Рецензия на монографию
УДК 340
https://doi.org/10.36511/2078-5356-2022-3-176-181

Рецензия на монографию В. Ф. Джафарли «Криминология кибербезопасности: в 5-ти томах» (М.: Проспект, 2021. 1 400 с.)

Коваленко Мария Андреевна[1], Милюков Сергей Федорович[2]
[1, 2]Российский государственный педагогический университет имени А. И. Герцена, Санкт-Петербург, Россия, dikoepolesf@gmail.com

Аннотация. В рецензии приведен взгляд авторов на монографическую серию В. Ф. Джафарли «Криминология кибербезопасности». Проанализированы исследованные в монографии аспекты формирования и развития системы криминологической кибербезопасности с точки зрения уголовно-правового, криминологического и междисциплинарного правовых ресурсов. Рассмотрены дискуссионные вопросы, связанные с проблемами внедрения информационно-коммуникационных технологий в сферу противодействия киберпреступности и определения границ цифрового вмешательства.
Ключевые слова: криминологическая обоснованность, кибербезопасность, цифровизация, уголовное законодательство, компьютерная преступность, искусственный интеллект
Для цитирования: Коваленко М. А., Милюков С. Ф. Рецензия на монографию В. Ф. Джафарли «Криминология кибербезопасности: в 5-ти томах» (М.: Проспект, 2021. 1 400 с.) // Юридическая наука и практика: Вестник Нижегородской академии МВД России. 2022. № 3 (59). С. 176—181. https://doi.org/10.36511/2078-5356-2022-3-176-181.

Monograph review

Review of the monograph V. F. Jafarli “Criminology of cybersecurity: in 5 volumes” (Moscow: Prospect Publ., 2021. 1400 p.)

Maria A. Kovalenko[1], Sergey F. Milyukov[2]
[1,2]Herzen State Pedagogical University of Russia, Saint-Petersburg, Russian Federation, dikoepolesf@gmail.com

Abstract. The review presents the authors' opinion of the monographic series by V. F. Jafarli “Criminology of cybersecurity”. The aspects of the formation and development of the system of criminological cybersecurity studied in the monograph are analyzed from the point of view of criminal law, criminological and interdisciplinary legal resources. The debatable issues related to the problems of introducing information and communication technologies in the field of combating cybercrime and determining the boundaries of digital interference are discussed.
Keywords: criminological validity, cybersecurity, digitalization, criminal law, computer crime, artificial intelligence
For citation: Kovalenko M. A., Milyukov S. F. Review of the monograph V. F. Jafarli “Criminology of cybersecurity: in 5 volumes” (Moscow: Prospect Publ., 2021. 1400 p.). *Legal Science and Practice: Bulletin of the Nizhny Novgorod Academy of the Ministry of Internal Affairs of Russia*, 2022, no. 3 (59), pp. 176—181. (In Russ.). https://doi.org/10.36511/2078-5356-2022-3-176-181.

Проблема обеспечения кибербезопасности является одной из самых серьезных задач для современного общества. Информационно-коммуникационные технологии (далее — ИКТ) лежат в основе сложных систем, которые обеспечивают деятельность многих организаций, органов государственной власти в ключевых секторах экономики и уже являются

неотъемлемой частью жизни большинства людей в мире.

Стремительное развитие процессов цифровизации имеет как положительные качества, способные решить стоящие перед государством задачи, так и негативные свойства, связанные, в частности с ростом убытков от преступных посягательств в сфере ИКТ, невозможностью человека в полной мере контролировать происходящие в цифровой среде процессы. Так, по данным аналитиков RTM Group в 2021 году ущерб от преступных действий с использованием компьютерных технологий в России составил 150 млрд рублей, а в 2022 году по прогнозу может достигнуть 165 млрд рублей [1]. В связи с проведением специальной военной операции на Украине этот ущерб серьезно возрастет в связи с широким применением противником цифровых технологий, в частности в работе центров информационно-психологических операций вооруженных сил Украины.

В этой связи многие ученые обращают внимание на недостаточно активное использование научно-технических достижений для решения криминологических задач, связанных с новыми противоправными проявлениями в цифровой среде, указывают на целесообразность использования цифровых технологий в качестве средств познания в сфере действия уголовного права [2, с. 51; 3, с. 424].

В связи с изложенным подготовленная В. Ф. Джафарли пятитомная монографическая серия представляет собой научное исследование вопросов интеграции уголовно-правового, криминологического и информационно-технологического ресурсов в систему криминологической безопасности в сфере ИКТ.

В первом томе монографической серии раскрываются общие теоретико-правовые и технологические основы идеи криминологической безопасности в сфере ИКТ. Далее второй, третий и четвертый тома монографии посвящены авторскому анализу аспектов уголовно-правового, криминологического и междисциплинарного правового ресурсов в формировании и развитии системы криминологической кибербезопасности. Пятый том монографической серии представляет собой подведение автором итогов исследования и обсуждение перспектив дальнейшего развития.

В качестве обоснования теории криминологической безопасности и производной от нее криминологической кибербезопасности автор приводит базовую теорию криминологической безопасности В. А. Плешакова, а также различные точки зрения на отдельные аспекты обеспечения криминологической безопасности О. А. Белькова, С. Я. Лебедева, Н. Ф. Кузнецовой, Д. А. Шестакова, И. М. Мацкевича, М. М. Бабаева, Е. Н. Рахмановой, А. А. Лапина.

Итогом проведенного анализа является выделение автором теории криминологической кибербезопасности как научной категории, объединяющей современные криминологические идеи и теоретико-прикладные концепции обеспечения защиты личности, общества и государства от преступности в сфере ИКТ.

Следует согласиться с мнением автора, что для создания эффективной системы криминологической кибербезопасности необходим комплекс инструментов, обеспечивающих разноплановый, междисциплинарный подход к познанию феномена общественной опасности. Характер цифровой реальности влияет на специфику преступного поведения и требует разработки междисциплинарного инструментария для адекватной оценки этой криминальной сферы и разработки соответствующих мер профилактики. Характер современного научного познания отличается получением нового результата путем синтеза и взаимодействия нескольких дисциплин, связи науки, общества и производства на основе современных средств коммуникации, достижений информатики, математики и других наук [4, с. 153]. Особенно актуальным является развитие междисциплинарных связей наук и технологий, в котором осуществляется взаимодействие НБИКС-технологий, основанное на объединении и взаимном усилении достижений нано-, био-, информационных и когнитивных технологий.

В этой связи представляется исключительно актуальным рассмотрение автором монографии вопроса о дискурсивном характере интернет-пространства (т. 1, с. 143), необходимости изучения сознания человека, процессов восприятия и интерпретации авторами и адресатами информации, поскольку объектом преступного воздействия в цифровой среде, помимо аппаратной инфраструктуры, также являются сознание, мысли, чувства, внутренний мир человека. Требуется проведение отдельных криминологических исследований для анализа преступлений, совершаемых под влиянием компьютерных игр, общения в социальных сетях, кибертравли, в результате формирования интернет-зависимости, «цифровой деменции» (психоневрологического расстройства со снижением когнитивных способностей и творческого потенциала личности).

Особенно уязвимой категорией перед подобного рода воздействием в киберпространстве являются несовершеннолетние, следствием чего является постоянный рост специфических угроз в интернет-пространстве в отношении несовершеннолетних (кибersталкинг [5], пропаганда суицидов, призывы к ненависти, распространение фэйковой информации, сексуальное развращение, вовлечение в преступную и иную представляющую опасность деятельность) [6; 7]. При этом до сих пор остаются нерешенными вопросы, связанные с полноценным прогнозированием направлений использования кибертехнологий, которые могут стать инструментом противоправной преступной деятельности.

Выходом из сложившейся ситуации автор рассматриваемой монографии считает достижение социальной справедливости путем выключения субъективного начала, максимального задействования объективного, непредвзятого подхода к юридическим фактам, способствующим формированию системы, «создающей ощущение страха, способной реализовать социально важнейшие принципы справедливости и неотвратимости наказания» (т. 2, с. 6). В целом можно согласиться с мнением автора о нежелательности субъективного, предвзятого подхода к юридическим фактам, однако, на наш взгляд, полностью нивелировать воздействие субъективного начала со стороны правоприменителя априори невозможно.

Следует согласиться с мнением автора, что российское уголовное законодательство страдает бессистемностью, наличием большого количества несоответствий, логических ошибок, тавтологий, норм-клонов и нечетких понятий, требует качественного усовершенствования и преобразования. Однако вызывает долю скепсиса предлагаемый автором способ оптимизации уголовного законодательства путем его цифрового анализа с помощью искусственного интеллекта (т. 2, с. 107). Подобная позиция отчасти облегчает работу законодателя, но в то же время и усложняет поиск ответственного за качество полученного таким образом уголовного закона. Кроме того, следует отметить, что создание технической возможности для реализации подобной оптимизации уголовного законодательства ограничена человеческим ресурсом и его способностью обучить искусственный интеллект в соответствии с поставленными целями, поэтому в таком случае исключить субъективный подход будет крайне сложно, а также определить насколько положительным будет эффект от подобного рода изменений.

Несмотря на развитие цифровых технологий, современное общество не стало лучше, напротив, негативных аспектов в развитии стало еще больше. Сегодня все уже так хорошо понимают обратную сторону инноваций, что нам сложно поверить в то, что оцифровка уголовного закона с помощью искусственного интеллекта приведет к его более эффективному применению. Роль ИКТ в данном процессе слишком преувеличена. Упование на могущество информационных технологий разрушает готовность должностных лиц нести ответственность за принятие решений. Современная проблема неадекватности уголовно-правового механизма противодействия преступности, на наш взгляд, связана по большей части не с отсутствием возможности создать эффективную систему уголовного законодательства, а в нежелании законодателя применять накопленные отечественной и зарубежной криминологией знания о подлинных процессах внутри преступного множества [8, с. 437; 9].

Отдельного внимания требует затронутый в монографии дискуссионный вопрос о возможности допущения искусственного интеллекта к принятию юридически значимых решений, в частности в рамках осуществления правосудия («электронные весы правосудия», концепция Х. Д. Аликперова [10]), в рамках правоохранительных мероприятий, например, для патрулирования участков местности с возможностью преследовать правонарушителя, для создания цифровой программы-фильтра, позволяющей обнаруживать факты преступлений, производить их оценку и подвергать уголовно-правовой регистрации.

Представляется весьма утопичным взгляд автора на развитие современных цифровых технологий, согласно которому будет достигнут такой уровень «взаимодействия человека и машины, оснащенной искусственным интеллектом, при котором не останется сомнений в справедливости процессуальных решений». Здесь мы разделяем позицию В. В. Хилюты [11, с. 126], который обращает внимание на то, что уже на стадии алгоритмизации процесса квалификации преступлений справедливо встает вопрос, какие правила требуется взять за основу? Уголовное право не сводится к набору строгих математических правил и формул, и справедливое решение — это не всегда бесспорное с математической точки зрения решение. Каждое преступление уникально по своей природе, и компьютер вряд ли способен без учета жизненного опыта человека оценить характер и степень общественной опасности деяния, которое

Legal Science and Practice: Journal of Nizhny Novgorod Academy of the Ministry of Internal Affairs of Russia, 2022, no. 3 (59)

является отражением его социальной сущности. Кроме того, внедрение цифровых технологий в правоприменительную деятельность всегда связано со злоупотреблениями со стороны субъектов, занимающихся криминализацией общественно опасных деяний и непосредственно контролирующих проявления отклоняющегося поведения. Поэтому «электронные весы правосудия» не могут быть беспристрастными, поскольку электронный ключ к этим весам всегда будет находиться в руках тщательно отобранной группы людей, а главный ключник (или ключница) расположится на верхних этажах власти [12]. Как справедливо отмечает профессор Д. А. Шестаков, любые современные цифровые технологии могут быть приспособлены глобальной олигархической властью для достижения ею своих экономических целей и всегда несут в себе риск необходимости отражения хакерских атак, возникновения технологических сбоев в работе, дистанционного отключения и несанкционированного доступа к ним [13].

В связи с чем возникает вопрос об эффективности и целесообразности подобных действий, которые неминуемо усиливают контроль над человеком и влекут ограничение его прав. На наш взгляд, внедрение ИКТ в процесс правоприменения должно ограничиваться организационной сферой с целью оптимизации делопроизводства, повышения доступности и открытости принимаемых процессуальных решений. При этом ни одна компьютерная программа не сможет заменить живого человеческого общения, которое необходимо при принятии юридически значимых решений в уголовном процессе, связанных с судьбой человека. Однако использование искусственного интеллекта в качестве помощника судьи вполне вероятно.

Еще один вызывающий дискуссию вопрос, поднимаемый автором монографической серии, связан с пределами использования современных научно-технических достижений в системе исполнения наказаний. В частности речь идет об использовании технологий чипирования, а также наделения определенных представителей сетевого сообщества презумпцией виновности. Полагаем, что такие предложения автора являются не приемлемыми. Категории «опасное состояние личности», «лицо, представляющее опасность» противоречат базовому принципу уголовного права — принципу виновности. Использование для дистанционного контроля за преступностью чипов, интегрируемых в живой организм, также вызывает недоумение, поскольку нарушает базовое конституционное право гражданина на невмешательство в организм человека без его согласия.

Автор отмечает неадекватность существующих санкций сути инновационных криминальных угроз, в связи с чем предлагает внести изменения в статьи 53 и 56 УК РФ, дополнив их возможностью применения ограничения или полного отлучения от сети «Интернет». Но, как показывает ряд исследований данного подхода, в связи с повсеместным использованием средств телекоммуникационной связи и их неограниченностью в обороте, такие меры не дают положительного эффекта. В частности, такой эксперимент был проведен десять лет назад в США и не привел к положительному результату. Современные технологии стремительно развиваются, но при этом нужно всегда внимательно задумываться о последствиях их применения для контроля над преступностью.

Весьма полезным видится предлагаемое В. Ф. Джафарли использование технологий обработки больших данных и искусственного интеллекта для сбора криминологической информации о состоянии киберпреступности. Данное предложение не является новым и уже активно используется в современной криминологии. Так, с помощью методов математического моделирования и прогнозирования стало доступно использование для познания преступности цифрового профилирования преступного поведения, с помощью которого сейчас стало возможным соотнесение конкретного цифрового устройства с определенным пользователем. Развитие нейробиологии расширило возможности применения методов восстановления сознания человека.

Однако возможности ИКТ используются в криминологии недостаточно, по-прежнему остается актуальным вопрос о том, как правильно применять к существующей теоретической базе новые цифровые методы и инструменты. Кроме того, достижения науки сопряжены с нравственными проблемами и криминальными рисками, которые также необходимо оценивать.

Следует согласиться с мнением автора монографии, что законодателем недооценивается значимость такого феномена, как криминологическая информация. Представляется актуальным исследование автором монографии перспектив формирования информационных ресурсов для сбора криминологической информации, цифрового оформления информации по уголовным делам, создания в отношении лиц с антиобщественным поведением цифровой диагностической карты. Создание

подобных ресурсов позволило бы значительно обогатить данные для научных исследований и выработки практических рекомендаций, а также значительно повысило бы качество работы правоохранительных органов. Выяснение с помощью компьютерного анализа тенденций, куда направляются криминальные усилия злоумышленников, позволили бы с опережением реагировать на подготавливаемые преступные деяния. ИКТ обладают значительным потенциалом для их использования в деле предупреждения преступности, реализация которого во многом зависит от готовности органов власти сотрудничать с ведущими научными центрами и специалистами, занимающимися разработкой соответствующих ИКТ и возможностями их внедрения в работу органов правопорядка.

Подводя итог, можно заключить, что данная монографическая серия В. Ф. Джафарли, безусловно, заслуживает широкого внимания как со стороны практиков, так и со стороны научного сообщества, студентов и аспирантов, несмотря на возможные сложности при восприятии текста неискушенным читателем. Особенно важными являются затронутые в работе вопросы, связанные с проблемами внедрения ИКТ в сферу противодействия киберпреступности и определения границ цифрового вмешательства, которые способствуют продолжению научной дискуссии и дальнейшей научной разработке поднятых проблем.

Список источников

1. Эксперты назвали низкую цифровую грамотность россиян причиной роста киберпреступности. URL: https://www.forbes.ru/tekhnologii/455881-eksperty-sprognozirovali-rost-userba-ot-kiberprestupnosti-v-rossii-do-165-mlrd-rublej (дата обращения: 20.07.2022).

2. Победкин А. В. Этико-аксиологические риски моды на цифровизацию для уголовного судопроизводства (об ошибочности технологичного подхода к уголовному процессу) // Вестник Московского университета МВД России. 2020. № 3.

3. Серебренникова А. В. Криминологические проблемы цифрового мира (цифровая криминология) // Всероссийский криминологический журнал. 2020. № 3.

4. Судакова Т. М. Междисциплинарность криминологии в контексте методологической и структурной трансформации науки // Всероссийский криминологический журнал. 2022. № 2.

5. Филатова М. А. Уголовная ответственность за кибersталкинг // Уголовное право. 2020. № 4. С. 77—83.

6. Коваленко М. А. Криминологическая характеристика информационного воздействия на несовершеннолетних в сети «Интернет» // В сборнике: Киберпреступность: риски и угрозы: материалы Всероссийского студенческого круглого научно-практического стола с международным участием / под ред. д. ю. н., доцента Е. Н. Рахмановой. СПб: Астерион, 2021. С. 176—181.

7. Коваленко М. А. Преступления в отношении несовершеннолетних с использованием информационного воздействия // Уголовное-законодательство: вчера, сегодня, завтра: материалы ежегодной Всероссийской научно-практической конференции. Санкт-Петербург, 18—19 мая 2021 года. Ч. 2. СПб: СПбУ МВД России, 2021. С. 165—169.

8. Милюков С. Ф. Кризис уголовно-правовой политики. Диагноз: острая криминологическая недостаточность // Обеспечение национальной безопасности — приоритетное направление уголовно-правовой, криминологической и уголовно-исполнительной политики: материалы XI Российского Конгресса уголовного права, посвященного памяти доктора юридических наук, профессора В. С. Комиссарова, состоявшегося 31 мая — 1 июня 2018 года. М.: Юрлитинформ, 2018.

9. Милюков С. Ф. О проектах нового Уголовного кодекса России // Уголовное право: стратегия развития в XXI веке: материалы XVII Международной научно-практической конференции, Москва, 23—24 января 2020 года / Московский государственный юридический университет им. О. Е. Кутафина. М., 2020. С. 45—49.

10. Аликперов Х. Д. Электронная система определения оптимальной меры наказания (постановка проблемы) // Криминология: вчера, сегодня, завтра. 2018. № 4 (51). С. 13—22.

11. Хилюта В. В. Цифровое переформатирование уголовного права // Вестник Московского университета МВД России. 2021. № 1.

12. Милюков С. Ф. Будут ли беспристрастны электронные весы правосудия? URL: https://www.criminology-club.ru/home/the-last-sessions/356-2019-02-26-20-10-22 (дата обращения: 20.07.2022).

13. Шестаков Д. А. Планетарная олигархическая преступная деятельность // Криминология: вчера, сегодня, завтра. 2012. № 2 (25). С. 12—22.

References

1. Experts called the low digital literacy of Russians the reason for the growth of cybercrime. URL: https://www.forbes.ru/tekhnologii/455881-eksperty-sprognozirovali-rost-userba-ot-kiberprestupnosti-v-rossii-do-165-mlrd-rublej (accessed 20.07.2022). (In Russ.)

2. Pobedkin A. V. Ethical and axiological risks of the fashion for digitalization for criminal proceedings (on the fallacy of the technological approach to the criminal process). *Bulletin of the Moscow University of the Ministry of Internal Affairs of Russia*, 2020, no. 3. (In Russ.)

3. Serebrennikova A. V. Criminological problems of the digital world (digital criminology). *All-Russian criminological journal*, 2020, no. 3. (In Russ.)

4. Sudakova T. M. Interdisciplinarity of criminology in the context of the methodological and structural trans-

formation of science. *All-Russian journal of criminology*, 2022, no. 2. (In Russ.)

5. Filatova M. A. Criminal liability for cyberstalking. *Criminal law*, 2020, no. 4, pp. 77—83. (In Russ.)

6. Kovalenko M. A. Criminological characteristics of information impact on minors on the Internet. In the collection: Cybercrime: risks and threats: materials of the All-Russian student round scientific and practical table with international participation / ed. by Associate Professor E. N. Rakhmanova. St. Petersburg: Asterion Publ., 2021. Pp. 176—181. (In Russ.)

7. Kovalenko M. A. Crimes against minors using information impact. Criminal legislation: yesterday, today, tomorrow: materials of the annual All-Russian scientific and practical conference. St. Petersburg, May 18—19, 2021. Part 2. St. Petersburg: SPbU of the Ministry of Internal Affairs of Russia, 2021. Pp. 165—169. (In Russ.)

8. Milyukov S. F. Crisis of criminal law policy. Diagnosis: acute criminological insufficiency. Ensuring national security is a priority area of criminal law, criminological and penitentiary policy: materials of the XI Russian Congress of Criminal Law, dedicated to the memory of Doctor of Law, Professor V. S. Komissarov, held on May 31 — June 1, 2018 . Moscow: Yurlitinform Publ., 2018. (In Russ.)

9. Milyukov S. F. On the drafts of the new Criminal Code of Russia. Criminal law: development strategy in the XXI century: materials of the XVII International scientific and practical conference, Moscow, January 23—24, 2020. Moscow State Law University. O. E. Kutafina. Moscow, 2020. Pp. 45—49. (In Russ.)

10. Alikperov Kh. D. Electronic system for determining the optimal measure of punishment (problem statement). *Criminology: yesterday, today, tomorrow*, 2018, no. 4 (51), pp. 13—22. (In Russ.)

11. Hilyuta V. V. Digital reformatting of criminal law. *Bulletin of the Moscow University of the Ministry of Internal Affairs of Russia*, 2021, no. 1. (In Russ.)

12. Milyukov S. F. Will the electronic scales of justice be impartial? URL: https://www.criminologyclub.ru/home/the-last-sessions/356-2019-02-26-20-10-22 (accessed 20.07.2022). (In Russ.)

13. Shestakov D. A. Planetary oligarchic criminal activity. *Criminology: yesterday, today, tomorrow*, 2012, no. 2 (25), pp. 12—22. (In Russ.)

Информация об авторах

М. А. Коваленко — без ученой степени;
С. Ф. Милюков — доктор юридических наук, профессор.

Information about the authors

M. A. Kovalenko — no academic degree;
S. F. Milyukov — Doctor of Law, Professor.

Рецензия поступила в редакцию 01.08.2022; принята к публикации 30.08.2022.

The review was submitted 01.08.2022; accepted for publication 30.08.202