Научная статья
УДК 343.974
DOI: 10.37973/KUI.2022.25.27.010

ОБЕСПЕЧЕНИЕ КРИМИНОЛОГИЧЕСКОЙ БЕЗОПАСНОСТИ В УСЛОВИЯХ ЦИФРОВОЙ ТРАНСФОРМАЦИИ

Татьяна Валентиновна Пинкевич,
Академия управления МВД России, Москва, Россия,
pinkevich@yandex.ru

Аннотация

Введение: статья посвящена рассмотрению проблемных вопросов обеспечения криминологической безопасности в условиях цифровой трансформации и способов их решения.

Материалы и методы: материалами исследования послужили: законодательная база, составляющая правовую основу обеспечения криминологической безопасности, цифровой экономики и цифровой трансформации, а также регламентирующая деятельность по защите личности, общества и государства от преступных посягательств; данные судебной практики, статистические показатели зарегистрированных преступлений, совершаемых с использованием цифровых технологий.

В качестве методологического инструментария выступили эмпирический и лингвистический методы познания, научно-аналитический подход, а также специально-юридические методы: формально-юридический и сравнительно-правовой.

Результаты исследования: на основании результатов исследования криминальных угроз личности, обществу и государству в условиях цифровой трансформации (преступлений, совершаемых с использованием информационно-коммуникационных технологий, в том числе легализации преступных доходов, финансирования терроризма, организации незаконного распространения наркотических средств и психотропных веществ, а также использования в противоправных целях цифровых валют) мы пришли к выводу о необходимости повышения эффективности обеспечения криминологической безопасности, что требует создания таких условий, которые позволят снизить уровень криминальных угроз и повысить уровень защищенности личности, общества и государства.

Обсуждение и заключения: с учетом результатов исследования современного состояния криминальных угроз России, характеризующегося беспрецедентным ростом преступлений, совершаемых с использованием цифровых технологий или в отношении них, низкой раскрываемостью и высоким уровнем латентности, обосновывается необходимость создания условий для эффективной работы системы обеспечения криминологической безопасности в условиях цифровой трансформации с учетом использования правовой конвергенции, модернизации образовательного процесса подготовки специалистов правоохранительной системы для их плодотворной деятельности в современных условиях, взаимодействия правоохранительных органов на межведомственном, внутриведомственном уровнях и международном уровне.

© Пинкевич Т.В., 2022

Ключевые слова: цифровые технологии, преступность, обеспечение криминологической безопасности, латентность, криминальные риски, криминологическая обстановка, цифровая трансформация

Для цитирования: Пинкевич Т.В. Обеспечение криминологической безопасности в условиях цифровой трансформации // Вестник Казанского юридического института МВД России. 2022. Т. 13. № 2 (48). С. 63-68. DOI: 10.37973/KUI.2022.25.27.010

Scientific article
UDC 343.974
DOI: 10.37973/KUI.2022.25.27.010

ENSURING CRIMINOLOGICAL SECURITY IN THE CONTEXT OF DIGITAL TRANSFORMATION

Tatyana Valentinovna Pinkevich,
Management Academy of MIA of Russia, Moscow, Russia,
pinkevich@yandex.ru

Abstract

Introduction: the article is devoted to the consideration of issues of ensuring criminological security in the conditions of digital transformation and ways to overcome them.

Materials and Methods: the study materials were the legislative framework that forms the legal basis for ensuring criminological security, digital economy and digital transformation, as well as regulating activities to protect individuals, society and the state from criminal encroachments; judicial practice data, statistical indicators of registered crimes committed using digital technologies.

The methodological tools were empirical and linguistic methods of cognition, scientific and analytical approach, as well as special legal methods: formal legal and comparative legal.

Results: the study of criminal threats to the individual, society and the state in the context of digital transformation (crimes committed using information and communication technologies, including the legalization of criminal proceeds, terrorist financing, the organization of illegal distribution of narcotic drugs and psychotropic substances, as well as the use of digital currencies for illegal purposes) allowed us to come to the conclusion that improving the efficiency of ensuring criminological security, which requires the creation of such conditions, which will reduce the level of criminal threats and increase the level of protection of the individual, society and the state.

Discussion and Conclusions: taking into account the study of the current state of criminal threats in modern Russia, the unprecedented growth of crimes committed using or in relation to digital technologies, low detection and high latency, the need to create conditions for the effective operation of the criminological security system in the context of digital transformation in digital technologies, taking into account the use of legal convergence is justified, modernization of the educational process for training specialists for the Russian law enforcement system, interaction of law enforcement agencies at the interdepartmental, intradepartmental and international levels.

© Pinkevich T.V., 2022

Keywords: digital technologies, crime, criminological security, latency, criminal risks, criminological situation, digital transformation

For citation: Pinkevich T.V. Ensuring Criminological Security in the Context of Digital Transformation // Bulletin of the Kazan Law Institute of MIA of Russia. 2022. Vol. 13, No. 2 (48). Pp. 63-68. DOI: 10.37973/KUI.2022.25.27.010

Введение

Стратегией национальной безопасности Российской Федерации определены задачи обеспечения криминологической безопасности, одной из которых является «предупреждение и пресечение правонарушений и преступлений, совершаемых с использованием информационно-коммуникационных технологий, в том числе легализации преступных доходов, финансирования терроризма, организации незаконного распространения наркотических средств и психотропных веществ, а также использования в противоправных целях цифровых валют» (п. 11 ст. 47). Активно развивающийся рынок цифровых технологий и их внедрение в современные управленческие системы не только диктуют новые правила, но и несут в себе большой потенциал криминологических угроз и рисков безопасности для России. Криминальная обстановка в данной сфере продолжает оставаться сложной, несмотря на предпринятые меры государства по обеспечению криминологической безопасности. В целях определения основных направлений обеспечения криминологической безопасности в сфере необходимо изучение современного состояния криминальных рисков, мониторинга деятельности по их снижению с целью выработки обоснованных предложений по снижению их уровня.

Обзор литературы

Изучению данной проблемы посвящены работы ряда криминологов и криминалистов: М.М. Бабаева А.Г. Горшенкова, Ю.В. Гаврилина, М.А. Ефремовой, А.Л. Лапина, С.Я. Лебедева, В.С. Овчинского, В.А. Плешакова, Э.Л. Сидоренко, Д.А. Симоненко и др. Именно их работы составили основу обеспечения криминологической безопасности в условиях цифровой трансформации. Кроме того, имеется ряд научных публикаций, в которых затрагиваются отдельные теоретические подходы криминологической безопасности в сфере цифровых технологий: А.В. Амосова, И.Р. Бегишев, Ю.Н. Жданова, Я.Г. Ищук, Д.А. Конев, А.В. Нестеренко, В.В. Смолин и др. Вместе с тем растущий интерес к изучению проблем обеспечения криминологической безопасности в современных условиях требует конкретизации деятельности по снижению рисков и угроз личности, обществу и государству.

Материалы и методы

Материалами исследования явились нормы законодательных актов, практика деятельности правоохранительных органов Российской Федерации, статистические данные, результаты исследований, проведенных автором и иными исследователями, научные работы в рамках обозначенной проблематики, а также материалы зарубежных и отечественных интернет-источников. В ходе работы над текстом использовались общенаучные и специальные методы (логический, системно-структурный, формально-юридический, сравнительно-правовой, статистический и др.).

Результаты исследования

Активно развивающийся рынок цифровых технологий и процессы их внедрения в современные управленческие системы способствуют развитию предприятий высокотехнологичных отраслей промышленности, повышению их конкурентоспособности. По оценкам экспертов, потенциальный экономический эффект от цифровизации российской экономики к 2025 году оценивается в 4,1 – 8,9 трлн руб., что составит 19 – 34% общего увеличения валового внутреннего продукта. Влияние цифровизации будет проявляться посредством оптимизации производственных и логистических операций, повышения эффективности рынка труда и производительности оборудования, эффективности НИОКР и разработки продуктов, а также снижения расхода ресурсов и производственных потерь.

В то же время необходимо иметь в виду, что цифровая трансформация влияет на уровень криминальных угроз и криминогенных рисков безопасности личности, общества и государства. Этот факт подтверждает криминологическая обстановка в сфере, которая на протяжении ряда последних лет остается сложной, так как быстрые темпы цифровой трансформации «не позволяют своевременно и в должной мере подготовить механизмы по снижению уровня угроз безопасности» [1, с.76].

Таким образом, прирост количества зарегистрированных преступлений в сфере в 2015 году составил 400%, 2016 и 2017 гг. соответственно, 110 и 115%, в 2018 г. – 190% (174 674), в 2020 г. – 73,4%, при увеличении по сравнению с предыдущим периодом на 87,5% (267,6 тыс.) количества особо тяжких и тяжких преступлений. В 2021 г. количество выявленных преступлений достигло 517,7 тыс., что на 1,4% больше, чем за аналогичный период предыдущего года, средний показатель раскрываемости составил 22%. Такое снижение раскрываемости обусловлено, прежде всего, отсутствием специальной подготовки в сфере цифровых технологий сотрудников правоохранительных органов, современной законодательной и технической базы, методических рекомендаций по проблемным вопросам выявления, предотвращения, пресечения и раскрытия этого вида преступлений.

Широкое распространение получили хакинг, кардинг и фишинг, создающие серьезные проблемы во всем мире. С каждым годом увеличивается количество хакерских атак. Так, например, в марте 2022 г. число DDoS-атак на российские компании выросло в полтора раза по сравнению с февралем и в восемь раз – по сравнению с аналогичным периодом прошлого года. При этом наибольшая нагрузка пришлась на финансовые организации: их доля в общем объеме атак выросла за год вдвое – до 35% и на государственные органы – 33%.

Особую озабоченность вызывает не только в России, но и на международном уровне уровень легализации криминальных доходов оценивается как высокий. Опасность данного вида преступной деятельности сопряжена с вовлечением в сферу легального оборота криминальных активов для дальнейшего их использования, «одновременно позволяя преступникам развивать и совершенствовать криминальную деятельность, финансировать такие наиболее опасные виды этой деятельности, как терроризм, незаконный оборот наркотических средств и психотропных веществ, торговля людьми, поддерживать организованные преступные формирования» [3, с. 3] и др. Названный вид преступлений чаще всего выявляется при совершении предикатных пре-

ступлений (незаконный оборот наркотиков, преступления коррупционной направленности и др.). В чистом виде по ст. 174 и 174.1 УК РФ квалифицируют преступные деяния гораздо реже. Так, согласно статистической отчетности, количество зарегистрированных преступлений за последние 10 лет составило 7946.

О высоком уровне латентности легализации криминальных доходов свидетельствует и существенный рост предикатных преступлений. Так, в 2021 г. выявлено: 179,7 тыс. фактов сбыта наркотических средств и психотропных веществ преступлений (в 2017 г. – 107, 5 тыс., в 2018 г. – 112, 9 тыс., в 2019 г. – 190, 1 тыс., 2020 г. 189, 9 тыс.); 35,1 тыс. преступлений коррупционной направленности (2017 г. – 29,6 тыс., 2018 г. – 30,5 тыс., 2019 г. – 31 тыс., 2020 г. – 30,8 тыс.). При этом, по данным экспертов, правоохранительными органами выявляется не более 10% легализованных доходов, что свидетельствует о высоком уровне латентности этих преступлений [1].

Результаты изучения судебной практики указанных преступлений свидетельствуют об их совершении с использованием виртуальной валюты (криптовалюты), это очевидно осложняет процессы выявления и расследования таких преступлений, а в преступной среде обеспечивают популярность данного способа совершения преступлений в силу анонимности расчетов с использованием виртуальных валют (криптовалют).

Все чаще появляются новые схемы вывода за рубеж финансовых активов, имеющих сомнительное происхождение, которые в большей части используются для обеспечения функционирования теневой экономики («серый» импорт, уклонение от уплаты налоговых и таможенных платежей). Через эти схемы также осуществляется легализация криминальных доходов, полученных от коррупционных преступлений, мошенничества в кредитно-финансовой сфере, преступлений в бюджетной сфере в зарубежных странах. Выведенные в иностранные юрисдикции криминальные доходы инвестируются, как правило, в объекты жилой и коммерческой недвижимости, легальный бизнес, предметы роскоши, а также хранятся на депозитных и иных счетах в зарубежных банках. Для сокрытия конечных бенефициаров и финансовых активов используются иностранные юридические лица и образования, как правило, регистрируемые в юрисдикциях с льготным налогообложением.

Масштабное использование виртуальной валюты (криптовалюты) прослеживается при незаконном обороте наркотических средств и психотропных веществ, о чем свидетельствует не только судебная практика. Так, россияне активно пользуются «теневым» Интернетом в секторе продажи наркотиков. Их количество ежедневно в среднем приближается к 300 тыс. пользователей, что составляет 11% общемирового числа пользователей Даркнета [4]. Об объемах продаж товара свидетельствует количество серверов на русскоговорящем ресурсе «Гидра» (Hydra). На начало 2020 г. их количество достигло 3,5 тысяч. При этом передача товара осуществляется на условиях 100% предоплаты криптовалютой.

Согласно полученным данным, только с 2015 по 2021 год судами РФ вынесено более 300 приговоров за незаконный оборот наркотических средств и психотропных веществ, осуществляемый с использованием цифровой валюты (криптовалюты), а также за последующую легализацию криминальных доходов. Изучив материалы уголовных дел, приговоров судов по делам данной категории, мы пришли к выводу, что данный вид криминальной деятельности является не только высокоприбыльным, но и высоколатентным, поскольку преступная деятельность осуществляется:

- организованными группами и преступными сообществами (в такие группы входят помимо организатора кураторы интернет-магазинов, складов, операторы, курьеры, закладчики и пр.), которые в своей преступной деятельности используют цифровые технологии;

- в их деятельности прослеживается использование блочно-сетевой структуры, что позволяет им не взаимодействовать лично, осуществлять только дистанционное общение, по сети Интернет (Даркнет, TOR, Hydra и др.) или мобильной связи, через известные мессенджеры и социальные сети. Между покупателем и продавцом о приобретении наркотиков осуществляется общение в ходе переписки по средствам мобильной связи, с использованием сети Интернет или мессенджера «Telegram».

Высокая степень организации преступной деятельности и принятые меры конспирации позволяют им в течение длительного периода оставаться не разоблаченными правоохранительными органами и совершать тяжкие и особо тяжкие преступления в сфере незаконного оборота наркотических средств и психотропных веществ.

Необходимо обратить внимание и на такие социальные явления, как экстремизм и терроризм, «которые в настоящее время представляют особую опасность, так как активно используют в своей преступной деятельности новейшие цифровые технологии» [1, с. 76]. Именно благодаря стремительному развитию в России цифровых

технологий террористы и экстремисты ускоренными темпами стали расширять географию своей деструктивной идеологии, появилась возможность анонимности их финансирования, повысилась эффективность объединения широкого круга разобщенных пользователей, находящихся в разных точках мира.

Использование цифровых технологий способствовало расширению возможностей по управлению разрозненными силами и средствами. Отмечается тенденция перехода использования в террористических экстремистских целях платформы Element, так как Telegram, Twitter стали фильтровать сообщения, что позволяет идентифицировать пользователей. Это дает преступникам возможность использовать для общения зашифрованные каналы и собственные уникальные серверы, что позволяет более безопасно осуществлять коммуникационные функции и предотвращает возможность их обнаружения. Появились и частные коммуникации, например, медиаплатформа «Аркан», поддерживающая запрещенную на территории России экстремистскую организацию «Исламское государство»», специализирующая на распространении экстремистской и террористической идеологии. Оказывая техническую помощь сторонникам запрещенного на территории России Исламского государства, «Аркан» создал 120 аккаунтов в Facebook; 78 – в Twitter; 224 – в Telegram; 18 – в WhatsApp; 20 – в Proton и т.д. Более того, подготовлены пропагандистские материалы для распространения в социальных сетях. Сторонники запрещенного на территории России Исламского государства объявляют о наличии собственных медиаучреждений, распространяющих пропаганду на различных языках. Так, например, группа Afag, поддерживающая террористические организации, опубликовала 15 публикаций по руководству и технологиям использования возможностей сети Интернет в экстремистских и террористических целях. В «Бюллетене технических новостей» ею были опубликованы рекомендации по использованию специальных приложений для шпионажа и контрмерам по слежению за террористами через мобильные устройства.

Представленные примеры свидетельствуют, что процессы цифровизации способствовали расширению экстремистской и террористической деятельности в киберпространстве, где 80% от общего числа выявленных преступлений экстремистской и террористической направленности совершаются с использованием цифровых технологий, что обусловливает трудности, связанные с их отслеживанием, при том что террористические и экстремистские группы стали принимать значительно больше мер предосторожности в этом направлении.

Обсуждение и заключения

С учетом особенностей современного состояния угроз криминологической безопасности и с целью обеспечения защищенности личности, общества, государства в условиях цифровой трансформации необходимо:

– исследование, социально-правовое обоснование совершенствования нормативного правового регулирования с учетом использования правовой конвергенции [5] и формирование новой системы криминологической безопасности, которые бы соответствовали цифровой трансформации общества;

– обеспечение криминологической безопасности в условиях цифровой трансформации требует серьезной подготовки и переподготовки сотрудников правоохранительных органов, что требует модернизации образовательного процесса;

– взаимодействие правоохранительных органов не только на межведомственном и внутриведомственном уровнях, но и взаимодействие с организациями, обеспечивающими кибербезопасность финансовых учреждений, операторов сотовой связи и интернет-провайдеров;

– эффективное использование возможностей международного полицейского взаимодействия и сотрудничества, позволяющее оперативно и комплексно реагировать на угрозы криминологической безопасности.

В настоящее время по инициативе Российской Федерации активно идет подготовка к внеочередной сессии ООН по вопросам обеспечения криминологической безопасности в исследуемой сфере.

Вместе с тем на национальном уровне необходима подготовка российской стратегии обеспечения криминологической безопасности в сфере информационно-цифровых отношений.

СПИСОК ИСТОЧНИКОВ

1. Конев Д.А. Криминологическая безопасность и ее обеспечение в сфере цифровых технологий: дис… канд. юрид. наук: 12.00.08. Омск, 2022. 200 с.

2. Волеводз А.Г. Противодействие компьютерным преступлениям: правовые основы международного сотрудничества. Москва: Юрлитинформ, 2002. 496 с.

3. Тагирова В.А. Уголовная ответственность за отмывание доходов от преступной деятельности и его предупреждение в США и России: вопросы теории и законотворчества: дис. … канд. юрид. наук: 12.00.08 . Казань, 2005. 280 с.
4. Сидоренко Э.Л. Криптовалюта как новый юридический феномен // Общество и право. 2019. № 3 (57). С. 193 – 197.
5. Клочкова Ю.А. Конвергенционные правовые системы как результат современной глобализации // Государственная власть и местное самоуправление. 2001. № 4. С. 6 – 10.

REFERENCES

1. Konev D.A. Kriminologicheskaya bezopasnost' i ee obespechenie v sfere cifrovyh tekhnologij: dis… kand. yurid. nauk: 12.00.08. Omsk, 2022. 200 s.
2. Volevodz A.G. Protivodejstvie komp'yuternym prestupleniyam: pravovye osnovy mezhdunarodnogo sotrudnichestva. Moskva: YUrlitinform, 2002. 496 s.
3. Tagirova V.A. Ugolovnaya otvetstvennost' za otmyvanie dohodov ot prestupnoj deyatel'nosti i ego preduprezhdenie v SSHA i Rossii: voprosy teorii i zakonotvorchestva: dis. … kand. yurid. nauk: 12.00.08 . Kazan', 2005. 280 s.
4. Sidorenko E.L. Kriptovalyuta kak novyj yuridicheskij fenomen // Obshchestvo i pravo. 2019. № 3 (57). S. 193 – 197.
5. Klochkova YU.A. Konvergencionnye pravovye sistemy kak rezul'tat sovremennoj globalizacii // Gosudarstvennaya vlast' i mestnoe samoupravlenie. 2001. № 4. S. 6 – 10.

Информация об авторе:
Пинкевич Татьяна Валентиновна, доктор юридических наук, профессор, профессор кафедры уголовной политики Академии управления МВД России, pinkevich@yandex.ru

Автор прочитал и одобрил окончательный вариант рукописи.

Information about the author:
Pinkevich Tatyana Valentinovna, Doctor of Law (Doctor habilitatus), Professor, Professor of the Criminal Policy of Management Academy of MIA of Russia, pinkevich@yandex.ru

The author has read and approved the final version of the manuscript.

Статья получена: 11.05.2022.
Статья принята к публикации: 24.06.2022.
Статья опубликована онлайн: 28.06.2022.

Против размещения полнотекстовой версии статьи в открытом доступе в сети Интернет не возражаю.