УДК 343.2

УГОЛОВНАЯ ОТВЕТСТВЕННОСТЬ ЗА ХИЩЕНИЕ, СОВЕРШЕННОЕ С ИСПОЛЬЗОВАНИЕМ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ, ПО ЗАКОНОДАТЕЛЬСТВУ РЕСПУБЛИКИ БЕЛАРУСЬ И ЗАРУБЕЖНЫХ ГОСУДАРСТВ

А. Н. Примаков
кандидат юридических наук, доцент,
доцент кафедры уголовного права, уголовного процесса и криминалистики
Могилевского института МВД (Беларусь)

Д. В. Романюк
курсант факультета милиции
Могилевского института МВД (Беларусь)

На основе результатов сравнительно-правового анализа норм уголовного законодательства Республики Беларусь и зарубежных государств, предусматривающих ответственность за хищения, совершенные с использованием информационно-телекоммуникационных технологий и компьютерной информации, в статье определены законодательные подходы к установлению основных уголовно-правовых признаков данных видов преступлений, обозначены проблемные и дискуссионные вопросы, связанные с их регламентацией, и сформулированы некоторые предложения по их разрешению.

Для наиболее эффективного противодействия обозначенной форме хищения отмечена необходимость в изменении судебно-следственного подхода к квалификации противоправных действий, ответственность за которые наступает по ст. 209 и 212 Уголовного кодекса Республики Беларусь. Определено, что при решении данного вопроса необходимо учитывать первоначальную позицию законодателя относительно специально выделенной в уголовном законе формы хищения, которая связана со сферой использования компьютерной техники (ст. 212 Уголовного кодекса Республики Беларусь), и трактовать ее в более широком правоприменительном значении.

Ключевые слова: *киберпреступления, хищение, мошенничество, информационно-телекоммуникационные технологии, компьютерная информация, уголовная ответственность, квалификация, регламентация.*

Введение. Естественные экономические, политические, социальные процессы и постоянно происходящие на их основе системные изменения, связанные с деятельностью государственных органов и институтов, учреждений и организаций, с существованием как в целом общества, так и каждого гражданина в отдельности, непременно создают предпосылки для совершения новых, все более изощренных и скрытых видов преступных действий. В XXI в. одной из уязвимых в этом направлении преступной деятельности стала сфера компьютеризации и информационно-телекоммуникационных технологий.

Хищения, совершаемые в указанной сфере как в Республике Беларусь, так и в ряде других зарубежных государств, прежде всего характеризуются высоким уровнем латентности, а процент их раскрываемости, согласно статистическим данным Министерства внутренних дел Республики Беларусь, составляет всего около 10 % [1; 2, с. 5; 3].

Очевидно и то обстоятельство, что для эффективного противодействия преступлениям рассматриваемой категории следует своевременно, с учетом аргументированной позиции научного сообщества и практических работников, законодательно регламентировать и внедрять уголовно-запрещающие правовые нормы. Однако из результатов проведенного ретроспективного анализа уголовного законодательства следует, что содержание статей Уголовного кодекса (далее — УК) Российской Советской Федеративной Социалистической Республики [4] за совершение некоторых видов

преступлений, например кражи и мошенничества, в том числе без учета обозначенной сферы применения, технически перешло в УК Республики Беларусь [5] и сохранилось до настоящего времени.

Проблемам уголовно-правовой характеристики хищений, связанных с использованием информационно-телекоммуникационных технологий и компьютерной информации, и вопросам их квалификации были посвящены работы Л. В. Боровых и Е. А. Корепановой [6], В. В. Крылова [7], И. А. Бобракова [8], С. П. Кушниренко [9] и др. Однако, по нашему мнению, законодательное закрепление конкретных средств дифференциации ответственности по данной категории преступлений в действующем УК Республики Беларусь [5] нельзя признать оптимальным без учета изучения норм уголовного законодательства Союзного государства и ряда зарубежных стран.

Целью настоящего исследования является изучение вопросов регламентации уголовной ответственности за хищения, совершенные с использованием информационно-телекоммуникационных технологий и компьютерной информации, в Республике Беларусь и других зарубежных странах, опыта расследования и определения законодательных подходов в части их квалификации. Представляется, что полученные результаты позволят определить эффективный механизм уголовно-правовой защиты охраняемых общественных отношений в сфере права собственности, а также выдвинуть некоторые предложения по совершенствованию норм действующего уголовного законодательства.

Основная часть. Уголовная ответственность за хищение, совершенное с использованием информационно-телекоммуникационных технологий и компьютерной информации, в нашей стране в зависимости от обстоятельств и способа его совершения предусмотрена ст. 212 «Хищение путем модификации компьютерной информации» или ст. 209 «Мошенничество» УК Республики Беларусь [5]. Под хищением путем модификации компьютерной информации в соответствии с его правоприменительным толкованием понимается «хищение имущества путем изменения информации, обрабатываемой в компьютерной системе, хранящейся на машинных носителях или передаваемой по сетям передачи данных, либо путем введения в компьютерную систему ложной информации» [10, с. 458]. Мошенничество как преступное деяние представляет собой завладение имуществом либо приобретение права на имущество путем обмана или злоупотребления доверием [5].

Практика расследования и квалификации данных видов преступлений показывает, что уголовная ответственность по ч. 1 ст. 212 УК Республики Беларусь [5] наступает, когда виновный, проводя компьютерные манипуляции, связанные с несанкционированным доступом к средствам информации и управляющими командами, осуществил перевод безналичных денежных средств с одного банковского счета на другой или на иной электронный кошелек и таким образом совершил хищение. При этом для определения наличия состава преступления обязательно требуется установить факт ввода, вывода данных в компьютерную систему, в процессе чего используемая компьютерная программа идентифицирует преступника как законного владельца денежных средств.

Уголовная ответственность по ч. 1 ст. 209 УК Республики Беларусь наступает, когда потерпевший под воздействием обмана или злоупотребления доверием самостоятельно осуществил банковский перевод и таким образом виновный завладел принадлежащими ему безналичными денежными средствами [5].

Вводя в действие ст. 212 УК Республики Беларусь [5], законодатель таким образом ужесточил наказание и выделил специальную форму хищения, рассчитанную на ситуации и, следовательно, сферу применения, когда имущество похищается исключительно с помощью компьютерной техники и информационно-телекоммуникационных технологий. При этом не вполне четкими и дискуссионными в данном случае представляются разграничение и квалификация уголовно-правовых признаков указанных составов преступлений, поскольку при их определении

усматривается один и тот же объект (общественные отношения, связанные с правом собственности) и предмет (как правило, безналичные денежные средства) посягательства, используется схожий способ его подготовки и совершения, сопряженный с обманом и воздействием на потерпевшего с целью получения доступа и завладения предметом хищения. Помимо этого, обман с целью завладения чужим имуществом как признак данной формы хищения может присутствовать и в том, и в другом случае (п. 1 примечания к гл. 24 «Преступления против собственности» УК Республики Беларусь) [5].

Другими словами, основное отличие здесь заключается в том, что при мошенничестве виновный завладевает предметом преступления «опосредованно» — через потерпевшего, не воздействуя на элементы управления банковским счетом (виновный не имеет доступа к управлению банковским счетом, перевод денежных средств осуществляется потерпевшим самостоятельно), а при хищении путем модификации компьютерной информации — «непосредственно» — через потерпевшего, воздействуя на элементы управления банковским счетом (виновный завладевает доступом к управлению банковским счетом и похищает денежные средства).

Думается, что при решении данного вопроса прежде всего необходимо учитывать и трактовать первоначальную позицию законодателя о специально выделенной в уголовном законе форме хищения, которая связана со сферой использования компьютерной техники и информационно-телекоммуникационных технологий, в более широком смысле. Таким образом, если при совершении имущественного преступления виновный использует обман и злоупотребление доверием, которые выступают способом его реализации и облегчают его исполнение, но при этом в качестве средства совершения преступления используется компьютерная информация, воздействие на предмет преступления осуществляется через компьютерную систему (компьютерные процессы) в любой форме, то такого рода деяния независимо от действий и поведения потерпевшего лица, по нашему мнению, должны квалифицироваться по ст. 212 УК Республики Беларусь [5].

Квалифицированные и особо квалифицированные составы мошенничества и хищения, совершенного путем модификации компьютерной информации, по квалифицирующим признакам практически идентичны. По ч. 2 ст. 209 и ч. 2 ст. 212 УК Республики Беларусь такие деяния квалифицируются за совершение их повторно или группой лиц; по чч. 3 указанных статей — если в результате их осуществления наступили общественно опасные последствия в виде крупного размера; по чч. 4 — если преступление было совершено организованной группой либо в виде особо крупного размера [5].

В Российской Федерации уголовная ответственность за хищение, совершенное с использованием компьютерной информации, предусмотрена несколькими нормами уголовного закона. Рассматриваемое общественно опасное деяние может подпадать под действие п. «г» ч. 3 ст. 158 «Кража» (кража, совершенная с банковского счета, а равно в отношении электронных денежных средств), ст. 159 «Мошенничество», ст. 159.3 «Мошенничество с использованием электронных средств платежа» и ст. 159.6 «Мошенничество в сфере компьютерной информации» УК Российской Федерации [11]. Отсюда можно сделать вывод о том, что российский законодатель, помимо состава кражи, которая может быть совершена с электронного банковского счета, и мошенничества (основного состава), принял решение о создании дополнительно нескольких смежных составов данного преступного деяния в зависимости от способа его совершения и сферы общественных отношений, которой причинен ущерб. При этом определения понятия «мошенничество» по своему смысловому содержанию в УК Российской Федерации и УК Республики Беларусь практически идентичны [11; 5].

Представляется, что отличие данных норм уголовного-правового запрета заключается в том, что при краже, совершенной с банковского счета, а равно в отношении

электронных денежных средств, способы ее совершения не связаны с обманом или злоупотреблением доверием, то есть не обладают обязательными признаками мошеннического завладения объектом посягательства, в остальных случаях эти признаки являются обязательными. Однако, как справедливо отмечает А. В. Макаров, на практике достаточно сложно их разграничить, поскольку ситуативно способ завладения электронными денежными средствами, в том числе в силу их специфической характеристики как предмета преступления, практически невозможно квалифицировать без признаков обмана или злоупотребления доверием [12, с. 26].

Об этом пишет и А. З. Абитов, утверждая, что хищения, связанные с электронным списанием денежных средств посредством фишинговых и иных ссылок, банковских автоматов, сопряженные с получением реквизитов банковских платежных карт и электронных кошельков, в следственной практике достаточно часто квалифицируются по разным статьям уголовного закона — чч. 1, 2 ст. 159, п. «г» ч. 3 ст. 158, ст. 159.3 УК Российской Федерации [13, с. 42]. О значительном количестве подобных квалифицирующих ошибок в следственной практике говорят и другие российские авторы [14, с. 108–110].

Помимо этого, результаты анализа размеров наказаний за совершение преступлений, предусмотренных ст. 158, 159, 159.3 и 159.6 УК Российской Федерации, позволяют сделать вывод о том, что их максимальные пределы являются одинаковыми (до 10 лет лишения свободы) [11]. Возникает вопрос: в чем смысл разграничения этих составов преступлений, если наказание независимо от их квалификации является одинаковым?

В этой части с положительной стороны следует отметить введенную специализированную норму — ст. 212 УК Республики Беларусь, которая предусматривает более строгое наказание (лишение свободы на срок от 5 до 12 лет), чем за наиболее схожее по содержанию признаков преступление — ст. 209 УК Республики Беларусь (лишение свободы на срок от 3 до 10 лет) [5].

Проведенный анализ положений уголовного законодательства государств — участников Содружества Независимых Государств показывает, что в Республике Таджикистан (ст. 247 УК) [15], Азербайджанской Республике (ст. 178 УК) [16], Грузии (ст. 180 УК) [17], Республике Молдова (ст. 190 УК) [18], Кыргызской Республике (ст. 209 УК) [19], Республике Армения (ст. 178 УК) [20] отсутствует самостоятельная норма либо признак какого-либо состава преступления, связанного с хищением имущества посредством использования информационно-телекоммуникационных технологий и компьютерной информации. То есть такого рода деяния квалифицируются на общих основаниях, как правило, по статье «Мошенничество», содержание которой по своему смысловому значению практически не отличается от аналогичной статьи, предусмотренной УК Республики Беларусь [5]. Представляется, что конструкции этих норм уголовного закона буквально в неизменном виде перешли из УК Российской Советской Федеративной Социалистической Республики и, на наш взгляд, требуют соответствующих изменений в обозначенной части [4].

В Республике Казахстан (п. 4 ч. 2 ст. 190 УК — «мошенничество путем обмана или злоупотребления доверием пользователя информационной системы») [21], Республике Узбекистан (п. «г» ч. 3 ст. 168 УК — мошенничество «с использованием информационной системы, в том числе информационных технологий») [22], Литовской Республике (ч. 2 ст. 274 УК — «мошенничество, совершенное лицом, имеющим судимость за преступления против собственности, или по предварительному сговору группой лиц посредством составления заведомо неправильной компьютерной программы, введения в компьютерную память неверных данных, а также путем иного воздействия на компьютерную информацию или ее обработку») [23], Туркменистане (п. «с» ч. 2 ст. 249 УК — «мошенничество, совершенное с применением информационных технологий») [24] введены дополнительные квалифицирующие признаки в статью «Мошенничество». Таким образом, формат введения

такого признака и определения более строгой меры ответственности показывает достаточно адекватный и эффективный подход законодателей указанных стран к сфере противодействия хищению имущества, совершенному с использованием информационно-телекоммуникационных технологий и компьютерной информации.

Рассматривая нормы уголовного законодательства Китайской Народной Республики (далее — КНР), следует отметить, что практически до конца XX в. в стране не было специальных положений об уголовной ответственности за преступления, связанные с компьютерной информацией, а также средствами ее автоматизированной обработки или передачи. Такие вопросы судебными органами разрешались на основе применения традиционных составов преступлений, прибегая, как правило, к крайне расширительному толкованию положений уголовного закона [25, с. 109].

Действующий уголовный закон КНР предусматривает достаточно много различных составов хищения имущества в форме мошеннических действий. Например, мошеннические действия с финансовыми векселями (ст. 194 УК КНР), получение в банке или иной финансовой организации мошенническим путем кредита на сравнительно крупную сумму в целях незаконного владения капиталом (ст. 193 УК КНР), накопление капитала мошенническими противозаконными способами в целях незаконного владения данным капиталом в сравнительно крупном размере (ст. 192 УК КНР) и др. [26]. Помимо этого, в ст. 265 УК КНР указано, что «преступлением является незаконное завладение каналами других людей, дублирование чужого номера электронной почты или пользование заведомо похищенными, дублированными электронными оборудованием и устройствами с целью извлечения прибыли» [27]. Статья 287 УК КНР представляет собой ссылочную уголовно-правовую норму, легитимирующую применение традиционных положений китайского уголовного законодательства к случаям совершения иных общеуголовных преступлений с использованием современных информационно-телекоммуникационных технологий [28].

Таким образом, как справедливо отмечает Е. А. Русскевич, в построении уголовно-правового механизма противодействия преступлениям, совершаемым с использованием информационно-телекоммуникационных технологий, китайский законодатель, в отличие от белорусского и российского, реализовал более сложную модель уголовно-правового противодействия киберпреступности. Развитие данной модели происходило в рамках трех основных направлений: защита критической инфраструктуры; расширение защиты информационных ресурсов частных лиц; установление ответственности провайдеров и виртуальных пособников [25, с. 112]. Однако такой сложный механизм не вполне применим и достаточно сложно реализуем в отечественной модели уголовно-правовой защиты общественных отношений, поскольку, как показывает опыт следственной практики Российской Федерации, создание множества смежных составов однородных видов преступлений порождает ряд практических, и в этом отношении даже достаточно грубых, квалификационных ошибок и противоречий.

Одной из первых стран мира, принявших меры по введению уголовной ответственности за совершение преступлений, связанных с использованием информационно-телекоммуникационных технологий, стали Соединенные Штаты Америки (далее — США), где прежде всего в силу передового развития компьютерных коммуникаций преступления рассматриваемого вида начали совершаться несколько раньше, чем в других странах. Уже в 1977 г. в США был разработан законопроект о защите федеральных компьютерных систем, который предусматривал уголовную ответственность за хищение денежных средств, ценных бумаг, имущества, услуг, ценной информации, совершенное с применением возможностей компьютерных технологий или компьютерной информации. Далее в 1984 г. на основе указанного законопроекта был принят закон о компьютерном мошенничестве и злоупотреблении с использованием компьютеров — основной нормативный правовой акт,

устанавливающий уголовную ответственность за преступления в сфере компьютерной информации [29, с. 60].

В настоящее время уголовная ответственность за совершение хищения с использованием информационно-телекоммуникационных технологий и компьютерной информации в уголовном законодательстве США предусмотрена § 1029 и § 1030 гл. 47 титула 18 Свода законов США [29; 30]. Наказание установлено в случаях осуществления несанкционированного доступа (когда постороннее лицо вторгается в компьютер или компьютерную систему и пользуется их данными) либо превышения санкционированного доступа (когда законный пользователь компьютера или компьютерной системы осуществляет доступ к хранящимся в них сведениям, на которые его полномочия не распространяются). Данным законом предусмотрены следующие виды преступлений:

- мошенничество, совершенное с использованием компьютера, под которым понимается получение доступа к компьютеру и его применение с целью получения какого-либо ценного имущества, включая время незаконного использования и эксплуатации компьютерной системы, ее сетей и серверов в течение года на сумму более пяти тысяч долларов США;
- мошенничество, сопряженное с торговлей компьютерными учетными записями (паролями) или подобной аутентификационной информацией, позволяющей получить несанкционированный доступ к компьютерной системе, повлекшее причинение ущерба торговым отношениям;
- использование технических приборов с целью получения несанкционированного доступа и материальной выгоды в размере более одной тысячи долларов США и др. [29, с. 61].

Таким образом, как справедливо отмечает А. В. Чернякова, законодательством США компьютерное мошенничество отграничено от традиционного, а его основное значение сводится к получению доступа к компьютеру и его использованию [30, с. 174].

Проведенный анализ норм уголовного законодательства Французской Республики [31] и Соединенного Королевства Великобритании и Северной Ирландии [30, с. 173–174] позволяет сделать вывод о том, что специальных статей, предусматривающих ответственность за хищение с использованием информационно-телекоммуникационных технологий и компьютерной информации, как в одной, так и в другой стране, не имеется. Уголовно-правовая защита во Французской Республике прежде всего направлена на охрану систем автоматизированной обработки данных (гл. «О посягательствах на системы автоматизированной обработки данных» книги 3 «Об имущественных преступлениях и проступках») и личных данных пользователей, размещенных в телекоммуникационных сетях (гл. «О посягательствах на личность» книги 2 «О преступлениях и проступках против личности») [30; 31]. В Англии уголовная ответственность за совершение в целом компьютерных преступлений предусмотрена различными законами (например, Закон о неправомерном использовании компьютера, Закон о телекоммуникациях (обман), Закон об электронном сообщении, Закон о борьбе с обманом в области социального обеспечения и др. [30]). То есть фактически действуют отсылочные нормы, в которых в одних случаях компьютерные данные выступают объектом преступления, в других — предметом, средством или способом его совершения [30, с. 173–174].

В УК Федеративной Республики Германия [32] мошенничество, связанное с информационно-телекоммуникационными технологиями и компьютерной информацией, закреплено как самостоятельное преступление. Так, ст. 263А предусмотрена ответственность за компьютерное мошенничество — действия с целью получения для себя или третьего лица противоправной имущественной выгоды, которыми наносится вред имуществу другого лица посредством воздействия на результат обработки данных электронных вычислительных машин путем составления

неправильных программ, использования неправильных или неполных данных, несанкционированного применения данных или иного неправомочного воздействия на процесс их обработки. Немецкий законодатель, как представляется, определил здесь более строгую меру ответственности, руководствуясь лишь позицией, исключительно связанной со способом совершения преступления.

Заключение. Таким образом, проведенный анализ действующего уголовного законодательства Республики Беларусь, Российской Федерации, государств — участников Содружества Независимых Государств, европейских и других государств, связанный с регламентацией уголовной ответственности за хищения, совершенные с использованием информационно-телекоммуникационных технологий и компьютерной информации, позволил сделать следующие выводы.

На современном этапе развития организации противодействия хищениям в сфере киберпространства прослеживаются следующие законодательные подходы к их уголовно-правовой регламентации:

- законодатель не вводил в уголовный закон специальную норму или дополнительный квалифицирующий признак, связанный с обозначенным видом хищения, наказание за его совершение наступает на общих основаниях (Республика Таджикистан, Азербайджанская Республика, Грузия, Республика Молдова, Французская Республика, Соединенное Королевство Великобритании и Северной Ирландии и др.);
- законодателем внесены изменения в уголовный закон и введен дополнительный квалифицирующий признак в общем составе рассматриваемого уголовно наказуемого деяния, предусматривающий более строгую меру наказания (Республика Казахстан, Республика Узбекистан, Литовская Республика, Туркменистан);
- законодателем внесены изменения в уголовный закон и введен отдельный специальный состав хищения, совершенного с использованием информационно-телекоммуникационных технологий и компьютерной информации, с более строгой мерой наказания (Республика Беларусь, Федеративная Республика Германия);
- законодателем внесены изменения в уголовный закон и введены множество отдельных составов хищений, связанных с использованием компьютерной информации и электронных данных в зависимости от сферы и обстоятельств их совершения (Российская Федерация, Соединенные Штаты Америки, Китайская Народная Республика).

Наиболее прогрессивным, практико-ориентированным и эффективным законодательным подходом, как представляется, является введение в уголовный закон отдельной специальный нормы, регламентирующей ответственность за хищения в сфере киберпространства, с установлением более строгой меры наказания по отношению к общему составу рассматриваемой категории преступлений.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Гольченко, Р. Ю. Актуальные вопросы раскрытия и расследования преступлений в цифровом пространстве / Р. Ю. Гольченко, Д. Ф. Минзянова, С. Л. Миролюбов // Научный компонент. – 2024. – № 3 (23). – URL: https://cyberleninka.ruи /article/n/aktualnye-voprosy-raskrytiya-i-rassledovaniya-prestupleniy-v-tsifrovom-prostranstve (дата обращения: 01.05.2025).

2. Казакевич, Г. А. О мерах, принимаемых МВД Республики Беларусь, по противодействию киберпреступности на современном этапе / Г. А. Казакевич // Вестник Академии МВД Республики Беларусь. – 2021. – № 1. – С. 5–8.

3. Киберпреступность и киберконфликты : Казахстан // TADVISER. – URL: https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%9A%D0%B8%D0%B1%D0%B5%D1%80%D0%BF%D1%80%D0%B5%D1%81%D1%82%D1%83%D0%BF%D0%BD%D0%BE%D1%81%D1%82%D1%8C_%D0%B8_%D0%BA%D0%B8%D0%B1%D0%B5%D1%80%D0%BA%D0%BE%D0%BD%D1%84%D0%BB%D0%B8%D0%BA%D1%82%D1%8B_:_%D0%9A%D0%B0%D0%B7%D0%B0%D1%85%D1%81%D1%82%D0%B0%D0%BD (дата обращения: 13.05.2025).

4. Уголовный кодекс Российской Советской Федеративной Социалистической Республики 1960 г. // НИУ ВШЭ. – URL: https://nnov.hse.ru/ba/law/igpr/sov_gos/14_ugol_kodeks (дата обращения: 01.05.2025).

5. Уголовный кодекс Республики Беларусь : 9 июля 1999 г. № 275-З : принят Палатой представителей 2 июня 1999 г. : одобр. Советом Респ. 24 июня 1999 г. : в ред. Закона Респ. Беларусь от 17 февр. 2025 г. № 61-З // ЭТАЛОН : информ.-поисковая система (дата обращения: 01.05.2025).

6. Боровых, Л. В. Направленность обмана в составе мошенничества с использованием платежных карт / Л. В. Боровых, Е. А. Корепанова // Вестник Пермского университета. Юридические науки. – 2016. – № 1 (31). – С. 98–104.

7. Крылов, В. В. Информационные компьютерные преступления : учеб. и практ. пособие / В. В. Крылов. – М. : Инфра-М — НОРМА, 1997. – 250 с.

8. Бобраков, И. А. Уголовное право : учебник / И. А. Бобраков. – Саратов : Вузовское образование, 2018. – 736 с.

9. Кушниренко, С. П. Цифровая информация как самостоятельный объект криминалистического исследования / С. П. Кушниренко // Вестник криминалистики. – 2006. – № 2 (18). – С. 43–47.

10. Уголовный кодекс Республики Беларусь: научно-практический комментарий / Т. П. Афонченко, Н. А. Бабий, Н. А. Швед [и др.] ; под ред. В. М. Хомича, А. В. Баркова, В. В. Марчука. – Минск : Нац. центр правовой информ. Респ. Беларусь, 2019. – 1000 с.

11. Уголовный кодекс Российской Федерации : 13 июня 1996 г. № 63-ФЗ : принят Гос. Думой Рос. Федерации 24 мая 1996 г. : одобр. Советом Федерации 5 июня 1996 г. : в ред. Федер. закона Рос. Федерации от 21 апр. 2025 г. № 102-ФЗ // КонсультантПлюс. Россия : справ. правовая система (дата обращения: 01.05.2025).

12. Макаров, А. В. Особенности и проблемы квалификации мошенничества, совершенного с использованием электронных средств платежа / А. В. Макаров // Российский судья. – 2019. – № 5. – С. 24–29.

13. Абитов, А. З. Проблема квалификации преступлений, связанных с хищением электронных денежных средств / А. З. Абитов // Законность. – 2019. – № 9. – С. 42–44.

14. Киктенко, А. А. Уголовная ответственность за кражу, совершенную с банковского счета, а равно в отношении электронных банковских средств : дис. … канд. юрид. наук : 5.1.4 / Киктенко Анна Александровна ; Москов. ун-т М-ва внутр. дел Рос. Федерации им. В. Я. Кикотя. – М., 2023. – 163 с.

15. Уголовный кодекс Республики Таджикистан : 21 мая 1998 г. № 574 : в ред. Закона Респ. Таджикистан от 15 апр. 2025 г. № 2163 // Информ. система «Континент». – URL: https://continent-online.com/Document/?doc_id=30397325#pos=2948;-56 (дата обращения: 01.05.2025).

16. Уголовный кодекс Азербайджанской Республики : 30 дек. 1999 г. № 787-IQ : в ред. Закона Азербайджанской Респ. от 11 апр. 2025 г. № 172-VIIQD // Информ. система «Континент». – URL: https://continent-online.com/Document/?doc_id=30420353#pos=2125;44&sdoc_params=text%3D%25D0%25BC%25D0%25BE%25D1%2588%25D0%25B5%25D0%25BD%25D0%25BD%25D0%25B8%25D1%2587%25D0%25B5%25D1%2581%25D1%2582%25D0%25B2%25D0%25BE%26mode%3Dindoc%26topic_id%3D30420353%26spos%3D1%26tSynonym%3D0%26tShort%3D1%26tSuffix%3D1&sdoc_pos=2 (дата обращения: 01.05.2025).

17. Уголовный кодекс Грузии // UNHCR. – URL: https://www.refworld.org/ru/legal/legislation/natlegbod/1999/ru/103652 (дата обращения: 01.05.2025).

18. Уголовный кодекс Республики Молдова : 18 апр. 2002 г. № 985-XV : в ред. Закона Респ. Молдова от 13 марта 2025 г. № 35 // Информ. система «Континент». – URL: https://continent-online.com/Document/?doc_id=30394923#pos=2518;-10&sdoc_params=text%3D%25D0%25BC%25D0%25BE%25D1%2588%25D0%25B5%25D0%25BD%25D0%25BD%25D0%25B8%25D1%2587%25D0%25B5%25D1%2581%25D1%2582%25D0%25B2%25D0%25BE%-26mode%3Dindoc%26topic_id%3D30394923%26spos%3D1%26tSynonym%3D0%26tShort%3D1%26tSuffix%3D1&sdoc_pos=0 (дата обращения: 01.05.2025).

19. Уголовный кодекс Кыргызской Республики : 28 окт. 2021 № 127 : в ред. Закона Кыргызской Респ. от 14 марта 2025 г. № 56 // ИС Параграф «Юрист». – URL: https://online.zakon.kz/Document/?doc_id=36675065&pos=2186;-46#pos=2186;-46&sdoc_params=text%3D%25D0%25BC%25D0%25BE%25D1%2588%25D0%25B5%25D0%25BD%25D0%25BD%25D0%25B8%25D1%2587%25D0%25B5%25D1%2581%25D1%2582%25D0%25B2%25D0%25BE%-26mode%3Dindoc%26topic_id%3D36675065%26spos%3D1%26tSynonym%3D1%26tShort%3D1%26tSuffix%3D1&sdoc_pos=0 (дата обращения: 01.05.2025).

20. Уголовный кодекс Республики Армения : 5 мая 2021 г. : с изм. от 23 дек. 2022 г. // HRlib. – URL: https://hrlib.kz/document/237051 (дата обращения: 01.05.2025).

21. Уголовный кодекс Республики Казахстан : 3 июля 2014 года № 226-V : в ред. Закона Респ. Казахстан от 18 марта 2025 г. № 175-VIII // ИС Параграф «Юрист». – URL: https://online.zakon.kz/Document/?doc_id=31575252 (дата обращения: 01.05.2025).

22. Уголовный кодекс Республики Узбекистан : 22 сент. 1994 г. № 2012-XII : в ред. Закона Респ. Узбекистан от 27 марта 2025 г. № ЗРУ-1051 // ИС Параграф «Юрист». – URL: https://online.zakon.kz/Document/?doc_id=30421110 (дата обращения: 01.05.2025).

23. О внесении изменений и дополнений в Уголовный, Исправительно-трудовой и Уголовно-процессуальный кодексы Литовской Республики : Закон Литовской Респ. от 19 июля 1994 г. № I-551 // Lietuvos Respublikos Seimo kanceliarija. – URL: https://e-seimas.lrs.lt/rs/legalact/TAD/TAIS.62409/ (дата обращения: 01.05.2025).

24. Уголовный кодекс Туркменистана : 12 июня 1997 г. № 222-I : в ред. Закона Туркменистана от 12 апр. 2025 г. // ИС Параграф «Юрист». – URL: https://online.zakon.kz/Document/?doc_id=31295286 (дата обращения: 01.05.2025).

25. Русскевич, Е. А. Уголовная ответственность за преступления в сфере компьютерной информации по законодательству Китайской Народной Республики: сравнительно-правовой анализ / Е. А. Русскевич // Журнал зарубежного законодательства и сравнительного правоведения. – 2018. – № 5 (72). – С. 108–113.

26. Уголовный кодекс КНР. Особенная часть (статьи 102–231) // Chinahelp.me. – URL: https://chinahelp.me/criminal/1599-2 (дата обращения: 01.05.2025).

27. Уголовный кодекс КНР. Особенная часть (статьи 232–276) // Chinahelp.me. – URL: https://chinahelp.me/criminal/ugolovnyj-kodeks-knr-osobennaya-chast-stati-232-276 (дата обращения: 01.05.2025).

28. Уголовный кодекс КНР. Особенная часть (статьи 277–367) // Chinahelp.me. – URL: https://chinahelp.me/criminal/ugolovnyj-kodeks-knr-osobennaya-chast-stati-277-367 (дата обращения: 01.05.2025).

29. Мазуров, В. А. Компьютерные преступления: анализ уголовного законодательства США и Германии / В. А. Мазуров, Д. П. Потапов, В. В. Сорокин // Известия Алтайского государственного университета. – 2005. – № 2. – С. 59–66.

30. Чернякова, А. В. Международный и зарубежный опыт уголовно-правового противодействия хищениям, совершаемым с использованием компьютерной информации / А. В. Чернякова // Юридическая наука и правоохранительная практика. – 2018. – № 4 (46). – С. 168–179.

31. Уголовный кодекс Французской Республики // Legifrance. – URL: https://www.legifrance.gouv.fr/codes/texte_lc/LEGITEXT000006070719/2021-03-19 (дата обращения: 01.05.2025).

32. Уголовный кодекс Германии // Публичная бесплатная политико-правовая интернет-библиотека Пашкова Романа. – URL: https://constitutions.ru/?p=24969 (дата обращения: 01.05.2025).

Поступила в редакцию 13.05.2025 г.

Контакты: alprimakov@mail.ru (Примаков Алексей Николаевич, Романюк Даниил Валерьевич)

Primakov A. N., Romanyuk D. V.

CRIMINAL LIABILITY FOR THEFT COMMITTED USING COMPUTER INFORMATION ACCORDING TO THE LEGISLATION OF THE REPUBLIC OF BELARUS AND FOREIGN STATES

Based on the results of a comparative legal analysis of the criminal legislation of the Republic of Belarus, the Russian Federation, the Commonwealth of Independent States, European and other countries that provide for liability for thefts committed using information and telecommunications technologies and computer information, the article defines legislative approaches to establishing the main criminal-legal features of these types of crimes, identifies problematic and controversial issues related to their regulation, and formulates some proposals for their resolution. In order to most effectively counteract this form of theft, it is noted that it is necessary to change the judicial and investigative approach to the qualification of illegal actions, liability for which occurs under Articles 209 and 212 of the Criminal Code of the Republic of Belarus. It is determined that when resolving this issue, it is necessary to take into account the initial position of the legislator regarding the form of theft specifically identified in the criminal law, which is associated with the use of computer

technology (Article 212 of the Criminal Code of the Republic of Belarus), and interpret it in a broader law enforcement meaning.

Keywords: *cybercrime, theft, fraud, information and telecommunication technologies, computer information, criminal liability, qualification, regulation.*