УДК 343.3

ГЕНЕЗИС ЗАКОНОДАТЕЛЬСТВА РЕСПУБЛИКИ БЕЛАРУСЬ ОБ УГОЛОВНОЙ ОТВЕТСТВЕННОСТИ ЗА СОВЕРШЕНИЕ ПРЕСТУПЛЕНИЙ ПРОТИВ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ

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

В статье отражены результаты историко-правового исследования генезиса уголовного законодательства Республики Беларусь об ответственности за совершение преступлений против компьютерной безопасности. Анализируются предпосылки выделения главы 31 УК, ключевые изменения 2021 года и их влияние на правоприменительную практику. Обосновывается необходимость дальнейшего совершенствования понятийного аппарата и дифференциации ответственности за совершение преступлений против компьютерной безопасности.

Развитие информационных технологий и цифровизация всех сфер жизнедеятельности общества привели к качественному изменению структуры преступности. Если в 2015 г. в Республике Беларусь было зарегистрировано 2 440 киберпреступления, то в 2020 г. – уже 25 561, что свидетельствует о десятикратном росте менее чем за пять лет [1]. Подобная динамика объективно потребовала адекватного правового реагирования, направленного на создание эффективного механизма уголовно-правовой охраны компьютерной безопасности. Вместе с тем процесс формирования соответствующего законодательства сопровождался как расширением круга криминализированных деяний, так и последующим пересмотром отдельных составов, что было обусловлено как потребностями правоприменительной практики, так и развитием научных представлений о природе посягательств в цифровой среде.

До принятия Уголовного кодекса Республики Беларусь от 9 июля 1999 г. № 275-З (далее – УК) [2] общественно опасные деяния, связанные с использованием компьютерной техники, квалифицировались по традиционным статьям о преступлениях против собственности, служебных преступлениях или разглашении тайны, а при отсутствии соответствующих признаков – вообще не могли быть квалифицированы. Такой подход был неэффективным, поскольку не учитывал нематериальный характер компьютерной информации и специфику механизма причинения вреда. Информация как самостоятельная ценность не охватывалась существовавшими составами в полной мере. Именно потребность уголовно-правового регулирования информационных общественных отношений вызвала появление в УК главы 31, которая первоначально именовалась: «Преступления против информационной безопасности» и объединяла семь статей (349 – 355 УК). Законодатель криминализировал несанкционированный доступ к компьютерной информации (статья 349 УК), модификацию компьютерной информации (статья 350 УК), компьютерный саботаж (статья 351 УК), неправомерное завладение компьютерной информацией (статья 352 УК), изготовление либо сбыт специальных средств для получения неправомерного доступа (статья 353 УК), разработку, использование либо распространение вредоносных программ (статья 354 УК), а также нарушение правил эксплуатации компьютерной системы или сети (статья 355 УК). Первым зарегистрированным в Беларуси преступлением в сфере высоких технологий стало деяние, совершенное 20 ноября 1998 г. Так, неустановленное лицо, внедрив в программное обеспечение «троянскую» программу BackOrifice, осуществило несанкционированный доступ к сетевым реквизитам пользователей крупнейшего столичного сервис-провайдера [4].

К концу 2010-х годов практика применения норм главы 31 УК выявила ряд проблем. Наиболее существенными из них стали: неопределенность понятия «существенный вред» как оценочной категории; отсутствие единообразного подхода к определению термина «компьютерная система»; трудности разграничения уголовно наказуемого несанкционированного доступа и административного правонарушения, предусмотренного статьей 23.4 Кодекса об административных правонарушениях (далее – КоАП); необходимость приведения национального законодательства в соответствие с международными стандартами, в частности с положениями Конвенции Совета Европы о преступности в сфере компьютерной информации (Будапештской конвенции). В соответствии с Законом Республики Беларусь от 26 мая 2021 г. № 112-З «Об изменении кодексов по вопросам уголовной ответственности», глава 31 УК была изложена в новой редакции и переименована: «Преступления против компьютерной безопасности» [3]. Количество статей сократилось с семи до пяти: статьи 350 и 351 УК были объединены в один альтернативный материальный состав, а статья 353 УК исключена. Помимо этого, была скорректирована диспозиция части 1 статьи 349 УК: из нее исключен такой признак субъективной стороны, как «иная личная заинтересованность», что было направлено на законодательное разграничение уголовной и административной ответственности.

Несмотря на проведенную модернизацию, анализ судебной практики свидетельствует о сохранении ряда дискуссионных вопросов. Например, понятие «существенный вред» по–прежнему остается оценочным,

что порождает неопределенность при квалификации. В судебной практике существенный вред чаще всего признается нематериальным и выражается в нарушении конституционных прав граждан, в частности права на тайну корреспонденции. Так, приговором суда Малоритского района Брестской области от 12 октября 2023 г. Г. был осужден по части 1 статьи 352 УК за несанкционированное копирование фрагментов личной переписки потерпевшей в социальных сетях с последующим их распространением [5]. Существенный вред выразился в нарушении конституционного права на тайну переписки и распространении сведений, которые потерпевшая желала сохранить в тайне. Применение аналогичного подхода прослеживается в приговоре суда Бобруйского района и г. Бобруйска от 20 марта 2023 г. [6]. Так, действия Г. по изменению пароля и блокированию доступа к странице бывшей супруги в социальной сети были квалифицированы по части 1 статьи 350 УК, а существенный вред выразился в нарушении конституционного права на защиту от незаконного вмешательства в личную жизнь. Однако одной ссылки на нарушение конституционных прав недостаточно: для признания вреда существенным нужно показать конкретные последствия – имущественные потери, дезорганизацию работы организаций или иные негативные изменения, которые можно измерить.

Остается актуальной проблема разграничения преступлений против компьютерной безопасности и смежных составов. Показательным является приговор суда Ш. района от 17 апреля 2024 г., в котором действия Ф. были квалифицированы по совокупности части 1 статьи 208, части 2 статьи 209 и части 2 статьи 212 УК. Ф. под угрозой распространения интимных изображений вымогал у потерпевшей денежные средства, а также, завладев реквизитами доступа к ее интернет-банкингу, похитил денежные средства путем модификации компьютерной информации [7]. Суд правильно разграничил составы, однако подобные дела демонстрируют сложность отграничения хищения путем модификации компьютерной информации от мошенничества и вымогательства, что требует от правоприменителя тщательного анализа субъективной стороны и способа завладения имуществом.

Заслуживает внимания вопрос о соотношении уголовной и административной ответственности. Исключение признака «иная личная заинтересованность» из диспозиции нормы части 1 статьи 349 УК создало ситуацию, при которой несанкционированный доступ, совершенный, например, из любопытства или хулиганских побуждений, при отсутствии корыстной заинтересованности и существенного вреда влечет лишь административную ответственность (статья 23.4 КоАП). Представляется, что такой подход не в полной мере учитывает степень общественной опасности деяния, поскольку посягательство на конституционные права граждан может причинять существенный нематериальный вред и при отсутствии корыстной заинтересованности.

Кроме того, недостаточно четко определен понятийный аппарат. Термины «компьютерная система», «компьютерная сеть», «машинный носитель», используемые в диспозициях норм главы 31 УК, а также в определении компьютерной информации (часть 18, статьи 4 УК), не имеют нормативного определения, что создает трудности при квалификации и требует обращения к подзаконным актам и доктринальным источникам. Использование узких технических терминов без однозначного толкования изначально создаёт трудности для правоприменителя.

Анализ приговоров по делам о преступлениях против компьютерной безопасности показывает, что суды в целом единообразно подходят к квалификации наиболее распространенных деяний. Так, приговором суда Солигорского района от 10 ноября 2023 г. [8] И. был осужден по части 1 статьи 349 УК за несанкционированный доступ к учетной записи онлайн-сервиса с использованием сохраненных в браузере логина и пароля потерпевшего; суд квалифицировал деяние как совершенное из корыстной заинтересованности. Приговором суда Браславского района от 2 октября 2025 г. [9] О. осужден по части 1 статьи 349 и части 2 статьи 354 УК за использование вредоносных программ для подбора паролей к учетным записям интернет-ресурсов в составе группы лиц по предварительному сговору. Данные примеры свидетельствуют о том, что нормы главы 31 УК применяются достаточно активно. Вместе с тем обращает на себя внимание тот факт, что в структуре судимости за компьютерные преступления устойчиво доминируют деяния, связанные с хищениями имущества путем модификации компьютерной информации (статья 212 УК) и мошенничеством (статья 209 УК). Показательным в этом контексте является приговор суда Первомайского района г. Минска от 11 января 2025 г. по делу П., которая в результате технического сбоя в программном обеспечении банка получила доступ к денежным средствам, отобразившимся на ее карт-счетах в результате ошибки [10]. Суд квалифицировал ее действия по части 4 статьи 212 УК, однако впоследствии переквалифицировал на часть 4 статьи 205 УК, указав, что обвиняемая не изменяла компьютерную информацию и не вносила заведомо ложные сведения, а лишь воспользовалась технической ошибкой. Данный пример показывает, что суды при квалификации деяний, связанных с использованием компьютерных систем, отдают приоритет традиционным составам, если отсутствуют признаки непосредственного воздействия на компьютерную информацию.

Таким образом, генезис законодательства Республики Беларусь об уголовной ответственности за совершение преступлений против компьютерной безопасности представляет собой последовательную смену трёх основных этапов, в которых нашла отражение эволюция правовой охраны компьютерной безопасности: до 1999 г. – квалификация соответствующих деяний по традиционным нормам; 1999–2021 гг. – формирование

и развитие главы 31 УК в первоначальной редакции; с 2021 г. – модернизация главы 31 УК, которая выразилась в переименовании, сокращении числа составов и корректировке диспозиций. Изменения 2021 г. были обусловлены потребностями правоприменительной практики и в целом способствовали повышению определенности уголовного закона, однако не устранили всех проблемных аспектов. В целях повышения эффективности уголовно–правовой охраны компьютерной безопасности представляется целесообразным: во-первых, закрепить в УК нормативное определение понятий «компьютерная система», «компьютерная сеть» и «машинный носитель»; во-вторых, конкретизировать критерии существенного вреда, в том числе путем указания на возможность его выражения в значительном имущественном ущербе; в-третьих, рассмотреть вопрос о криминализации неправомерного завладения компьютерной информацией, совершенного из корыстной заинтересованности и не повлекшего существенного вреда, по аналогии с хищениями, не причинившими значительного ущерба.

ЛИТЕРАТУРА

1. Сведения о регистрации и предварительном расследовании преступлений по Республике Беларусь за 2006–2021 годы / М-во внутр. дел Респ. Беларусь, Информ.-аналит. упр. – Минск : [б. и.], 2007–2022.
2. 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).
3. 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).
4. История УПК // Управление по раскрытию преступлений в сфере высоких технологий МВД Респ. Беларусь. – URL: https://minsk.mvd.gov.by/ru/page/upravlenie-po-raskrytiyu-prestuplenij-v-sfere-vysokih-tehnologij/istoriya-urpsvt (дата обращения: 08.10.2026).
5. Приговор суда Малоритского района Брестской области от 12 окт. 2023 г. по делу № ***/16У2358 (ч. 1 ст. 352 УК) // Банк данных «Судебная практика» ЭТАЛОН-ONLINE. – URL: https://etalonline.by/dpt/?tbd=70 (дата обращения: 08.10.2026).
6. Приговор суда Бобруйского района и г. Бобруйска от 20 марта 2023 г. (ч. 1 ст. 350 УК) // Банк данных «Судебная практика» ЭТАЛОН-ONLINE. – URL: https://etalonline.by/dpt/?tbd=70 (дата обращения: 08.10.2026).
7. Приговор суда Шкловского района Могилевской области от 17 апр. 2024 г. (ч. 1 ст. 208, ч. 2 ст. 209, ч. 2 ст. 212 УК) // Банк данных «Судебная практика» ЭТАЛОН-ONLINE. – URL: https://etalonline.by/dpt/?tbd=70 (дата обращения: 08.10.2026).
8. Приговор суда Солигорского района Минской области от 10 нояб. 2023 г. (ч. 1 ст. 349 УК) // Банк данных «Судебная практика» ЭТАЛОН-ONLINE. – URL: https://etalonline.by/dpt/?tbd=70 (дата обращения: 08.10.2026).
9. Приговор суда Браславского района Витебской области от 2 окт. 2025 г. (ч. 1 ст. 349, ч. 2 ст. 354 УК) // Банк данных «Судебная практика» ЭТАЛОН-ONLINE. – URL: https://etalonline.by/dpt/?tbd=70 (дата обращения: 08.10.2026).
10. Приговор суда Первомайского района г. Минска от 11 янв. 2025 г. по делу П. (ч. 4 ст. 205 УК) // Банк данных «Судебная практика» ЭТАЛОН-ONLINE. – URL: https://etalonline.by/dpt/?tbd=70 (дата обращения: 08.10.2026).