УДК 343.3/.7:004 https://doi.org/10.33619/2414-2948/131/53

ЮРИДИЧЕСКАЯ ОТВЕТСТВЕННОСТЬ ЗА ПРАВОНАРУШЕНИЯ В ИНФОРМАЦИОННОЙ СФЕРЕ КЫРГЫЗСКОЙ РЕСПУБЛИКИ: ПРОБЕЛЫ УГОЛОВНОГО И АДМИНИСТРАТИВНОГО ЗАКОНОДАТЕЛЬСТВА В УСЛОВИЯХ ЦИФРОВИЗАЦИИ

©Сейдакматов Н. А., *ORCID: 0009-0004-2261-4967, канд. юрид. наук,*
Кыргызско-Российская академия образования, г. Бишкек, Кыргызстан

LEGAL LIABILITY FOR OFFENSES IN THE INFORMATION SPHERE OF THE KYRGYZ REPUBLIC: GAPS IN CRIMINAL AND ADMINISTRATIVE LAW IN THE CONTEXT OF DIGITAL TRANSFORMATION

©Seidakmatov N., *ORCID: 0009-0004-2261-4967, Ph.D.,*
Kyrgyz-Russian Academy of Education, Bishkek, Kyrgyzstan

Аннотация. Анализируется система юридической ответственности за правонарушения в информационной сфере Кыргызской Республики после кодификационной реформы 2021 года и принятия Закона «О кибербезопасности Кыргызской Республики» (2024) и Цифрового кодекса КР (2025). На основе действующих норм Уголовного кодекса КР, Кодекса КР о правонарушениях и официальной статистики МВД КР выявлены структурные пробелы правового регулирования: узость главы 40 УК КР «Преступления против кибер-безопасности», фрагментарность (точечный, а не системный характер) вносимых изменений, недостаточная согласованность уголовной, административной и цифровой отраслей законодательства, низкая раскрываемость и латентность киберпреступлений. Сформулированы предложения по устранению выявленных пробелов.

Abstract. The article analyzes the system of legal liability for offenses in the information sphere of the Kyrgyz Republic following the 2021 codification reform and the adoption of the Law "On Cybersecurity of the Kyrgyz Republic" (2024) and the Digital Code of the Kyrgyz Republic (2025). Based on the current provisions of the Criminal Code of the Kyrgyz Republic, the Code of Offenses of the Kyrgyz Republic, and official statistics from the Ministry of Internal Affairs of the Kyrgyz Republic, structural gaps in legal regulation are identified: the narrow scope of Chapter 40 of the Criminal Code, "Offenses against Cybersecurity"; the fragmentary (piecemeal rather than systemic) nature of legislative amendments; insufficient coordination between criminal, administrative, and digital branches of legislation; and the low detection rate and high latency of cybercrimes. Proposals for addressing the identified gaps are formulated.

Ключевые слова: информационная безопасность; кибербезопасность; юридическая ответственность; Уголовный кодекс Кыргызской Республики.

Keywords: information security; cybersecurity; legal liability; Criminal Code of the Kyrgyz Republic.

Актуальность темы обусловлена нарастающим разрывом между темпами цифровизации государственного управления, финансового сектора и повседневной жизни граждан Кыргызской Республики, с одной стороны, и способностью действующего уголовного и административного законодательства своевременно и системно реагировать на новые формы противоправного поведения в информационной сфере с другой. По официальным данным

Тип лицензии CC: Attribution 4.0 International (CC BY 4.0)

МВД КР, в 2025 г было зарегистрировано более 1500 киберпреступлений, а за первые три месяца 2026 г уже 1140, при этом ущерб граждан от действий киберпреступников за 2025 г превысил 826 млн. сомов, из которых возмещено менее 10%. При этом, по экспертным оценкам, фиксируется не более 15% реально совершаемых посягательств, а уголовные дела возбуждаются лишь по половине зарегистрированных случаев. Представитель МВД КР прямо указывает на то, что «наиболее болезненная проблема — пробелы в законодательстве», отмечая, что нормы принимаются точечно, тогда как необходим пакетный подход с одновременными изменениями Уголовного, Уголовно-процессуального кодексов и Кодекса о правонарушениях (https://clck.ru/3WRbgA).

До 2021 г основу составлял Уголовный кодекс КР 2017 г, где ответственность за посягательства на компьютерную информацию была сосредоточена в гл. 42 «Преступления против информационной безопасности» (ст. 304–306): неправомерный доступ к компьютерной информации, создание вредоносных программ, компьютерный саботаж [6].

С 1 декабря 2021 г вступил в силу новый Уголовный кодекс КР от 28 октября 2021 г №127, где профильная глава была переименована в главу 40 «Преступления против кибер-безопасности» и включает ст. 319 (несанкционированный доступ к компьютерной информации и электронным документам, в информационную систему или сеть электросвязи), 320 (создание вредоносных программных продуктов), 321 (кибер-саботаж) и 322 (массовое распространение электронных сообщений). Одновременно был принят Кодекс КР о правонарушениях от 28 октября 2021 г №128, разграничивший уголовную и административную (проступочную) ответственность физических, должностных и юридических лиц (https://clck.ru/3WRbiv) [7].

Параллельно с кодифицированным законодательством действует комплекс специальных актов: 17 июля 2024 г принят Закон КР №121 «О кибербезопасности Кыргызской Республики», вводящий понятия киберинцидента, кибератаки и информационной инфраструктуры и возлагающий контроль на профильные госорганы [1].

Контроль за защитой информации в государственных информационных системах возложен совместно на профильный комитет по информационным технологиям и связи и Государственный комитет национальной безопасности КР. Наконец, 31 июля 2025 г принят Цифровой кодекс КР № 178, который систематизировал регулирование цифровых отношений, включая защиту персональных данных, ранее регулировавшуюся отдельным Законом «Об информации персонального характера» 2008 г. Данный закон был инициирован в том числе в связи с ростом числа киберпреступлений, совершаемых с использованием персональных данных граждан. Закон «Об информации персонального характера» утратил силу 5 февраля 2026 г, а Цифровой кодекс введен в действие по истечении шести месяцев со дня официального опубликования вводящего закона, принятого Жогорку Кенешем 18 июня 2025 г (https://clck.ru/3WRbmg; https://dpa.gov.kg/ru/npa/17; https://clck.ru/3WRbo9).

Действующая гл. 40 УК КР охватывает лишь классические компьютерные посягательства (несанкционированный доступ, вредоносное ПО, кибер-саботаж, массовая рассылка), но не содержит самостоятельных составов, отражающих современные способы совершения информационных правонарушений — фишинг, использование дипфейков, автоматизированный сбор и продажу баз данных, компрометацию облачной инфраструктуры. Правоохранители прямо указывают на растущую сложность выявления преступлений, совершенных с использованием дипфейков, что подтверждает объективную потребность в специализации уголовно-правовых норм (https://clck.ru/3WRbcT).

Наиболее показательный пример — регулирование ответственности за так называемое дропперство (передачу третьим лицам доступа к банковским счетам, электронным средствам платежа и SIM-картам для обналичивания похищенных средств). Законом КР от 18 июля 2025

Тип лицензии CC: Attribution 4.0 International (CC BY 4.0)

г №151 Уголовный кодекс дополнен ст. 209-1 «Умышленная передача или продажа третьим лицам электронных средств платежа, кошелька виртуального актива и SIM-карты» [2-5].

Показательно, что данная норма помещена не в главу о киберпреступлениях, а в главу 28 УК КР «Преступления против собственности», что свидетельствует об отсутствии единого системного подхода к классификации информационных правонарушений и рассредоточении родственных составов по разным разделам кодекса. При этом сами представители МВД КР признают недостаточность точечных решений и необходимость пакетной реформы сразу нескольких кодексов (https://clck.ru/3WRbgA).

Несмотря на введение уголовной ответственности за дропперство, статистика привлечения к ответственности остается несопоставимой с масштабом проблемы: в 2025 г к ответственности привлечено 226 дропперов на фоне тысяч зарегистрированных киберпреступлений и сотен миллионов сомов ущерба, что указывает на разрыв не столько в материальных нормах, сколько в процессуальном и организационном обеспечении их применения (сбор цифровых доказательств, трансграничное взаимодействие, квалификация деяний, совершенных организованными группами) (https://clck.ru/3WRbbX).

Кодекс КР о правонарушениях №128 изначально не содержал развитой системы составов, обеспечивающих защиту персональных данных и информационной инфраструктуры некритического уровня, эта функция долгое время оставалась не обеспеченной адекватными административными санкциями. Данный пробел лишь частично закрыт последними изменениями: с 23 ноября 2025 г организации, обрабатывающие персональные данные, могут быть привлечены к ответственности в виде штрафов по новым статьям Кодекса о правонарушениях (413-2–413-5) (https://clck.ru/3WRbvi).

Однако сохраняются следующие проблемы: Разрыв во времени между введением материальных обязанностей операторов персональных данных Цифровым кодексом (с февраля 2026 г) и относительно небольшим периодом апробации соответствующих составов административной ответственности, что не позволяет пока оценить их эффективность; Отсутствие четких критериев разграничения административного проступка и преступления (например, ст. 319 УК КР «Несанкционированный доступ к компьютерной информации» и смежных составов Кодекса о правонарушениях) по признаку общественной опасности и размера причиненного вреда, что создает риск неединообразной квалификации; Недостаточность санкций для юридических лиц — операторов критической информационной инфраструктуры за нарушение требований Закона «О кибербезопасности» №121, притом что закон возлагает контрольные функции сразу на два госоргана без четкого разграничения их компетенции и, соответственно, ответственности за бездействие (https://theins.ru/news/283314).

Помимо материально-правовых, выделяются следующие системные проблемы:

1. *Высокая латентность*. По экспертным оценкам, фиксируется не более 15% реально совершенных киберпосягательств, что указывает на недостаточность существующих механизмов выявления правонарушений и низкий уровень доверия граждан и организаций к правоохранительной системе в данной сфере (https://clck.ru/3WRbgA).

2. *Территориальная концентрация и специализация правоприменения*. Около 60% преступлений в стране приходится на Бишкек с растущей долей кибермошенничества, что свидетельствует о неравномерности ресурсного и кадрового обеспечения профильных подразделений в регионах (https://clck.ru/3WRbcT).

3. *Отсутствие единого координационного механизма* между органом, ответственным за реагирование на киберинциденты (Координационный центр по обеспечению кибербезопасности), органом защиты персональных данных (созданным в рамках Цифрового кодекса) и следственными органами, что затрудняет сквозное расследование дел, где

Тип лицензии CC: Attribution 4.0 International (CC BY 4.0)

посягательство одновременно затрагивает информационную инфраструктуру и персональные данные граждан.

4. *Международно-правовая гармонизация*. Действующее законодательство КР пока не в полной мере учитывает трансграничный характер киберугроз и рекомендации международных механизмов (например, показателей Глобального индекса кибербезопасности МСЭ, включающего правовую составляющую как один из пяти базовых компонентов оценки национальной кибербезопасности) [8-10].

Исходя из выявленных пробелов, представляется целесообразным провести системную (а не точечную) кодификацию составов, связанных с информационными правонарушениями, в рамках единой главы УК КР и соответствующего раздела Кодекса о правонарушениях, включая перенос смежных составов (в частности, ст. 209-1 УК КР) в профильную главу либо установление четкой перекрестной системы ссылок, также дифференцировать административную и уголовную ответственность по формализованным критериям размера ущерба и общественной опасности, устранив пробелы в разграничении смежных составов Кодекса о правонарушениях и УК КР. Очень важными задачами являются синхронизирование сроков и предметного содержания актов, регулирующих кибербезопасность (Закон №121), персональных данных (Цифровой кодекс) и ответственности (УК КР, Кодекс о правонарушениях), закрепив единый понятийный аппарат, также усиление процессуального и институционального обеспечения — цифровой криминалистики, трансграничное взаимодействие, специализацию следователей и судей, поскольку, как отмечают сами правоприменители, проблема состоит не только в материальных нормах, но и в их практическом применении (https://clck.ru/3WRbkL).

Необходимо учитывать международный опыт и рекомендации профильных международных организаций при дальнейшем реформировании законодательства КР в данной сфере. Таким образом, реформа 2021–2025 годов (новый УК КР, Кодекс о правонарушениях, Закон «О кибербезопасности», Цифровой кодекс) существенно обновила правовую базу ответственности за правонарушения в информационной сфере Кыргызской Республики, однако не устранила ее ключевой недостаток — фрагментарность и запаздывающий, реактивный характер законодательных изменений по отношению к динамике киберугроз. Официальная статистика роста числа зарегистрированных киберпреступлений, крупный неверифицированный ущерб и низкая раскрываемость подтверждает, что нормотворческая работа должна перейти от точечных поправок к системной, пакетной модернизации уголовного, административного и цифрового законодательства КР с одновременным укреплением институционального и процессуального обеспечения правоприменения.

Список литературы:

1. Закон Кыргызской Республики от 17 июля 2024 года №121 «О кибербезопасности Кыргызской Республики”. https://clck.ru/3WRbdj

2. Закон Кыргызской Республики от 18 июля 2025 года №151 «О внесении изменения в Уголовный кодекс Кыргызской Республики». https://clck.ru/3WRbeG

3. Закон Кыргызской Республики от 27 января 2025 года №30 «О внесении изменений в Кодекс Кыргызской Республики о правонарушениях». https://clck.ru/3WRbez

4. Закон Кыргызской Республики от 28 октября 2021 года № 126 «О порядке введения в действие Уголовного кодекса Кыргызской Республики». https://clck.ru/3WRbfZ

5. Иринин К. В. Эффективность назначения наказания в виде штрафа несовершеннолетним // Инновации. Наука. Образование. 2021. №45. С. 1283.

6. Кодекс Кыргызской Республики о правонарушениях от 28 октября 2021 года №128 (с изменениями и дополнениями) https://clck.ru/3WRbiB

Тип лицензии CC: Attribution 4.0 International (CC BY 4.0)

7. Уголовный кодекс Кыргызской Республики от 28 октября 2021 года № 127 (с изменениями и дополнениями по состоянию на 19.03.2026 г.).

8. Цифровой кодекс Кыргызской Республики от 31 июля 2025 года №178. https://cbd.minjust.gov.kg/3-48/edition/35412/ru

9. International Telecommunication Union (ITU). Global Cybersecurity Index 2024. Geneva: ITU, 2024.

10. International Telecommunication Union (ITU). UN cybersecurity report assesses global progress and highlights areas for improvement. Geneva: ITU, 2024.

References:

1. Zakon Kyrgyzskoj Respubliki ot 17 iyulya 2024 goda №121 «O kiberbezopasnosti Kyrgyzskoj Respubliki”. https://clck.ru/3WRbdj

2. Zakon Kyrgyzskoj Respubliki ot 18 iyulya 2025 goda №151 «O vnesenii izmeneniya v Ugolovnyj kodeks Kyrgyzskoj Respubliki». https://clck.ru/3WRbeG

3. Zakon Kyrgyzskoj Respubliki ot 27 yanvarya 2025 goda №30 «O vnesenii izmenenij v Kodeks Kyrgyzskoj Respubliki o pravonarusheniyakh». https://clck.ru/3WRbez

4. Zakon Kyrgyzskoj Respubliki ot 28 oktyabrya 2021 goda № 126 «O poryadke vvedeniya v dejstvie Ugolovnogo kodeksa Kyrgyzskoj Respubliki». https://clck.ru/3WRbfZ

5. Irinin, K. V. (2021). Effektivnost′ naznacheniya nakazaniya v vide shtrafa nesovershennoletnim. *Innovatsii. Nauka. Obrazovanie,* (45), 1283. (in Russian).

6. Kodeks Kyrgyzskoj Respubliki o pravonarusheniyakh ot 28 oktyabrya 2021 goda №128 (s izmeneniyami i dopolneniyami) https://clck.ru/3WRbiB

7. Ugolovnyj kodeks Kyrgyzskoj Respubliki ot 28 oktyabrya 2021 goda № 127 (s izmeneniyami i dopolneniyami po sostoyaniyu na 19.03.2026 g.).

8. Tsifrovoj kodeks Kyrgyzskoj Respubliki ot 31 iyulya 2025 goda №178. https://cbd.minjust.gov.kg/3-48/edition/35412/ru

9. International Telecommunication Union (ITU). Global Cybersecurity Index 2024. Geneva: ITU, 2024.

10. International Telecommunication Union (ITU). UN cybersecurity report assesses global progress and highlights areas for improvement. Geneva: ITU, 2024.

Поступила в редакцию 09.08.2026 г.

Принята к публикации 16.08.2026 г.

Ссылка для цитирования:

Сейдакматов Н. А. Юридическая ответственность за правонарушения в информационной сфере Кыргызской Республики: пробелы уголовного и административного законодательства в условиях цифровизации // Бюллетень науки и практики. 2026. Т. 12. №10. С. 476-480. https://doi.org/10.33619/2414-2948/131/53

Cite as (APA):

Seidakmatov, N. (2026). Legal Liability for Offenses in the Information Sphere of the Kyrgyz Republic: Gaps in Criminal and Administrative Law in the Context of Digital Transformation. *Bulletin of Science and Practice, 12*(10), 476-480. (in Russian). https://doi.org/10.33619/2414-2948/131/53

Тип лицензии CC: Attribution 4.0 International (CC BY 4.0)