

УДК 343.71:004(100)

ПРОБЛЕМЫ КВАЛИФИКАЦИИ IT-ХИЩЕНИЙ И МЕЖДУНАРОДНЫЙ ОПЫТ ИХ РАЗРЕШЕНИЯ

Минина Виктория Владимировна

старший преподаватель кафедры юриспруденции
Учреждения образования «Могилевский государственный университет
имени А.А. Кулешова»
(г. Могилев, Беларусь)
minina@m.msu.by

Аннотация. Белорусское уголовное законодательство прошло значительный путь эволюции, адаптируясь к реалиям цифровой экономики. Вместе с тем, правоприменительная практика продолжает сталкиваться с проблемами квалификации и расследования хищений в сфере информационных технологий. Фундаментальная сложность заключается в экстерриториальном, транснациональном характере киберпреступности.

Ключевые слова. Киберпреступность, модификация компьютерной информации, мошенничество, предмет хищения.

В отличие от традиционных имущественных посягательств, где преступник, орудие и предмет преступления локализованы в едином физическом пространстве, цифровая среда стирает государственные границы. Злоумышленник может находиться на территории одного государства, использовать серверы и программное обеспечение, маршрутизированные через страны Европы или Азии, а похищенные безличные средства выводить через каскад подставных счетов («дропов») в третьей юрисдикции. Проблема установления места совершения преступления, сбора цифровых доказательств и идентификации виновных лиц становится главным вызовом для правоохранительной системы.

Для пресечения деятельности подобных транснациональных сетей и организованных групп правоохранительными органами Республики Беларусь ведется масштабная работа по ликвидации их технической и финансовой инфраструктуры. По данным Следственного комитета Республики Беларусь, только за 2025 год была выявлена информационная база 110 скам-сообществ, осуществлявших преступления посредством фишинга и иных форм киберхищений, а также зафиксирована деятельность порядка 24 теневых дроп-сервисов, оказывавших услуги по легализации и выводу похищенных денежных средств. Благодаря принятым мерам удалось заблокировать аккаунты, чат-боты и каналы 65

скам-групп и 16 дроп-сервисов, что позволило существенно подорвать финансовую логистику организованной киберпреступности [2].

Особый научный и практический интерес представляет сравнительно-правовой анализ с законодательством Российской Федерации, которая является основным партнером Республики Беларусь в рамках Союзного государства и, к сожалению, наиболее частой страной локализации киберпреступных элементов, действующих в отношении белорусских граждан.

В отличие от Республики Беларусь, где высокотехнологичные хищения квалифицируются по единой специализированной норме (ст. 212 УК «Хищение имущества путем модификации компьютерной информации»), российский законодатель пошел по пути максимальной детализации и дробления мошеннических составов. Еще в 2012 году Уголовный кодекс Российской Федерации (далее — УК РФ) был дополнен сразу несколькими специальными нормами, среди которых особое место заняли статья 159.3 (Мошенничество с использованием электронных средств платежа) и статья 159.6 (Мошенничество в сфере компьютерной информации) [6].

Диспозиция статьи 159.6 УК РФ предусматривает ответственность за хищение чужого имущества или приобретение права на чужое имущество путем ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации [6]. На первый взгляд, данная норма является полным аналогом белорусской статьи 212 УК. Однако российская правоприменительная практика пошла по совершенно иному, весьма ограничительному пути.

Долгое время в правоохранительных органах России шли дискуссии: как квалифицировать действия лица, которое нашло чужую банковскую карту (в том числе бесконтактную) и расплатилось ею в магазине или сняло наличные в банкомате? В Республике Беларусь такие действия безоговорочно образуют состав хищения путем модификации (ст. 212 УК). В России же точка в этом споре была поставлена Постановлением Пленума Верховного Суда РФ от 30 ноября 2017 г. № 48 (в ред. 2022 г.).

Высшая судебная инстанция России разъяснила, что хищение денежных средств, совершенное с использованием виновным чужой или поддельной платежной карты путем выдачи наличных в банкомате, либо путем оплаты товаров в терминале, не образует состава мошен-

ничества, так как при этом не оказывается обманного воздействия на человека (работника банка или магазина), а банкомат и терминал не могут быть субъектами заблуждения [3]. Также эти действия не признаются мошенничеством в сфере компьютерной информации (ст. 159.6 УК РФ), так как виновный не осуществляет целенаправленного взлома программного обеспечения, а лишь использует готовый механизм оплаты.

Для решения этой коллизии в 2018 году в УК РФ был введен принципиально новый квалифицирующий признак в классическую статью 158 УК РФ «Кража» – пункт «г» части 3: «кража, совершенная с банковского счета, а равно в отношении электронных денежных средств».

Сравнивая этот подход с белорусским, Д. В. Гриб в своем исследовании отмечает, что российская модель переводит акцент со способа преступления (компьютерной модификации) на локализацию предмета (банковский счет). Иными словами, любое тайное неправомерное списание денег со счета в России сегодня признается классической кражей (п. «г» ч. 3 ст. 158 УК РФ), а не IT-преступлением [1, с. 78]. При этом российский законодатель отнес кражу с банковского счета к категории тяжких преступлений вне зависимости от суммы похищенного, что делает уголовную репрессию в РФ значительно более жесткой на начальном этапе по сравнению с белорусской статьей 212 УК (которая в ч. 1 является преступлением, не представляющим большой общественной опасности).

Следует обратить пристальное внимание на опыт государств Центральной Азии, которые в последние годы провели масштабную модернизацию уголовного закона в ответ на цифровизацию экономики. Концептуально иной подход к правовой регламентации IT-хищений демонстрирует Республика Казахстан.

Уголовный кодекс Республики Казахстан (далее — УК РК), принятый в 2014 году пошел по пути имплементации цифровых способов совершения преступления в качестве квалифицирующих признаков в классические составы посягательств на собственность.

Так, в статье 188 УК РК «Кража» предусмотрен специальный квалифицирующий признак (пункт 4 части 2): кража, совершенная «путем незаконного доступа в информационную систему либо изменения информации, передаваемой по сетям телекоммуникаций» [4]. Аналогичным образом сконструирована статья 190 УК РК «Мошенничество», часть 2 которой отягчает ответственность за мошенничество, совершенное «путем обмана или злоупотребления доверием пользователя информационной системы или сети Интернет» [4]. Главное преимуще-

щество казахстанской модели заключается в отсутствии искусственного дробления составов: правоприменителю не нужно разграничивать «компьютерное» и «обычное» хищение как разные виды преступлений, достаточно лишь установить использование IT-инфраструктуры какотягчающего обстоятельства единого деликта.

Схожая, но еще более жесткая уголовно-правовая политика реализуется в Республике Узбекистан. В действующей редакции статьи 169 УК РУз «Кража» закреплён пункт «б» части 3: кража, совершенная «с незаконным (несанкционированным) проникновением в информационную систему или ее использованием». Аналогичный признак («с использованием информационной системы, в том числе информационных технологий») введен в часть 2 статьи 168 УК РУз «Мошенничество» [5]. Особенность узбекского опыта заключается в категоризации данных деяний: совершение хищения с использованием информационных технологий автоматически переводит преступление в разряд тяжких, за которое предусмотрено безальтернативное наказание в виде лишения свободы на срок от пяти до восьми лет. Столь суровые санкции обусловлены стремлением государства обеспечить максимальную превенцию посягательств на электронную финансовую систему страны.

Таким образом, сравнивая белорусскую (выделение самостоятельного IT-состава – ст. 212 УК), российскую (дробление на компьютерное мошенничество и банковскую кражу) и центральноазиатскую (внедрение IT-квалификаторов в традиционные статьи) модели, можно констатировать, что идеальной юридической конструкции пока не выработано. Белорусский подход представляется наиболее сбалансированным с точки зрения теории уголовного права, поскольку он подчеркивает двухобъектную природу деяния (посягательство и на собственность, и на информационную безопасность посредством модификации данных). Однако общим вектором для всех стран СНГ является признание киберхищений деяниями повышенной общественной опасности, требующими ужесточения уголовной репрессии.

Список литературы

1. Гриб, Д. В. Хищение имущества путем использования информационных технологий в Уголовном кодексе Российской Федерации и Республики Беларусь: сравнительный аспект / Д. В. Гриб // Вестник Московского университета МВД России. – 2019. – № 4. – С. 75–80. – URL: <https://cyberleninka.ru/article/n/hischenie-imuschestva-putem-ispolzovaniya-informatsionnyh-tehnologii-v-ugolovnom-kodekse-rossii-skoi-federatsii-i-respubliki-belarus> (дата обращения: 04.05.2026).

2. Киберпреступность-2025: что происходит на самом деле // Следственный комитет Республики Беларусь. – URL: <https://sk.gov.by/ru/news-ru/view/kiberprestupnost-2025-chto-proisходит-na-samom-dele-15685/> (дата обращения: 29.04.2026).
3. О судебной практике по делам о мошенничестве, присвоении и растрате : постановление Пленума Верхов. Суда Рос. Федерации от 30 нояб. 2017 г. № 48 : в ред. от 15 дек. 2022 г. № 38 // КонсультантПлюс. Россия : справ. правовая система (дата обращения: 29.04.2026).
4. Уголовный кодекс Республики Казахстан : 3 июля 2014 г. № 226-V ЗРК : принят Парламентом Респ. Казахстан 3 июля 2014 г. : в ред. Закона Респ. Казахстан от 8 марта 2026 г. // Информационно-правовая система нормативных правовых актов Республики Казахстан «Әділет». – URL: <https://adilet.zan.kz/rus/docs/K1400000226> (дата обращения: 04.05.2026).
5. Уголовный кодекс Республики Узбекистан : 22 сент. 1994 г. № 2012-XII : утвержден Законом Респ. Узбекистан от 22 сент. 1994 г. : в ред. Закона Респ. Узбекистан от 11 марта 2026 г. № ЗРУ-1121 // Национальная база данных законодательства Республики Узбекистан (LexUZ). – URL: <https://lex.uz/docs/111457> (дата обращения: 04.05.2026).
6. Уголовный кодекс Российской Федерации : 13 июня 1996 г. № 63-ФЗ : принят Гос. Думой 24 мая 1996 г. : одобр. Советом Федерации 5 июня 1996 г. : в ред. от 20 фев. 2026 г. // КонсультантПлюс. Россия : справ. правовая система (дата обращения: 29.04.2026).