УДК 343.3

ПРЕСТУПЛЕНИЯ ПРОТИВ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ: УГОЛОВНО-ПРАВОВАЯ ХАРАКТЕРИСТИКА И ПРОБЛЕМЫ КВАЛИФИКАЦИИ

Д. С. КРУГЛЕНЯ
(Представлено: Е. В. Чижик)

В статье исследуются объективные и субъективные признаки преступлений против компьютерной безопасности по законодательству Республики Беларусь (глава 31 УК). Анализируются проблемы квалификации, связанные с оценочными признаками существенного вреда, неопределённостью технических терминов и разграничением со смежными составами.

Ключевые слова: *компьютерная безопасность, компьютерная информация, несанкционированный доступ, существенный вред.*

Цифровая трансформация общественных отношений и стремительное внедрение информационно-коммуникационных технологий во все сферы жизнедеятельности государства и общества привели к качественному изменению структуры преступности. Рост числа посягательств в виртуальном пространстве создает реальную угрозу для нормального функционирования как отдельных институтов, так и национальной безопасности Республики Беларусь в целом. Осознавая масштаб потенциальных угроз, законодатель определил компьютерную безопасность в качестве самостоятельного объекта уголовно-правовой охраны, закрепив его в отдельной главе 31 Уголовного кодекса Республики Беларусь (далее – УК) [1]. Законом Республики Беларусь от 26 мая 2021 г. № 112-З «Об изменении кодексов по вопросам уголовной ответственности» глава была переименована из «Преступления против информационной безопасности» в «Преступления против компьютерной безопасности»; количество составов сокращено с семи до пяти, объединены ранее самостоятельные статья 350 (модификация компьютерной информации) и статья 351 (компьютерный саботаж) в состав с альтернативными действиями [2].

Анализ судебной практики показал, что за период с 2021 года по первое полугодие 2025 года за преступления, предусмотренные статьями 349-355 УК, осуждено 52 лица, при этом фактов осуждения по статье 355 УК (нарушение правил эксплуатации компьютерной системы или сети) не выявлено. Несмотря на относительно небольшое число осуждённых по статьям главы 31 УК, удельный вес судимости за компьютерные преступления в общей структуре судимости увеличился и составил 0,6 % [3, с. 40-41]. Низкая правоприменительная активность во многом объясняется трудностями квалификации, что и предопределяет актуальность настоящего исследования.

В главе 31 УК законодатель включил пять составов преступлений: несанкционированный доступ к компьютерной информации (статья 349), уничтожение, блокирование или модификация компьютерной информации (статья 350), неправомерное завладение компьютерной информацией (статья 352), разработка, использование, распространение либо сбыт вредоносных компьютерных программ или специальных программных или аппаратных средств (статья 354) и нарушение правил эксплуатации компьютерной системы или сети (статья 355).

Родовым объектом преступлений против компьютерной безопасности выступают общественные отношения, обеспечивающие состояние защищённости (конфиденциальности, целостности, подлинности, доступности и сохранности) компьютерной информации при её получении, передаче, обработке, накоплении, хранении, распространении, предоставлении, а также компьютеров, компьютерных систем и сетей, машинных носителей, содержащих, обрабатывающих или передающих такую информацию. Специфичность указанных составов обусловлена особенностями их предмета – компьютерной информации, определение которой закреплено в статье 4 УК: «это информация, хранящаяся в компьютерной системе, сети или на машинных носителях, обрабатываемая компьютерной системой либо передаваемая в пространстве с помощью любых программно-технических средств» [1].

Деяние при совершении преступлений против компьютерной безопасности проявляется в активном поведении субъекта. Большинство составов преступлений сконструированы как материальные, поэтому общественно опасные последствия выступают обязательным признаком объективной стороны, который подлежит установлению в каждом конкретном случае. Преступления считаются оконченными с момента наступления последствий – существенного вреда или тяжких последствий. Исключение составляет статья 354 УК, имеющая формальный состав: преступление считается оконченным с момента совершения любого из указанных действий (разработка, использование, распространение или сбыт), независимо от наступления вредных последствий.

Существенный вред может носить как материальный, так и нематериальный характер. По делам рассматриваемой категории он наиболее часто носит неимущественный характер и выражается в нарушении конституционных прав граждан, незаконном вмешательстве в личную жизнь, дискредитации деловой

репутации, причинении морального вреда, нарушении работы организаций. Понятие тяжких последствий также является оценочным. Перечень тяжких последствий в части 2 статьи 349 УК (крушения, аварии, катастрофы, несчастные случаи с людьми, отрицательные изменения в окружающей среде) не является исчерпывающим [6, с. 529].

Субъект преступлений против компьютерной безопасности – физическое вменяемое лицо, достигшее шестнадцатилетнего возраста (общий субъект). Исключение составляет преступление, предусмотренное статьей 355 УК, субъект которого специальный: лицо, имеющее доступ к компьютерной системе или сети (системный администратор, оператор, иное лицо, на законных основаниях использующее компьютер) [6].

Субъективная сторона большинства основных составов характеризуется умышленной формой вины. Вместе с тем преступления, предусмотренные частью 1 и 2 статьи 349 УК (за исключением несанкционированного доступа из корыстной заинтересованности), частью 3 статьи 350, частью 3 статьи 352, частью 3 статьи 354, статьей 355 УК могут быть совершены только по неосторожности, т. е. форму и вид вины определяет психическое отношение лица к наступившим последствиям. Так, по части 1 статьи 349 УК лицо сознаёт, что без соответствующего разрешения с нарушением системы защиты получает доступ к компьютерной информации, предвидит возможность причинения существенного вреда, но без достаточных оснований рассчитывает на его предотвращение (легкомыслие) или не предвидит такой возможности, хотя должно было и могло её предвидеть (небрежность). При этом если несанкционированный доступ совершён из корыстной заинтересованности, преступление характеризуется умышленной формой вины, а наступление последствий не является обязательным.

Иллюстрацией комплексного анализа объективных и субъективных признаков может служить дело Б., осуждённого за умышленное блокирование компьютерной информации. Как установил суд, Б. заблокировал доступ к электронным учебным материалам и системам дистанционного обучения, предназначенным для обеспечения учебного процесса в учреждениях образования. Суд пришёл к выводу о том, что преступными действиями Б. причинён существенный вред, который выразился в нарушении нормальной работы учреждений образования и нарушении прав граждан на получение образования [3, с. 43]. В данном случае судом были установлены как объективные признаки – блокирование компьютерной информации и наступление существенного вреда, так и субъективные – прямой умысел виновного на блокирование.

Проблемные аспекты квалификации преступлений против компьютерной безопасности.

Первая группа проблем связана с отсутствием единообразного определения ряда технических терминов, использованных законодателем при конструировании составов. Диспозиции норм статей главы 31 УК насыщены специальными техническими терминами (система защиты, компьютерная система и сеть, машинный носитель, программно-аппаратное средство), которые не имеют нормативного определены. В пункте 3 постановления Президиума Верховного Суда Республики Беларусь от 18 декабря 2019 г. № 4 «О практике рассмотрения судами уголовных дел о преступлениях против информационной безопасности (глава 31 УК)» (далее – Постановление № 4) указано, что компьютерная система представляет комплекс аппаратных и программных средств, предназначенных для автоматизированного сбора, хранения, обработки, передачи и получения информации [4]. Однако в различных научно-практических комментариях компьютерная система трактуется по-разному: как отдельный компьютер, как комплексы с хотя бы одной электронно-вычислительной машиной (далее – ЭВМ) или как организационно упорядоченная совокупность массивов информации и информационных технологий, образующим элементом которой является хотя бы одна ЭВМ [5]. Это порождает различные подходы к квалификации.

Вторая проблема – определение существенного вреда. В части 1 статьи 349, части 1 статьи 350, статье 352 и части 1 статьи 355 УК существенный вред является обязательным признаком объективной стороны, однако критерии его разграничения с несущественным вредом в законодательстве не определены. В доктрине существуют различные подходы к количественной оценке материального вреда. В соответствии с постановлением № 4, вывод о причинении существенного вреда должен подтверждаться достаточной совокупностью доказательств и мотивироваться в приговоре [4], однако количественные критерии не определены. Это создает условия для субъективного усмотрения правоприменителя и нарушает принцип правовой определенности.

Третья проблема – отграничение преступлений против компьютерной безопасности от смежных составов. Зачастую возникает необходимость отграничения статьи 349 УК (несанкционированный доступ) от статьи 350 УК (уничтожение, блокирование или модификация компьютерной информации), а также от преступлений против собственности (статьи 205-212 УК), вымогательства (статья 208 УК) и мошенничества (статья 209 УК).

Показательным является дело П., который, неправомерно завладев авторизационными данными (логинами и паролями) для доступа к профилю потерпевшей в социальной сети и почтовому ящику, вводил в компьютерную систему заведомо ложную информацию о лице, производящем действия по авторизации от имени законного пользователя. Районный суд признал П. виновным в модификации компьютерной информации (часть 1 статьи 350 УК) и несанкционированном доступе к компьютерной информации (часть 1 статьи 349 УК). Однако суд апелляционной инстанции не согласился с осуждением П. за умышленную

модификацию: установлено, что П. не совершал действий, направленных на умышленную модификацию компьютерной информации, а вводил логин и пароль с целью ознакомления с личной перепиской потерпевшей. Компьютерная информация при введении логина и пароля изменена не была. Действия П. были переквалифицированы на часть 1 статьи 203-1 УК (незаконные действия в отношении информации о частной жизни и персональных данных) [3, с. 44]. Данный пример демонстрирует, что разграничение между модификацией компьютерной информации и иными составами должно проводиться прежде всего по субъективной стороне – направленности умысла виновного, а также по факту изменения информации.

Четвёртая проблема – квалификация по совокупности преступлений. Несанкционированный доступ к компьютерной информации, неправомерное завладение ею или использование вредоносных программ нередко выступают способом совершения иных преступлений – хищений (статьи 205-212 УК), мошенничества (статья 209 УК), вымогательства (статья 208 УК). Если неправомерное завладение компьютерной информацией выступает в качестве способа совершения иного преступления, имеет место совокупность преступления, предусмотренного статьей 352 УК, и соответствующего преступления, способом которого явилось неправомерное завладение. Аналогичный подход применим и к статье 349 УК: несанкционированный доступ, совершённый в целях последующего хищения имущества, квалифицируется по совокупности с соответствующей статьёй о хищении.

Так, гражданин Новиков скрыто установил на компьютер потерпевшей компьютерную программу keylog_run.exe, предназначенную для несанкционированного завладения информацией, вводимой посредством клавиатуры. С её помощью он скопировал логины и пароли к учётным записям потерпевшей в социальных сетях, затем осуществил доступ к её странице и сменил пароль, после чего потребовал 300 рублей за разблокировку. В данном случае действия Новикова образуют совокупность преступлений: использование вредоносной компьютерной программы (часть 1 статьи 354 УК), несанкционированный доступ к компьютерной информации (часть 1 статьи 349 УК), неправомерное завладение компьютерной информацией (часть 1 статьи 352 УК) и вымогательство (часть 1 статьи 208 УК) [6]. Этот пример демонстрирует, что преступные посягательства в сфере компьютерной информации редко исчерпываются рамками одной статьи главы 31 УК и требуют квалификации по нескольким статьям.

Пятая проблема связана с разграничением несанкционированного копирования и простого просмотра информации. Сам факт вызова или просмотра компьютерной информации состава преступления, предусмотренного статьей 352 УК, не образует – для этого необходимо установить факт копирования информации на другой носитель, отличный от исходного. Спорным является вопрос об автоматическом копировании информации в оперативную память компьютера, которое предшествует выводу информации на экран. Такое копирование является автоматическим (неконтролируемым) временным процессом, носящим вспомогательную функцию, при котором отсутствует факт переноса информации на другой материальный носитель как результат волевого деяния лица.

Таким образом, можно сделать следующие выводы. Родовым объектом преступлений против компьютерной безопасности являются общественные отношения, обеспечивающие защищённость компьютерной информации и компьютерных систем, сетей и машинных носителей, а специфика составов определяется предметом – компьютерной информацией, определение которой закреплено в статье 4 УК. Большинство составов главы 31 УК являются материальными и требуют установления общественно опасных последствий; по конструкции объективной стороны только статья 354 УК имеет формальный состав. Что касается субъективной стороны, то основные составы характеризуются умышленной формой вины, при этом ряд составов (часть 1 статьи 349, статья 355 УК) может совершаться по неосторожности по отношению к последствиям, тогда как статья 354 УК совершается исключительно с прямым умыслом. Основными проблемами квалификации остаются: отсутствие нормативного определения ключевых технических терминов, неопределённость оценочного признака «существенный вред», трудности отграничения смежных составов главы 31 УК от преступлений против собственности, а также сложность квалификации по совокупности преступлений. В целях повышения эффективности уголовно-правовой охраны компьютерной безопасности представляется целесообразным: во-первых, закрепить в УК определения понятий «компьютерная система», «компьютерная сеть» и «машинный носитель»; во-вторых, установить минимальный количественный критерий существенного вреда по аналогии с примечанием к главе 24 УК (ущерб в значительном размере).

ЛИТЕРАТУРА

1. Уголовный кодекс Республики Беларусь : 9 июля 1999 г. № 275-З : принят Палатой представителей 2 июня 1999 г. : одобрен Советом Республики 24 июня 1999 г. : в ред. Закона Респ. Беларусь от 17 февраля 2025 г. № 61-З // ЭТАЛОН : информ.-поисковая система (дата обращения: 08.10.2026).
2. Об изменении кодексов по вопросам уголовной ответственности : Закон Респ. Беларусь от 26 мая 2021 г., № 112-З // Нац. прав. интернет-портал Респ. Беларусь. – URL: https://pravo.by/document/?guid=12551&p0=H12100112 (дата обращения: 08.10.2026).

3. Царук, Р. О судебной практике по делам о киберпреступлениях и мошенничестве, совершенных с использованием информационно-коммуникационных технологий (ст. 208, 209, 212, 222, 349-355 УК) / Р. Царук // Судовы веснік. – 2026. – № 2. – С. 40–47.
4. О практике рассмотрения судами уголовных дел о преступлениях против информационной безопасности (глава 31 УК) : постановление Президиума Верхов. Суда Респ. Беларусь от 18 дек. 2019 г., № 4 // ЭТАЛОН : информ.-поисковая система (дата обращения – 08.10.2026).
5. Научно-практический комментарий к Уголовному кодексу Республики Беларусь / Т. П. Афонченко [и др.] ; под ред. В. М. Хомича, А. В. Баркова, В. В. Марчука. - Минск : Нац. центр правовой информ. Респ. Беларусь, 2019. – 997 с.
6. Уголовное право : учеб. пособие / А. В. Барков [и др.] : под ред. А. Л. Савенка, А. В. Шидловского, К. С. Захилько. – Минск : БГУ, 2023. – 607 с. (Совершенствование магистерской программы по уголовной юстиции).