УДК 343.9(575.2)/10.81.00 DOI: 10.36979/1694-500X-2021-21-7-85-89

СОВРЕМЕННАЯ КРИМИНОЛОГИЯ: СОСТОЯНИЕ И ТЕНДЕНЦИИ РАЗВИТИЯ В КЫРГЫЗСКОЙ РЕСПУБЛИКЕ

Г.Б. Жунушова, Э.С. Салыжанова

Исследуется состояние современной криминологии в Кыргызской Республике, а также тенденция ее развития. Рассмотрены этапы развития криминологии и ее особенности с момента становления. Определены проблемы, связанные с кризисом в политической системе в Кыргызстане и развитием нанотехнологий с целью изучения эмпирических и компаративистских исследований личности политического преступника и такого нового явления, как киберпреступность.

Ключевые слова: киберпространство; современная криминология; киберпреступность; личность политического преступника; тенденция развития криминологии; Кыргызстан.

ЗАМАНБАП КРИМИНОЛОГИЯ: КЫРГЫЗ РЕСПУБЛИКАСЫНДАГЫ АБАЛЫ ЖАНА ӨНҮГҮҮ ТЕНДЕНЦИЯЛАРЫ

Г.Б. Жунушова, Э.С. Салыжанова

Бул макалада заманбап криминологиянын Кыргыз Республикасындагы абалы, ошондой эле анын өнүгүү тенденциясы изилдөөгө алынган. Криминологиянын өнүгүү этаптары жана анын калыптанышынан тартып өзгөчөлүктөрү каралган. Саясий кылмышкердин инсандыгын эмпирикалык жана компаративистикалык изилдөө жана киберкылмыш сыяктуу жаңы көрүнүштү изилдөө менен Кыргызстандагы саясий кризис жана нанотехнологиянын өнүгүшү менен байланышкан көйгөйлөр аныкталган.

Түйүндүү сөздөр: кибермейкиндик; заманбап криминология; киберкылмыш; саясий кылмышкердин инсандыгы; криминологиянын өнүгүү тенденциялары; Кыргызстан.

MODERN CRIMINOLOGY: TRENDS AND PERSPECTIVES OF DEVELOPMENT IN THE KYRGYZ REPUBLIC

G.B. Zhunushova, E.S. Salyzhanova

The paper studies the state of modern criminology in Kyrgyz Republic, as well as the trend of its development. The stages of criminology development and its features from the moment of its formation are studied. The problems associated with the crisis in the political system in Kyrgyzstan and the development of nanotechnology are identified in order to study empirical and comparative studies of the personality of a political criminal and a new phenomenon as cybercrime.

Keywords: cyberspace; modern criminology; cybercrime; identity of a political criminal; trend in the development of criminology; Kyrgyzstan.

Значение современной криминологии для государства и общества подвергается изменениям, которые зависит от ситуации и требуют постоянного мониторинга.

Анализируя историческую справку о тенденции развития криминологии, в Кыргызстане определяют криминологию в два этапа. На *первом этапе* бурно развивалась криминология

с конца 1980-х – начала 1990-х гг. Благодаря появлению новой политики «перестройка» – без цензурного ограничения, стали публиковаться первые результаты исследования, появился доступ к уголовной статистике. Один из первых статистических сборников был выпущен в 1990–1991 гг. под названием «Преступность и правонарушения в СССР» со статистическими данными республик бывшего СССР. Проводились первые серии фундаментальных эмпирических исследований преступности, а также компаративистские исследования зарубежных экспертов [1].

На *втором этапе* было отмечено использование накопленных знаний отечественными специалистами и экспертами. Данный этап считается кризисным для криминологии по причине того, что отсутствует финансирование и недостаточно квалифицированных кадров для проведения эмпирических криминологических исследований. Сюда же можно отнести наличие проблем доступа к данным уголовной статистики, без которого невозможны криминологический анализ и прогноз изменений преступности и ее видов. Развитие криминологии во втором этапе не прекратилось, но она отставала в своем развитии и ограничивалась только публикацией научных статей без практического анализа.

На сегодняшний день современная криминология подвергается изменениям благодаря таким особенностям, как глобализация, которая базируется на миграционных, технологических и финансовых факторах. Как отмечает Т. Селлин, «результат массовой миграции неизбежен без «конфликта культур» [2] и становления цивилизации со всеми вытекающими криминогенными последствиями» [3]. Соответственно, особенности современной криминологии повлияли на развитие национального и международного права. Если раньше отечественная криминология заостряла свое внимание на эмпирических криминогенных исследованиях и ее результатах на уровне национальной преступности, то сейчас изучаются и международные преступления.

Важной проблемой для современного мира является виртуальная реальность – киберпространство. Мир стремительно развивается в IT-технологиях, и, как следствие, криминология формирует для себя новые понятия – киберпреступность и кибердевиантность [4]. Уличная преступность сменяется новыми субъектами киберпреступности – в большинстве случаев подростками и молодежью. Проблема определяется высокой латентной и мало изученной новой сферой [5].

Понятие «киберпреступность» определяется как преступность, связанная с использованием компьютеров, информационных технологий и глобальных сетей [6].

Жертвами киберпреступности становятся не только люди, но и целые государства. Согласно статистике, сайт Internet Complaint Center (IC3), созданный для регистрации заявлений о совершенных в отношении пользователей киберпреступлений, начитывает за 2019 г. 467 361 жалобу. Основными тремя видами преступлении были зафиксированы неуплата, вымогательство и мошенничество. Мошенничество характеризуется несколькими новыми видами преступлений, такими как фишинг, вишинг, смишинг и фарминг. Отмечается, что жертвы интернет-преступлений потеряли больше денег из-за мошенничества в связи с введением деловой электронной почты, а также мошенничества с инвестициями [7].

Определяется новая тенденция связи киберпреступности с организованной преступностью с целью отмывания денег. Виртуальное пространство позволяет проводить махинации со счетами через онлайн-аукционы или банки, применяя способы скрытия движения преступных доходов и производить незаконные сделки [8].

Аналитики пришли к выводу, что проблемы, связанные с киберпреступностью можно разрешить технологическими, организационными и правовыми подходами. Это разработка защитных технологий, проведение организационных мероприятий и усовершенствование правовых механизмов, а именно: проведение мероприятий по исследованию личности киберпреступника [9].

В Кыргызстане новая редакция Уголовного кодекса КР от 2 февраля 2017 года предусматривает ответственность за преступления в области информации и информационных систем – «Преступления против информационной безопасности» [10]. Разработчики новой редакции учли тот момент, что компьютерное преступление рассматривается в узком смысле понятия

кибепреступности, оно весьма справедливо определено, как преступление, направленное против информационной безопасности.

Актуальность проблемы также нашла свое отражение в рамках Концепции цифровой трансформации «Цифровой Кыргызстана 2019–2023» [11], которая была одобрена решением Совета безопасности Кыргызской Республики от 14 декабря 2018 года № 2 [12], а также в «Стратегии кибербезопасности Кыргызской Республики на 2019–2023 годы» [13], являющаяся Приложением 1 к Постановлению Правительства Кыргызской Республики «Об утверждении Стратегии кибербезопасности Кыргызской Республики на 2019–2023 годы» от 24 июля 2019 года № 369 [14], были также определены основные проблемы и пути их решения. Отмечается, что на сегодняшний день в Кыргызской Республике отсутствуют базовые условия для обеспечеиия цифровой трансформации и развития национальной отрасли информационных технологий в целом, а именно:

1) отсутствие документа, который будет единым для ведения государственной политики в области обеспечения кибербезопасности;
2) отсутствие систем и подходов для обнаружения и предотвращения компьютерных атак;
3) нехватка информативности о компьютерной гигиене и цифровой грамотности среди государственных служащих и сотрудников правоохранительных органов.

Ожидаемые результаты от реализации Стратегии предполагают создание условий для разработки отраслевых программ, специальную правовую базу, площадку для информационно-ресурсной поддержки и взаимодействия, внедрения систем тестирования и сертификации средств защиты информации и средств криптографической защиты информации и внедрения специальных дисциплин в школах, средних и высших профессиональных образованиях Кыргызстана.

Постановлением Правительства КР «О некоторых вопросах в сфере обеспечения кибербезопасности КР» [15], «Положение о Координационном центре по обеспечению кибербезопасности ГКНБ» от 21 мая 2020 года [16] был утвержден главный уполномоченный орган в сфере обеспечения кибербезопасности, реагирования на компьютерные инциденты, а также по выявлению, предупреждению и пресечению причин и условий, способствующих подготовке и реализации компьютерных атак – Государственный комитет национальной безопасности.

Согласно практике, которая сложилась после принятия соответствующих мер со стороны правительства Кыргызстана, 19 октября 2020 г. группа злоумышленников под названием The Black Pirate взломали сайт Жогорку Кенеша. Под их контролем якобы оказались логины, пароли, личные данные, номера телефонов, почта, пароли нескольких государственных сайтов, а также база данных граждан Кыргызстана. Группа The Black Pirate требовала 10 тысяч долларов, чтобы данные не утекли к «Даркнет» [17]. По данным пресс-службы Жогорку Кенеша, во время беспорядков 5–6 октября 2020 г. были украдены компьютеры одного или нескольких сотрудников аппарата парламента, в которых были сохранены пароли для администрирования сайта [18]. Отсюда можно сделать вывод, что после митингов и захвата Белого дома сайт Жогорку Кенеша был недоступен, а база данных законопроектов была уничтожена. Спустя определенное время, сайт парламента был восстановлен, над обеспечением безопасности сайта работали технические специалисты [19]. Вопрос касательно уголовной ответственности группы «The Black Pirate» до сих пор не решен по причине того, что не найдены лица, которые совершили преступление и поставили под угрозу всю информационную безопасность государства, в частности базы данных граждан и законопроектов.

Обеспокоенность хакерскими проделками в Кыргызстане эксперты высказывали с 2012 г. По мнению ведущего специалиста Центра электронного менеджмента знаний КРСУ И. Подольских, «меры безопасности принимаются постфактум – когда злонамеренное вторжение уже произошло. Эксперты по безопасности сходятся во мнении: меры, принятые до соединения внутренней сети с открытой, например, Интернетом, пресекают большинство попыток вторжения».

Можно прийти к выводу, что все предпринятые действия со стороны правительства Кыргызстана не оправдывают своих действий и ставят под сомнение возможность в дальнейшем реагировать на хакерские атаки.

Также в Кыргызстане имеется тенденция политического кризиса, связанная с неоднократными задержаниями государственных и муниципальных служащих [20]. Отечественная и зарубежная криминология достаточно изучила личность преступника, но такие категории, как личность политического преступника и ее различные виды и типы описаны и объяснены недостаточно. П.А. Кабанов выделил «характеристики, которые позволяют выявить ближайшие к преступлению и преступности причинные связи, причинные комплексы и цепочки», и сформировал мотивацию личности политического преступника как «центр внутренней структуры личности, интернирующий ее активность» [21], а именно, как криминальную политическую активность. Проблема исследования личности преступника рассматривается в соотношении с общеуголовными преступниками, к такому выводу пришел немецкий криминолог Мерген, который определил четыре характерных признака, отличая политического преступника от общеуголовного преступника. Следует отметить, что не всегда характерные черты Мергена можно определить у политического преступника, у некоторых они проявляются частично, у некоторых не проявляются вообще [22–23].

Процесс становления политических преступников – это тонкая грань между преступником общеуголовным и политическим. Возможен переход от общеуголовных к политическим, и наоборот. Превращение общеуголовных преступников в политических может происходить по разным объективным и субъективным причинам. В большинстве случаев, общеуголовный преступник строит преступную карьеру, накапливая свой капитал, затем легитимно или нелегитимно проникает в политическую сферу. Целью определяется получение дополнительных полномочий либо доступ к ресурсам для удовлетворения личных и корпоративных интересов. П.А. Кабанов справедливо отметил, что «в этих случаях практически невозможно найти узкую грань между политическими и корыстными интересами». Порой сами преступники не замечают, какая цель была на самом деле определена, не могут увидеть и различать деяния, совершенные ими с применением реформированных средств и методов, порицаемые уголовным законодательством [21, с. 42–43].

Отечественная криминология проводит исследования, и эмпирические исследования проводятся не в полной мере из-за ограниченного доступа к статистическим данным. Надо признать, что личность политического преступника – очень сложный субъект для криминологического анализа и требует тщательного изучения в политико-криминологических исследованиях в области антропологии по причине особенностей, определяемых в Кыргызстане.

Состояние и тенденция развития криминологии на сегодня в Кыргызстане повторяют ошибки второго этапа, пытаются определить рамки новой сферы криминологии, но изучив ее недостаточно. Мнение С.М. Иншакова правильно описывает нашу ситуацию: «Состояние и тенденция развития криминологии верна, объективна, но слишком пессимистична» [24].

Литература

1. *Квашис В.Е.* Смертная казнь: Мировые тенденции, проблемы и перспективы / В.Е. Квашис. М.: Юрайт, 2008. С. 256.
2. *Кудрявцев В.Н.* Преступность и нравы переходного периода / В.Н. Кудрявцев. М.: Гардарики, 2002. С. 186.
3. *Селлин Т.* Конфликт норм поведения / Т. Селлин // Социология преступности. М.: Прогресс, 1966. С. 282–287.
4. *Кудрявцев В.Н.* Стратегии борьбы с преступностью / В.Н. Кудрявцев. М.: Юристъ, 2003. С. 156.
5. *Гилинский Я.* Криминология: теория, история, эмпирическая база, социальный контроль / Я. Гилинский. 3-е изд. СПб.: Алеф-Пресс, 2014. С. 69–72.
6. Cambridge Advanced Learner's Dictionary. URL: http: //dictionary.cambridge.org (дата обращения: 14.12.2020).
7. FBI Releases the Internet Crime Complaint Center 2019 Internet Crime Report // February 11, 2020. URL: https://www.fbi.gov/news/pressrel/press-releases/

fbi-releases-the-internet-crime-complaint-center-2019-internet-crime-report (дата обращения: 15.12.2020).
8. BSI, Die Lage der IT-Sicherheit in Deutschland 2011, S. 4, Tropina, T. Cybercrime and Organized Crime, Freedom from Fear Magazine. 2010. Issue 3. URL:https://www.bsifuerbuerger.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2011.pdf?__blob=publicationFile (дата обращения: 15.12.2020).
9. *Номоков В.А.* Киберпреступность как новая криминальная угроза. 2012 / В.А. Номоков, Т.Л. Тропина. URL: file:///C:/Users/User/Downloads/kiberprestupnost-kak-novaya-kriminalnaya-ugroza.pdf (дата обращения: 15.12.2020).
10. Уголовный кодекс Кыргызской Республики от 2 февраля 2017 года № 19. URL: http://cbd.minjust.gov.kg/act/view/ru-ru/111527 (дата обращения: 25.12.2020).
11. «Дорожная карта» по реализации Концепции цифровой трансформации «Цифровой Кыргызстан 2019–2023» от 5 октября 2020 года № 347-р. URL: http://cbd.minjust.gov.kg/act/view/ru-ru/216896 (дата обращения: 26.12.2020).
12. Решение Совета безопасности Кыргызской Республики «О мерах по цифровому развитию Кыргызской Республики» от 14 декабря 2018 года № 2. URL:http://www.president.kg/ru/sobytiya/13077_prezident_sooronbay_gheenbekov_podpisal_reshenie_soveta_bezopasnosti_omerah_pocifrovomu_razvitiyu_kirgizskoy_respubliki (дата обращения: 26.12.2020).
13. Стратегия кибербезопасности Кыргызской Республики на 2019–2023 годы от 24 июля 2019 года № 369. URL: http://cbd.minjust.gov.kg/act/view/ru-ru/15479 (дата обращения: 26.12.2020).
14. Приложение 1. Постановления Кыргызской Республики «Об утверждении Стратегии кибербезопасности Кыргызской Республики на 2019–2023 годы» от 24 июля 2019 года № 369. URL: http://cbd.minjust.gov.kg/act/view/ru-ru/15478?cl=ru-ru (дата обращения: 26.12.2020).
15. Постановление Правительства КР «О некоторых вопросах в сфере обеспечения кибербезопасности КР» от 21 мая 2020 года № 266. URL: https://www.gov.kg/ru/npa/s/2498 (дата обращения: 26.12.2020).
16. Положение о Координационном центре по обеспечению кибербезопасности ГКНБ от 21 мая 2020 года // Информационно-правовой портал «Токтом».
17. Сайт Жогорку Кенеша взломали хакеры. Что они требуют. URL: https://ru.sputnik.kg/incidents/20201019/1050120170/kyrgyzstan-zhk-khaker-vzlom-sayt.html (дата обращения: 27.12.2020).
18. Неизвестные взломали сайт парламента и потребовали выкуп 10 тысяч долларов. В Жогорку Кенеше назвали это «хакерской атакой». URL: https://kloop.kg/blog/2020/10/19/neizvestnye-vzlomali-sajt-parlamenta-i-potrebovali-vykup-v-10-tysyach-dollarov-v-zhogorku-keneshe-nazvali-eto-hakerskoj-atakoj/ (дата обращения: 27.12.2020).
19. Сайт Жогорку Кенеша восстановлен. Неизвестные взломали компьютер с паролями. URL:https://24.kg/obschestvo/169878_sayt_jogorku_kenesha_vosstanovlen_neizvestnyie_vzlomali_kompyuter_sparolyami/ (дата обращения: 27.12.2020).
20. *Губкин И.О.* О статусе политзаключенного. URL: http://politzek.narod.ru/pisma/gubkin.htm (дата обращения: 27.12.2020).
21. *Кабанов П.А.* Личность политического преступника: понятие и соотношение со смежными категориями / П.А. Кабанов // Следователь. 2005. № 10.
22. *Лунеев В.В.* Мотивация преступного поведения / В.В. Лунеев. М., 1991. С. 107.
23. *Салахова А.И.* Понятие и криминологическая характеристика личности политического преступника / А.И. Салахова // Актуальные вопросы экономики и права в современной России: сб. науч. трудов. Нижнекамск, 1999. Вып. 3. С. 80–81.
24. *Иншаков С.М.* Криминология: учебник. М., 2000. 432 с.