt@mail.ru

ПРОБЛЕМЫ КВАЛИФИКАЦИИ МАЛОЗНАЧИТЕЛЬНЫХ ДЕЯНИЙ ПРИ СОВЕРШЕНИИ ПРЕСТУПЛЕНИЙ В КИБЕРПРОСТРАНСТВЕ

Аннотация. *В статье рассматриваются проблемы квалификации малозначительных деяний при совершении преступлений в киберпространстве. Анализируются сложности определения общественной опасности правонарушений, совершаемых с использованием информационных технологий, обусловленные нематериальным характером причиняемого вреда и трудностями фиксации последствий в цифровой среде.*

При написании статьи применялись методы системного анализа, сравнительно-правовой метод, формально-юридический метод и метод правового моделирования. Системный анализ позволил комплексно рассмотреть проблему квалификации малозначительных деяний в контексте киберпреступности. Сравнительно-правовой метод использовался для сопоставления традиционных критериев оценки общественной опасности с особенностями цифровой среды. Формально-юридический метод применялся при анализе действующего уголовного законодательства и выявлении пробелов правового регулирования. Метод правового моделирования использовался для разработки предложений по совершенствованию уголовно-правовых норм.

Научная новизна исследования заключается в обосновании необходимости учета нематериального вреда при квалификации малозначительных деяний, совершенных в киберпространстве. Предложено внести дополнения в ст. 14 УК РФ, устанавливающие, что нарушение конфиденциальности информации, компрометация персональных данных, подрыв деловой репутации и разглашение охраняемой законом тайны свидетельствуют о повышенной общественной опасности деяния, исключающей возможность признания его малозначительным. Сделан вывод о необходимости ужесточения уголовной ответственности за преступления, посягающие на информационную безопасность, путем усиления санкций, введения дополнительных видов наказаний и криминализации новых способов совершения правонарушений в цифровой среде.

Ключевые слова*: малозначительность деяния, киберпреступность, информационные технологии, общественная опасность, нематериальный вред, уголовная ответственность, квалификация преступлений, цифровая среда, совершенствование законодательства, противодействие преступности.*

TARNOVSKY Alexander Vladimirovich,
graduate student of the Department of Criminal Law
of the Federal State Budgetary Educational Institution of Higher Education
“Southwestern State University”

PROBLEMS OF QUALIFICATION OF MINOR ACTS IN THE COMMISSION OF CRIMES IN CYBERSPACE

Annotation. *The article examines the problems of qualifying minor acts when committing crimes in cyberspace. It analyzes the difficulties of determining the public danger of offenses committed using information technologies, due to the intangible nature of the harm caused and the difficulties of fixing the consequences in the digital environment.*

When writing the article, the methods of system analysis, the comparative legal method, the formal legal method and the method of legal modeling were used. Systematic analysis made it possible to comprehensively consider the problem of qualifying minor acts in the context of cybercrime. The comparative legal method was used to compare traditional criteria for assessing public danger

with the characteristics of the digital environment. The formal legal method was used to analyze the current criminal legislation and identify gaps in legal regulation. The legal modeling method was used to develop proposals for improving criminal law.

The scientific novelty of the study lies in the justification of the need to take into account intangible harm when qualifying minor acts committed in cyberspace. It was proposed to make additions to Art. 14 of the Criminal Code of the Russian Federation, establishing that violation of confidentiality of information, compromise of personal data, undermining business reputation and disclosure of secrecy protected by law indicate an increased public danger of an act that excludes the possibility of recognizing it as insignificant. It was concluded that it is necessary to toughen criminal liability for crimes encroaching on information security by strengthening sanctions, introducing additional types of punishments and criminalizing new ways of committing offenses in the digital environment.

Key words*: insignificance of the act, cybercrime, information technology, public danger, intangible harm, criminal liability, qualification of crimes, digital environment, improvement of legislation, combating crime.*

Согласно положениям части 2 статьи 14 Уголовного кодекса Российской Федерации (далее – УК РФ), деяние (действие или бездействие), которое хотя формально и содержит признаки преступления, предусмотренного данным Кодексом, но вследствие своей малозначительности не представляет общественной опасности, не признается преступлением. Малозначительное деяние характеризуется тем, что оно совершается с прямым умыслом и включает все объективные и субъективные признаки состава преступления, установленные уголовным законом, однако отсутствуют общественно опасные последствия в виде причиненного ущерба либо реальной угрозы его причинения охраняемым общественным отношениям.

Малозначительность деяния предполагает отсутствие существенного вреда или угрозы причинения вреда охраняемым законом интересам, несмотря на формальное соответствие признакам конкретного состава преступления [1, с. 32]. Это означает, что при оценке общественной опасности содеянного необходимо учитывать реальный характер и степень вреда, причиненного либо могущего быть причиненным объекту уголовно-правовой охраны. Применение данной нормы позволяет дифференцировать уголовную ответственность и исключить привлечение к ней лиц, чьи действия не представляют существенной угрозы для общества.

Для признания деяния малозначительным и, следовательно, не образующим состава преступления, необходимо наличие двух обязательных условий:

1. Формальное соответствие признакам преступления, предусмотренного УК РФ. Это означает, что деяние объективно подпадает под диспозицию соответствующей уголовно-правовой нормы, то есть содержит все необходимые объективные и субъективные признаки состава преступления, установленные законом [2, с. 26].
2. Отсутствие общественной опасности деяния. Деяние не причиняет вреда охраняемым законом общественным отношениям и не создает реальной угрозы такого причинения. Таким образом, несмотря на формальное соответствие признакам преступления, деяние не оказывает негативного влияния на общественные интересы и не влечет существенных последствий для общества [3, с. 284].

Данное положение отражает фундаментальный принцип уголовного права, согласно которому преступлением признается лишь деяние, обладающее общественной опасностью. Малозначительность деяния исключает его преступность, несмотря на формальное соответствие признакам состава преступления, поскольку отсутствует существенное нарушение либо реальная угроза нарушения охраняемых уголовным законом общественных отношений.

Таким образом, даже если деяние формально подпадает под диспозицию уголовно-правовой нормы, но не причиняет значимого вреда или угрозы его причинения объекту уголовно-правовой охраны, оно не может быть признано преступлением. Этот подход обеспечивает дифференциацию уголовной ответственности и предотвращает неоправданное уголовное преследование лиц за действия, не представляющие существенной общественной опасности, что соответствует принципам гуманизма и справедливости уголовного права.

Глобальное распространение современных информационных технологий не только стимулировало прогрессивное развитие цивилизации, но и привело к возникновению ряда негативных последствий. Одним из наиболее значимых является ежегодно возрастающая динамика преступлений в сфере информационно-коммуникационных технологий, которые представляют собой обратную сторону процесса технологического прогресса [4, с. 85].

Рост числа преступлений в цифровой сфере обусловлен использованием информационных технологий в противоправных целях, что порождает серьезные вызовы для правовой системы [5, с. 136]. В связи с этим актуализируется необходимость разработки эффективных правовых механизмов, направленных на предупреждение, выявление и пресечение преступлений, совершаемых с использованием информационно-коммуникационных технологий.

Таким образом, несмотря на положительный вклад информационных технологий в развитие общества, негативные явления, связанные с их неправомерным использованием, требуют особого внимания со стороны юридической науки и практики. Это предполагает комплексное правовое осмысление проблем, возникающих в цифровом пространстве, и совершенствование законодательства для обеспечения надлежащей защиты прав и законных интересов граждан и организаций в условиях информационного общества.

Проблема криминализации деяний является одним из центральных вопросов в сфере уголовной политики. Эффективность практического решения задач, связанных с криминализацией, во многом обусловлена качеством законодательного регулирования. Это включает разработку критериев для оценки характера и степени общественной опасности деяний, установление оснований их признания преступными, а также определение условий и оснований привлечения к уголовной ответственности.

Кроме того, успешное разрешение данной проблемы зависит от правовой регламентации действий, которые вследствие своей малозначительности не представляют общественной опасности. Регулирование и правоприменение непреступных уголовно-правовых деяний, как справедливо отмечает Д.А. Гарбатович, играет существенную роль в обеспечении справедливости и эффективности применения уголовно-правовых норм [6, с. 25].

Необходимо отметить, что наличие в уголовном законодательстве нормы о малозначительности деяния способствует уменьшению числа преступлений путем исключения из категории уголовно наказуемых тех действий, которые, хотя формально и соответствуют признакам состава преступления, предусмотренного законом, однако вследствие своей малозначительности не представляют общественной опасности (согласно части 2 статьи 14 УК РФ). Таким образом, случаи хищения чужого имущества, ущерб от которых превышает определенную сумму, в большинстве случаев не признаются малозначительными.

В контексте киберпространства определение общественной опасности деяния представляет особую сложность, обусловленную спецификой виртуальной среды:

- Нематериальный характер деяния: причиненный ущерб может выражаться в утрате или незаконном распространении информации, ущербе деловой репутации, компрометации конфиденциальных данных, что затрудняет количественную оценку вреда в материальном выражении [7, с. 51].
- Сложности фиксации последствий: установление и документирование реальных ущербов, причиненных в цифровой среде, сопряжены с техническими трудностями и требуют специальных знаний в области информационных технологий. Это осложняет процесс объективной оценки степени общественной опасности деяния и влияет на корректность его правовой квалификации [8, с. 187].
- Отсутствие непосредственного контакта: преступник и потерпевший не взаимодействуют физически, что затрудняет идентификацию субъекта преступления, сбор доказательственной базы и установление причинно-следственной связи между действиями виновного лица и наступившими неблагоприятными последствиями для конкретного субъекта или охраняемого законом интереса [9, с. 118].

По мнению А.К. Клименко, включение безналичных и электронных денежных средств в качестве предмета хищения существенно повышает общественную опасность соответствующих противоправных деяний. Превышение установленного порога стоимости в 2 500 рублей, по его мнению, однозначно свидетельствует о высокой степени общественной опасности преступления.

Для формирования единообразной правоприменительной практики при квалификации хищений безналичных и электронных денежных средств, достигающих уровня уголовно наказуемого деяния, а также для выявления случаев хищений, которые вследствие малозначительности не представляют общественной опасности и не являются преступлениями, необходимо учитывать повышенную степень общественной опасности такого предмета преступления, как безналичные и электронные денежные средства, по сравнению с наличными. В этой связи представляется обоснованным установить для хищений безналичных и электронных денежных средств, имеющих криминальный характер, стоимостный порог в размере 1 000 рублей. Данное предложение обусловлено необходимостью государства способствовать развитию среды, укрепляющей

доверие граждан к цифровым технологиям, и обеспечивать защиту их имущественных интересов в сфере электронных финансовых операций. Таким образом, при совершении хищения указанных денежных средств на сумму 1 000 рублей и более должно возбуждаться уголовное дело, проводиться установление лица, совершившего преступление, и в последующем обеспечиваться возмещение причиненного ущерба в порядке, предусмотренном уголовным и уголовно-процессуальным законодательством [10, с. 32].

Представляется, что данный подход не является вполне обоснованным, поскольку большинство преступлений, совершаемых в сети Интернет, сопровождаются значительно более высоким совокупным ущербом. В связи с этим возникает необходимость соотнесения установленных стоимостных порогов, таких как сумма в 1 000 рублей, с реальными масштабами и особенностями киберпреступности. Более того, при квалификации содеянного следует учитывать индивидуальные обстоятельства каждого конкретного случая.

Следует отметить, что сумма в 1 000 рублей может обладать существенным значением для потерпевшего в определенный момент времени. К примеру, если указанные денежные средства являлись последними на его счету до получения заработной платы или пенсии, их утрата способна привести к серьезным негативным последствиям для его жизнедеятельности. В подобных обстоятельствах говорить о малозначительности деяния, исключающей уголовную ответственность, не представляется возможным, поскольку причиненный вред имеет реальный и ощутимый характер.

Кроме того, при оценке общественной опасности деяния необходимо принимать во внимание не только материальный ущерб, выраженный в количественных показателях, но и его качественные характеристики. К таким характеристикам относятся социально-экономическое положение потерпевшего, значимость утраченных средств для обеспечения его основных жизненных потребностей, а также общая обстановка совершения преступления. Такой подход соответствует принципам справедливости и индивидуализации уголовной ответственности

Установление единого стоимостного порога для квалификации хищений безналичных и электронных денежных средств без учета специфики киберпреступлений может привести к недостаточной защите прав и законных интересов граждан. Преступления, совершаемые в киберпространстве, часто характеризуются массовостью и трансграничностью, что увеличивает их общественную опасность и осложняет процесс привлечения виновных к ответственности.

В этой связи представляется целесообразным предоставлять судам возможность исходить из обстоятельств каждого конкретного случая при оценке малозначительности деяния. Такой подход позволит учитывать все фактические данные дела, в том числе величину причиненного ущерба, значимость утраченных средств для потерпевшего, способ совершения преступления и степень вины правонарушителя.

Учет индивидуальных особенностей дела способствует более справедливому применению уголовного закона и обеспечивает баланс между публичными интересами и правами личности. Это соответствует правовым позициям Верховного Суда Российской Федерации, который неоднократно указывал на необходимость учитывать при назначении наказания характер и степень общественной опасности преступления, личность виновного и иные обстоятельства, влияющие на степень ответственности.

Таким образом, при квалификации малозначительных деяний, совершенных в киберпространстве, следует избегать механистического применения стоимостных критериев и обращаться к содержательной оценке общественной опасности деяния. Это позволит обеспечить эффективную уголовно-правовую защиту прав и законных интересов граждан в условиях развития цифровых технологий и повышения значимости электронных средств платежа в экономической жизни общества.

Нематериальный характер рассматриваемых правонарушений заключается в том, что причиненный вред проявляется через утрату или незаконное распространение информации, подрыв деловой репутации, компрометацию конфиденциальных данных. Эти обстоятельства создают сложности при количественной оценке ущерба в материальном выражении, поскольку вред не всегда может быть исчислен в денежном эквиваленте.

Высокий уровень общественной опасности хищений безналичных и электронных денежных средств, посягающих не только на имущественные права, но и нарушающих банковскую тайну, был прямо отмечен в пояснительной записке к проекту Федерального закона «О внесении изменений в Уголовный кодекс Российской Федерации» (в части усиления уголовной ответственности за хищение денежных средств с банковского счёта или электронных денежных средств). Данная оценка подчёркивает необходимость усиления уголовно-правового воздействия на лиц, совершающих преступления в сфере информационных технологий и электронных финансов, учитывая их потенциально серьёзные последствия для финансовой системы и общества в целом.

В свете изложенного представляется обоснованным предложить внесение дополнений в статью 14 УК РФ, устанавливающих, что при оценке малозначительности деяния, совершённого с использованием информационно-телекоммуникационных сетей, следует учитывать не только размер причинённого материального ущерба, но и характер и степень нематериального вреда. В качестве критерия целесообразно закрепить положение, согласно которому нарушение конфиденциальности информации, компрометация персональных данных, подрыв деловой репутации, а также разглашение банковской, коммерческой или иной охраняемой законом тайны свидетельствуют о повышенной общественной опасности деяния, исключающей возможность признания его малозначительным.

Обоснование данного подхода заключается в том, что в условиях цифровизации общества нематериальный вред, причиняемый преступлениями в киберпространстве, зачастую имеет более серьезные и длительные последствия, чем материальный ущерб. Нарушение права на неприкосновенность частной жизни, утрата доверия к информационным системам, подрыв авторитета и деловой репутации организаций способны привести к существенным негативным изменениям в социальной и экономической сферах. Учет нематериального вреда при квалификации деяния обеспечит справедливое и соразмерное применение уголовно-правовых мер, усилит защиту прав и законных интересов граждан и юридических лиц, а также будет способствовать эффективному противодействию киберпреступности.

Учитывая повышенную общественную опасность преступлений, посягающих на информационную безопасность и нарушающих банковскую тайну, представляется необходимым внести изменения в Уголовный кодекс Российской Федерации с целью усиления уголовной ответственности за такие деяния. Предлагается ужесточить санкции по соответствующим статьям, увеличив размеры штрафов и сроки лишения свободы, а также предусмотреть дополнительные виды наказаний, включая запрет на определенные виды профессиональной деятельности. Кроме того, целесообразно дополнить Особенную часть Кодекса новыми составами преступлений, отражающими современные способы совершения правонарушений в сфере информационных технологий, такие как неправомерный доступ к критической информационной инфраструктуре или использование цифровых технологий для совершения финансовых махинаций. Данные меры обеспечат адекватную уголовно-правовую реакцию на киберпреступления и усилят защиту прав и законных интересов граждан и организаций в цифровой среде.

Проведённое исследование свидетельствует о том, что для решения проблемы определения малозначительности деяния в контексте преступлений, совершаемых в киберпространстве, необходим комплексный подход, учитывающий специфику цифровой среды. Традиционные критерии оценки общественной опасности, основанные на размере материального ущерба, не позволяют в полной мере отразить характер и степень вреда, причиняемого правонарушениями в сфере информационных технологий. Нематериальные последствия, такие как нарушение конфиденциальности, компрометация персональных данных и подрыв деловой репутации, способны оказывать более серьёзное негативное влияние на общественные отношения, чем прямые имущественные потери.

В связи с этим возникает необходимость внесения изменений в уголовное законодательство, направленных на установление дополнительных критериев малозначительности деяния в отношении преступлений, совершённых с использованием информационно-телекоммуникационных сетей. Закрепление положения о том, что нарушение неприкосновенности частной жизни, разглашение законодательно охраняемой тайны и причинение иного нематериального вреда исключают возможность признания деяния малозначительным, обеспечит справедливое и соразмерное применение уголовно-правовых мер. Это усилит защиту прав и законных интересов граждан и организаций в условиях цифровизации общества.

Кроме того, повышенная общественная опасность преступлений, посягающих на информационную безопасность и нарушающих банковскую тайну, обуславливает необходимость ужесточения уголовной ответственности за подобные деяния. Ужесточение санкций, введение дополнительных видов наказаний и криминализация новых способов совершения правонарушений в цифровой среде позволят обеспечить эффективное противодействие киберпреступности и адекватную уголовно-правовую охрану общественных отношений в сфере информационных технологий. Реализация предложенных мер будет способствовать укреплению правопорядка и формированию безопасной и доверительной среды для развития цифровой экономики и информационного общества.

Список литературы:

[1] Багиров Ч.М. Малозначительность деяния и его уголовно-правовое значение: диссертация кандидата юридических наук / Ч.М. Багиров. Тюмень, 2005. 168 с.

[2] Востриков, М. В. К вопросу о малозначительности деяния: какие признаки общественной опасности относят деяние к малозначительному / М. В. Востриков, О. В. Поликашина // Уголовное судопроизводство. – 2024. – № 4. – С. 26-31.

[3] Багиров, Ч. М. Использование категории «малозначительность деяния» правоприменителем / Ч. М. Багиров // Вопросы российского и международного права. – 2021. – Т. 11, № 9А. – С. 283-302.

[4] Мордвинов, К. В. Киберпреступность в России: актуальные вызовы и успешные практики борьбы с киберпреступностью / К. В. Мордвинов, У. А. Удавихина // Теоретическая и прикладная юриспруденция. – 2022. – № 1(11). – С. 83-88.

[5] Ивличев, П. С. Информационные технологии обеспечения безопасности платежных средств в свете современных тенденций в киберпреступности / П. С. Ивличев, Н. А. Ивличева // Экономика и предпринимательство. – 2017. – № 2-1(79). – С. 135-139.

[6] Гарбатович Д.А. Установление границ криминализации деяний посредством регламентации и правоприменения нормы о малозначительном деянии // Российская юстиция. 2020. N 2. С. 25 - 27.

[7] Предупреждение современной преступности (киберпреступность), 18 июля 2021 года. – Қазақстан Республикасы ІІМ Б. Бейсенов атындағы Қарағанды академиясы Карагандинская академия МВД Республики Казахстан им. Б. Бейсенова, 2021. – 182 с.

[8] Романенко, А. С. Некоторые аспекты борьбы с киберпреступностью / А. С. Романенко // Актуальные проблемы права, экономики и управления (см. в книгах). – 2015. – № 11. – С. 187-188.

[9] Гаджиева, А. А. Современная киберпреступность и проблемы ее профилактики / А. А. Гаджиева // Проблемы экономики и юридической практики. – 2023. – Т. 19, № 2. – С. 116-120

[10] Клименко, А. К. Влияние преступных и непреступных (малозначительных) хищений безналичных и электронных денежных средств на процесс криминализации и разграничение последних / А. К. Клименко // Российский следователь. – 2023. – № 9. – С. 31-34.

Spisok literatury:

[1] Bagirov Ch.M. Maloznachitel`nost` deyaniya i ego ugolovno-pravovoe znache-nie: dissertaciya kandidata yuridicheskix nauk / Ch.M. Bagirov. Tyumen`, 2005. 168 s.

[2] Vostrikov, M. V. K voprosu o maloznachitel`nosti deyaniya: kakie priznaki obshhestvennoj opasnosti otnosyat deyanie k maloznachitel`nomu / M. V. Vostrikov, O. V. Polikashina // Ugolovnoe sudoproizvodstvo. – 2024. – № 4. – S. 26-31.

[3] Bagirov, Ch. M. Ispol`zovanie kategorii “maloznachitel`nost` deyaniya” pra-voprimenitelem / Ch. M. Bagirov // Voprosy` rossijskogo i mezhdunarodnogo prava. – 2021. – T. 11, № 9A. – S. 283-302.

[4] Mordvinov, K. V. Kiberprestupnost` v Rossii: aktual`ny`e vy`zovy` i uspeshny`e praktiki bor`by` s kiberprestupnost`yu / K. V. Mordvinov, U. A. Udavixina // Teoreticheskaya i prikladnaya yurisprudenciya. – 2022. – № 1(11). – S. 83-88.

[5] Ivlichev, P. S. Informacionny`e texnologii obespecheniya bezopasnosti platezhny`x sredstv v svete sovremenny`x tendencij v kiberprestupnosti / P. S. Ivlichev, N. A. Ivlicheva // E`konomika i predprinimatel`stvo. – 2017. – № 2-1(79). – S. 135-139.

[6] Garbatovich D.A. Ustanovlenie granicz kriminalizacii deyanij posred-stvom reglamentacii i pravoprimeneniya normy` o maloznachitel`nom deyanii // Rossij-skaya yusticiya. 2020. N 2. S. 25 - 27.

[7] Preduprezhdenie sovremennoj prestupnosti (kiberprestupnost`), 18 iyulya 2021 goda. – Қazaқstan Respublikasy` IIM B. Bejsenov aty`ndaғy` Қaraғandy` akademiyasy` Karagandinskaya akademiya MVD Respubliki Kazaxstan im. B. Bejsenova, 2021. – 182 s.

[8] Romanenko, A. S. Nekotory`e aspekty` bor`by` s kiberprestupnost`yu / A. S. Romanenko // Aktual`ny`e problemy` prava, e`konomiki i upravleniya (sm. v knigax). – 2015. – № 11. – S. 187-188.

[9] Gadzhieva, A. A. Sovremennaya kiberprestupnost` i problemy` ee profilak-tiki / A. A. Gadzhieva // Problemy` e`konomiki i yuridicheskoj praktiki. – 2023. – T. 19, № 2. – S. 116-120

[10] Klimenko, A. K. Vliyanie prestupny`x i neprestupny`x (maloznachitel`ny`x) xishhenij beznalichny`x i e`lektronny`x denezhny`x sredstv na process kriminalizacii i razgranichenie poslednix / A. K. Klimenko // Rossijskij sledovatel`. – 2023. – № 9. – S. 31-34.