Научная статья
https://doi.org/10.24412/2220-2404-2025-7-20
УДК 343.2/.7

ПЕРСПЕКТИВЫ ОБЕСПЕЧЕНИЯ КРИМИНОЛОГИЧЕСКОЙ БЕЗОПАСНОСТИ ЦИФРОВОГО ПРЕДПРИНИМАТЕЛЬСТВА

Финкель М.В.
Дубинин, Финкель и партнеры

Аннотация. *Цель. В настоящей статье произведен анализ аспектов обеспечения криминологической безопасности сферы предпринимательской деятельности в эпоху Шестого технологического уклада экономики. Обозначены проблемы, исторически неизбежно вызываемые инновациями, а также перспективные научные методы, нацеленные на защиту рассматриваемой сферы. В процессе изучения были использованы как общенаучные (анализ, синтез), так и частно-научные (уголовно-правовой, криминологический) методы познания. В ходе подготовки публикации были использованы отечественные исследования в области технологий и криминологии. Произведенный анализ позволил сделать вывод об отсутствии единого теоретического подхода к обеспечению криминологической безопасности цифрового предпринимательства. Выводы и заключения: материалы публикации могут быть использованы в целях оптимизации правоохранительной теории и практики, формирования и развития системы криминологической безопасности сферы предпринимательской деятельности.*

Ключевые слова: *Шестой технологический уклад экономики, криминологическая кибербезопасность, сфера предпринимательской деятельности, цифровая экономика, цифровое предпринимательство.*

Финансирование: *инициативная работа.*

Original article

PROSPECTS FOR ENSURING CRIMINOLOGICAL SECURITY OF DIGITAL ENTREPRENEURSHIP

Marina V. Finkel
Dubinin, Finkel and Partners

Abstract. *Objective. This article analyzes the aspects of ensuring criminological security of the business sphere in the era of the Sixth Technological Order of the Economy. The problems that are historically inevitably caused by innovations, as well as promising scientific methods aimed at protecting the sphere under consideration, are identified. In the process of studying, both general scientific (analysis, synthesis) and specific scientific (criminal law, criminological) methods of cognition were used. During the preparation of the publication, domestic research in the field of technology and criminology was used. The analysis made it possible to conclude that there is no single theoretical approach to ensuring criminological security of digital entrepreneurship. Findings and conclusions: the publication materials can be used to optimize law enforcement theory and practice, the formation and development of a criminological security system in the sphere of entrepreneurial activity.*

Keywords: *Sixth technological order of the economy, criminological cybersecurity, business sphere, digital economy, digital entrepreneurship.*

Funding: *Independent work.*

Введение.

Стремительное развитие цифровых технологий и постепенный переход мировой экономики в условия Шестого технологического уклада побуждают научное сообщество разрабатывать и предлагать для практической реализации актуальные концепции для защиты цифровой экономики, а в ее рамках цифрового предпринимательства.

Подчеркнем, что главной целью здесь является выработка единого научного подхода к обеспечению криминологической кибербезопасности рассматриваемых объектов.

Обсуждение.

Мировая экономика развивается благодаря постоянному научно-техническому прогрессу, который генерирует технологические инновации. Эти инновации, в свою очередь, повышают производительность труда, модернизируют производственные процессы и приводят к смене технологических укладов.

Теория технологических укладов, основанная на работах Н.Д. Кондратьева, становится все более значимой и определяющей в экономической науке XXI в. Согласно этой теории, развитие технологий происходит волнообразно, с циклами продолжительностью 50-70 лет, завершающимися кризисами и последующим переходом к новым, более прогрессивным технологиям.

Технологический уклад представляет собой комплексную систему, где ключевую роль играют отрасли, использующие определенный вид энергии.

История знает пять индустриальных и один постиндустриальный технологический цикл.

Первый уклад, основанный на энергии воды, возник в 1785 г. За ним последовали уклады, базиру-

ющиеся на энергии пара и угля (с 1830 г.), электричестве (1890-1940 гг.), углеводородах и двигателях внутреннего сгорания (с 1940 г.) Современный, пятый уклад (с 1990 г.) характеризуется доминированием электронной и атомной энергетики.

По мере интеграции в пятый технологический уклад и его полной реализации, глобальная экономика приближается к наступлению первого постиндустриального уклада. Теоретически, этот переход должен произойти к 2040 г., однако, учитывая динамику научно-технического развития, его наступление может быть ускорено.

Ключевым фактором, определяющим новую «волну Кондратьева», станет НБИКС-конвергенция, представляющая собой синергию нанотехнологий, биотехнологий, информационных технологий, когнитивных наук и социальных технологий [1; 2].

Очевидно, что в условиях рассматриваемых укладов активно развивается не только экономика, но и сопутствующая ей преступность. Соответственно, цифровой экономике и развивающемуся в ее рамках цифровому предпринимательству в полной мере угрожает цифровая преступность. Последняя развивается стремительно, старательно перенимая инновационные средства и способы, реализуемые в сфере законной экономической деятельности. Организованная преступность рекрутировала в свои ряды информационных технологов, весьма основательно разбирающихся в существующих системах информационной защиты субъектов предпринимательской деятельности.

Отметим, что технологические уклады экономики развиваются одновременно во множестве стран. Это обусловлено тем, что современные цифровые технологии обладают признаком трансграничности, и в этом суть мировой цифровой экономики. Соответственно, и современная организованная преступность обладает такой же особенностью, успешно действуя буквально со всех частей света.

Соответственно, возникает потребность в выработке не локального или регионального, а универсального подхода к обеспечению криминологической безопасности легальных цифровых правоотношений. Наилучшим образом, на наш взгляд, осуществить эффективную защиту сферы предпринимательской деятельности различных уровней возможно путем формирования и развития системы криминологической кибербезопасности, в качестве объектов которой выступает практически вся совокупность социальных и экономических отношений.

Теория криминологической безопасности начала формироваться в 1990-е гг., получив развитие, соответствующее эпохе цифровых технологий, в свою очередь, в рамках теории криминологической кибербезопасности. Сущность и социальное предназначение данной теории заключается в обеспечении защиты всей совокупности отношений. При этом теория криминологической кибербезопасности не замыкается лишь на противодействии преступлениям в рамках Главы 28 УК РФ «Преступления в сфере компьютерной информации», а простирается на познание различных криминальных посягательств, охваченных большинством норм Особенной части УК РФ.

Переходя к раскрытию сущности криминологической безопасности цифрового предпринимательства, подчеркнем важность раскрытия такого универсального термина, как «кибербезопасность». Существуют определения не юридического характера, которыми оперируют специалисты-технологи, согласно которым, к примеру, кибербезопасность определяется через свойство или состояние системы «сохранять надежность и функциональную устойчивость в условиях современного информационного противоборства». Либо кибербезопасность понимается, как «информационная безопасность компьютерных информационно-управляющих систем, обеспечивающая их высокую надежность и функциональную устойчивость в условиях современного информационного противоборства» [3, с. 5-6].

С точки зрения В.Ф. Джафарли, с которой мы соглашаемся, «проблемность в подобном раскрытии термина «кибербезопасность» заключается в том, что, таким образом, рассматриваемое понятие приобретает чрезмерно упрощенно-«цифровой» характер, в связи с чем, может сложиться впечатление, что под кибербезопасностью следует понимать, в основном, систему мер, направленных на защиту от угроз, нацеленных на программно-техническую инфраструктуру. Здесь нельзя упускать из виду, что компьютерная техника, выступая, прежде всего, в качестве средства коммуникации, имеет своим предназначением прием-передачу информации не только между программно-техническими устройствами, но и между людьми. То есть, объектом воздействия является, помимо аппаратной инфраструктуры, также сознание, мысли, чувства, внутренний мир человека» [4, с. 103].

Под *криминологической безопасностью цифрового предпринимательства* следует понимать состояние защищенности цифровых финансовых и нефинансовых активов от различных угроз некриминального характера, исходящих от информационно-телекоммуникационного пространства. Соответственно, *криминологическая безопасность цифрового предпринимательства* - состояние защищенности ее цифровых финансовых и нефинансовых активов от различных угроз криминального характера, исходящих от информационно-телекоммуникационного пространства.

Имеются предпосылки для создания *теории криминологической безопасности цифрового предпринимательства как научной подкатегории*, входящей в категорию «теория криминологической кибербезопасности». Данный подход обязывает нас к выделению в рамках рассматриваемой теории самостоятельных объекта и предмета познания.

Так, в качестве *объекта познания в рамках теории криминологической безопасности цифрового предпринимательства* следует понимать обществен-

ные отношения, которые складываются в процессе деятельности, направленной на обеспечение безопасности цифровых финансовых и нефинансовых активов.

Соответственно, в качестве *предмета рассматриваемой теории* подлежат изучению:

- преступность в сфере предпринимательской деятельности как явление, ее проявления как основная угроза криминологической безопасности рассматриваемой сферы от инновационных преступных посягательств, совершаемых исключительно в киберпространстве;
- личность преступника, использующего цифровые технологии или киберпространство для совершения инновационных криминальных посягательств, как субъект криминальной угрозы;
- криминогенные факторы как основной источник угроз криминологической кибербезопасности;
- процессы воздействия на инновационные криминальные угрозы, то есть их предупреждение, профилактика, предотвращение и пресечение;
- выработанные и подлежащие выработке защитные механизмы от инновационных преступных посягательств, а именно криминологическая защита цифрового предпринимательства;
- проблемы, связанные с жертвой инновационных преступлений – индивидуальным предпринимателем или коммерческой организацией, то есть виктимологическая профилактика.

Исходя из вышеизложенного, следует отметить, что *криминологическая безопасность цифрового предпринимательства как самостоятельная система* представляет собой совокупность информационно-технологических, научно-практических, правовых, организационных, кадровых, этических мер, обеспечиваемых путем задействования различных ресурсов, в числе которых уголовно-правовой, уголовно-правоприменительный, цифровой, научно-практический, коммерческий, общественный и образовательный.

Результаты.

Проведенный анализ позволил определить сущность Шестого технологического уклада экономики и теории криминологической безопасности цифрового предпринимательства. Очевидно, что правоохранительная практика в сфере защиты предпринимательской деятельности пока не может предоставить адекватного ответа цифровой преступности по причине отсутствия достаточного числа подготовленных соответствующим образом специалистов.

Заключение.

Отмеченное выше позволяет предложить меры организационного и образовательного характера, нацеленные на подготовку и переподготовку в рамках теории криминологической безопасности сферы экономической (предпринимательской) деятельности действующих и будущих сотрудников правоохранительных органов, прежде всего тех, в чьи функциональные обязанности входит предупреждение рассмотренной в статье преступности.

Конфликт интересов

Не указан.

Рецензия

Все статьи проходят рецензирование в формате double-blind peer review (рецензенту неизвестны имя и должность автора, автору неизвестны имя и должность рецензента). Рецензия может быть предоставлена заинтересованным лицам по запросу.

Conflict of Interest

None declared.

Review

All articles are reviewed in the double-blind peer review format (the reviewer does not know the name and position of the author, the author does not know the name and position of the reviewer). The review can be provided to interested persons upon request.

Список источников:

1. Каблов Е.Н. Шестой технологический уклад // Наука и жизнь. 2010. № 4.

2. Наумович О.В. Высокотехнологичный уклад как социально-экономический феномен // Журнал международного права и международных отношений. 2010. № 2.

3. Бородакий Ю.В., Добродеев А.Ю., Бутусов И.В. Кибербезопасность как основной фактор национальной и международной безопасности XXI века (часть 1) / Вопросы кибербезопасности. 2014. №1 (2). С. 5-6.

4. Джафарли В.Ф. Формирование и развитие системы криминологической безопасности в сфере информационно-коммуникационных технологий: дисс… д-ра юрид. наук. М., 2022. 540 с.

References:

1. Kablov E.N. The Sixth Technological Order // Science and Life. 2010. No. 4.

2. Naumovich O.V. High-tech order as a socio-economic phenomenon // Journal of International Law and International Relations. 2010. No. 2.

3. Borodakiy Yu.V., Dobrodeev A.Yu., Butusov I.V. Cybersecurity as the Main Factor of National and International Security of the 21st Century (Part 1) / Cybersecurity Issues. 2014. No. 1 (2). P. 5-6.

4. Dzhafarli V.F. Formation and Development of the Criminological Security System in the Sphere of Information and Communication Technologies: Diss… Doctor of Law. Moscow, 2022. 540 p.

Информация об авторе:

Финкель Марина Вячеславовна, управляющий партнер, адвокат адвокатского бюро г. Москвы «Дубинин, Финкель и партнеры», e-mail: m.finkel@lawyerspro.ru.

Marina V. Finkel, Managing partner, lawyer of the Moscow law firm «Dubinin, Finkel and Partners»

Статья поступила в редакцию / The article was submitted 30.06.2025;
Одобрена после рецензирования / Approved after reviewing 13.07.2025;
Принята к публикации / Accepted for publication 20.07.2025.
Автором окончательный вариант рукописи одобрен.