

№ 5 (129)
2025

ВЕСТНИК УНИВЕРСИТЕТА

имени О.Е. Кутафина (МГЮА)

Право есть
искусство добра
и справедливости

*Jus est ars
boni et aequi*

В номере

Выпуск ПРОТИВОДЕЙСТВИЕ ПРЕСТУПЛЕНИЯМ В СФЕРЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

АВТОРИТЕТНОЕ МНЕНИЕ

26 Рускевич Е. А.

Цифровизация уголовного законодательства:
непростые последствия простых решений

34 Афанасьева О. Р., Шиян В. И.

Киберпреступность в регионах России:
современные тенденции и меры предупреждения

ВЕКТОР ЮРИДИЧЕСКОЙ НАУКИ

137 Воронин В. Н.

Использование искусственного интеллекта
при назначении наказания в зарубежных странах
и принцип справедливости

148 Антонян Е. А.

Китайский опыт борьбы с преступлениями
в сфере информационных технологий

169 Пан Дунмэй

Уголовно-правовое регулирование
незаконного привлечения средств
через ICO на основе технологий блокчейн

№ 5 (129)
2025

ВЕСТНИК УНИВЕРСИТЕТА имени О.Е. Кутафина (МГЮА)

Выпуск

**ПРОТИВОДЕЙСТВИЕ ПРЕСТУПЛЕНИЯМ
В СФЕРЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ**

Издается с 2014 года
Выходит один раз в месяц

Председатель редакционного совета:

БЛАЖЕЕВ Виктор Владимирович — ректор Университета имени О.Е. Кутафина (МГЮА), кандидат юридических наук, профессор, г. Москва, Россия

Заместитель председателя редакционного совета:

ГРАЧЕВА Елена Юрьевна — заведующий кафедрой финансового права Университета имени О.Е. Кутафина (МГЮА), доктор юридических наук, профессор, г. Москва, Россия

Главный редактор:

ШПАКОВСКИЙ Юрий Григорьевич — профессор кафедры экологического и природоресурсного права Университета имени О.Е. Кутафина (МГЮА), доктор юридических наук, профессор, г. Москва, Россия

Ответственный секретарь:

СЕВРЮГИНА Ольга Александровна — эксперт отдела научно-издательской политики Научно-исследовательского института Университета имени О.Е. Кутафина (МГЮА), г. Москва, Россия

Редакционный совет:

АФАНАСЬЕВ Сергей Федорович — заведующий кафедрой арбитражного процесса, адвокатуры и нотариата Саратовской государственной юридической академии, доктор юридических наук, профессор, г. Саратов, Россия

БЕЗВЕРХОВ Артур Геннадьевич — директор Юридического института Самарского национального исследовательского университета имени академика С.П. Королева, заведующий кафедрой теории и истории государства и права и международного права, доктор юридических наук, профессор, г. Самара, Россия

БИРЮКОВ Павел Николаевич — заведующий кафедрой международного и евразийского права Воронежского государственного университета, доктор юридических наук, профессор, г. Воронеж, Россия

БУКАЛЕРОВА Людмила Александровна — заведующий кафедрой уголовного права, уголовного процесса и криминалистики Российского университета дружбы народов, доктор юридических наук, профессор, г. Москва, Россия

ВОЛКОВ Геннадий Александрович — профессор кафедры экологического и земельного права юридического факультета Московского государственного университета имени М.В. Ломоносова, доктор юридических наук, г. Москва, Россия

ДЮФЛО Ален — эксперт-практик международного класса в области права, основатель адвокатского бюро «Дюффо и партнеры», преподаватель Университета Лион III имени Жана Мулена, г. Лион, Франция

ЕГОРОВА Мария Александровна — профессор кафедры конкурентного права, помощник проректора по научно-исследовательской деятельности Университета имени О.Е. Кутафина (МГЮА), доктор юридических наук, профессор, г. Москва, Россия

ЕРШОВА Инна Владимировна — первый проректор Университета имени О.Е. Кутафина (МГЮА), заведующий кафедрой предпринимательского и корпоративного права, доктор юридических наук, профессор, г. Москва, Россия

ЕФИМОВА Людмила Георгиевна — заведующий кафедрой банковского права Университета имени О.Е. Кутафина (МГЮА), доктор юридических наук, профессор, г. Москва, Россия

ЖАВОРОНКОВА Наталья Григорьевна — доктор юридических наук, профессор, г. Москва, Россия

ЗРАЖЕВСКАЯ Татьяна Дмитриевна — профессор кафедры конституционного и муниципального права Воронежского государственного университета, Уполномоченный по правам человека в Воронежской области, доктор юридических наук, профессор, г. Воронеж, Россия

ЗУБАРЕВ Сергей Михайлович — заведующий кафедрой административного права и процесса Университета имени О.Е. Кутафина (МГЮА), доктор юридических наук, профессор, г. Москва, Россия

ИЩЕНКО Евгений Петрович — профессор кафедры криминалистики Университета имени О.Е. Кутафина (МГЮА), доктор юридических наук, профессор, г. Москва, Россия

ИЩЕНКО Нина Сергеевна — заведующий кафедрой правоведения Гомельского филиала Международного университета «МИТСО», кандидат юридических наук, г. Гомель, Республика Беларусь

КИСЕЛЕВ Сергей Георгиевич — профессор Института права и национальной безопасности РАНХиГС при Президенте РФ, профессор Института международных отношений и социально-политических наук Московского государственного лингвистического университета, доктор филологических наук, профессор, г. Москва, Россия



Журнал рекомендован Высшей аттестационной комиссией Министерства науки и высшего образования РФ для публикации основных результатов диссертаций на соискание ученой степени доктора и кандидата наук.
Материалы журнала включены в систему Российского индекса научного цитирования.

© Университет имени О.Е. Кутафина (МГЮА), 2025

КОМАРОВА Валентина Викторовна — профессор кафедры конституционного и муниципального права Университета имени О.Е. Кутафина (МГЮА), доктор юридических наук, профессор, г. Москва, Россия

ЛАПИНА Марина Афанасьевна — профессор Департамента правового регулирования экономической деятельности Финансового университета при Правительстве РФ, доктор юридических наук, г. Москва, Россия

МИРОШНИЧЕНКО Владимир Михайлович — ректор Академии безопасности и специальных программ, доктор экономических наук, профессор, г. Москва, Россия

НИКИТИН Сергей Васильевич — заведующий кафедрой гражданского и административного судопроизводства Российского государственного университета правосудия имени В.М. Лебедева, доктор юридических наук, профессор, г. Москва, Россия

НОВОСЕЛОВА Людмила Александровна — заведующий кафедрой интеллектуальных прав Университета имени О.Е. Кутафина (МГЮА), доктор юридических наук, профессор, г. Москва, Россия

ПЛЮЩИКОВ Вадим Геннадьевич — директор Аграрно-технологического института Российского университета дружбы народов, доктор сельскохозяйственных наук, профессор, г. Москва, Россия

РАССОЛОВ Илья Михайлович — профессор кафедры информационного права и цифровых технологий Университета имени О.Е. Кутафина (МГЮА), доктор юридических наук, доцент, г. Москва, Россия

РОЗА Фабрис — профессор кафедры трудового права Университета Реймс Шампань-Арденны, Франция

РОССИНСКАЯ Елена Рафаиловна — заведующий кафедрой судебных экспертиз Университета имени О.Е. Кутафина (МГЮА), доктор юридических наук, профессор, г. Москва, Россия

РЫЛЬСКАЯ Марина Александровна — директор Института проблем эффективного государства и гражданского общества Финансового университета при Правительстве Российской Федерации, доктор юридических наук, доцент, г. Москва, Россия

СИНЮКОВ Владимир Николаевич — проректор по научно-исследовательской деятельности Университета имени О.Е. Кутафина (МГЮА), профессор кафедры теории государства и права, доктор юридических наук, профессор, г. Москва, Россия

СОКОЛОВА Наталья Александровна — заведующий кафедрой международного права, научный руководитель Научно-исследовательского института Университета имени О.Е. Кутафина (МГЮА), доктор юридических наук, профессор, г. Москва, Россия

УСТЮКОВА Валентина Владимировна — и.о. заведующего сектором экологического, земельного и аграрного права Института государства и права РАН, доктор юридических наук, профессор, г. Москва, Россия

ЦАЙ ЦЗЮНЬ — директор Юридического института Хэнаньского университета, доктор юридических наук, профессор, г. Кайфэн, КНР

ЦОПАНОВА Индира Георгиевна — декан юридического факультета Российской таможенной академии, кандидат юридических наук, доцент, г. Москва, Россия

ШИЛЬСТЕЙН Давид — профессор права, заведующий кафедрой уголовного права Университета Париж 1 Пантеон-Сорбонна, г. Париж, Франция

ЩЕГОЛЕВ Виталий Валентинович — проректор Московского гуманитарно-экономического университета по научной работе и международному сотрудничеству, доктор политических наук, г. Москва, Россия

Ответственный редактор выпуска:

ВОРОНИН Вячеслав Николаевич — доцент кафедры уголовного Университета имени О.Е. Кутафина (МГЮА), кандидат юридических наук, доцент

В журнале публикуются статьи по научным специальностям группы 5.1 «Право» (юридические науки)	5.1.1. Теоретико-исторические правовые науки. 5.1.2. Публично-правовые (государственно-правовые) науки. 5.1.3. Частноправовые (цивилистические) науки. 5.1.4. Уголовно-правовые науки. 5.1.5. Международно-правовые науки.
РЕГИСТРАЦИЯ СМИ	Журнал зарегистрирован Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) ПИ № ФС77-67361 от 5 октября 2016 г.
ISSN	2311-5998 (Print), 2782-6163 (Online)
ПЕРИОДИЧНОСТЬ	12 раз в год
УЧРЕДИТЕЛЬ И ИЗДАТЕЛЬ	Федеральное государственное автономное образовательное учреждение высшего образования «Московский государственный юридический университет имени О.Е. Кутафина (МГЮА)» Садовая-Кудринская ул., д. 9, стр. 1, вн. тер. г. муниципальный округ Пресненский, г. Москва, Россия, 123242
АДРЕС РЕДАКЦИИ	Садовая-Кудринская ул., д. 9, стр. 2, г. Москва, Россия, 125993 Тел.: 8 (499) 244-88-88 (доб. 687). E-mail: vestnik@msal.ru
ПОДПИСКА И РАСПРОСТРАНЕНИЕ	Свободная цена Журнал распространяется через объединенный каталог «Пресса России» и интернет-каталог агентства «Книга-Сервис» Подписной индекс 40650. Подписка на журнал возможна с любого месяца
ТИПОГРАФИЯ	Отпечатано в Издательском центре Университета имени О.Е. Кутафина (МГЮА) Садовая-Кудринская ул., д. 9, стр. 2, г. Москва, Россия, 125993
ВЫПУСКНЫЕ ДАННЫЕ	Дата выхода в свет: 31.07.2025 Объем 27,4 усл. печ. л. (16,6 а. л.), формат 84×108/16 Тираж 150 экз. Печать цифровая. Бумага офсетная

При использовании опубликованных материалов журнала ссылка на «Вестник Университета имени О.Е. Кутафина (МГЮА)» обязательна. Перепечатка допускается только по согласованию с редакцией. Точка зрения редакции не всегда совпадает с точкой зрения авторов публикаций.

Редактор Л. А. Мункуева

Корректор С. И. Ершова

Компьютерная верстка Е. Г. Булычев

**№ 5 (129)
2025**

COURIER

OF THE KUTAFIN MOSCOW STATE LAW UNIVERSITY (MSAL)

Edition

Countering Crimes
in the Field of Information Technology

Published from the year of 2014
Monthly journal

Chairperson of the Council of Editors:

BLAZHEEV Victor Vladimirovich — Rector of Kutafin Moscow State Law University (MSAL), Cand. Sci. (Law), Professor, Moscow, Russia

Vice-Chairperson of the Council of Editors:

GRACHEVA Elena Yurievna — Head of the Department of Financial Law of Kutafin Moscow State Law University (MSAL), Dr. Sci. (Law), Professor, Moscow, Russia

Chief Editor:

SHPAKOVSKIY Yuriy Grigorievich — Professor of the Department of Environmental and Natural Resources Law of Kutafin Moscow State Law University (MSAL), Dr. Sci. (Law), Professor, Moscow, Russia

Executive Secretary Editor:

SEVRYUGINA Olga Alexandrovna — Expert of the Research and Publishing Policy Department of the Research Institute of Kutafin Moscow State Law University (MSAL), Moscow, Russia

Council of editors:

AFANASIEV Sergey Fedorovich — Head of the Department of Arbitrazh Procedure, Advocacy and Notary of Saratov State Academy of Law, Dr. Sci. (Law), Professor, Saratov, Russia

BEZVERKHOV Arthur Gennadevich — Director of the Law Institute of the National Research University named after Academician Sergey P. Korolev, Dr. Sci. (Law), Professor, Samara, Russia

BIRIUKOV Pavel Nikolaevich — Head of the Department of International and Eurasian Law of Voronezh State University, Doctor of Law, Professor, Voronezh, Russia

BUKALEROVA Ludmila Alexandrovna — Head of the Department of Criminal Law, Criminal Procedure and Criminology of the Peoples' Friendship University of Russia, Dr. Sci. (Law), Professor, Moscow, Russia

VOLKOV Gennadiy Aleksandrovich — Professor of the Department of Environmental and Land Law of the Faculty of Law of Lomonosov Moscow State University, Dr. Sci. (Law), Moscow, Russia

DUFLOT Alain — an expert practitioner in the field of law, founder of the law firm «Dufлот & Partners», Lecturer at the Jean Moulin Lyon 3 University, Lyon, France

EGOROVA Maria Alexandrovna — Professor of the Department of Competition Law, Assistant of Vice-Rector for Research of Kutafin Moscow State Law University (MSAL), Dr. Sci. (Law), Professor, Moscow, Russia

ERSHOVA Inna Vladimirovna — First Vice-Rector of Kutafin Moscow State Law University (MSAL), Head of the Department of Business and Corporate Law of Kutafin Moscow State Law University (MSAL), Dr. Sci. (Law), Professor, Moscow, Russia

EFIMOVA Lyudmila Georgievna — Head of the Department of Banking Law of Kutafin Moscow State Law University (MSAL), Dr. Sci. (Law), Professor, Moscow, Russia

ZHAVORONKOVA Natalya Grigorevna — Dr. Sci. (Law), Professor, Moscow, Russia

ZRAZHEVSKAYA Tatyana Dmitrievna — Professor of the Department of Constitutional and Municipal Law of Voronezh State University, Commissioner for Human Rights in the Voronezh Region, Dr. Sci. (Law), Professor, Voronezh, Russia

ZUBAREV Sergey Mikhailovich — Head of the Department of Administrative Law and Procedure of Kutafin Moscow State Law University (MSAL), Dr. Sci. (Law), Professor, Moscow, Russia

ISHCHENKO Evgeniy Petrovich — Head of the Department of Criminalistics of Kutafin Moscow State Law University (MSAL), Dr. Sci. (Law), Professor, Moscow, Russia

ISHCHENKO Nina Sergeyevna — PhD in Law, Professor, Head of the Department of Jurisprudence of the Gomel Branch of the International University «MITSO», Gomel, Republic of Belarus

KISELEV Sergey Georgievich — Professor, Institute of Law and National Security, RANEPA University; Professor, Institute of International Relations and Socio-Political Sciences, Moscow State Linguistic University, Dr. Sci. (Philosophy), Professor, Moscow, Russia

KOMAROVA Valentina Viktorovna — Professor of the Department of Constitutional and Municipal Law of Kutafin Moscow State Law University (MSAL), Dr. Sci. (Law), Professor, Moscow, Russia

LAPINA Marina Afanasyeva — Professor of the Department of Legal Regulation of Economic Activity of the Financial University

Recommended by the Higher Attestation Commission of the Ministry of Science and Higher Education of the Russian Federation for publication of results of doctoral theses.
Materials included in the journal Russian Science Citation Index



© Kutafin Moscow State Law University (MSAL), 2025

under the Government of the Russia, Dr. Sci. (Law), Moscow, Russia

MIROSHNICHENKO Vladimir Mikhailovich — Rector of the Academy of Security and Special Programs, Dr. Sci. (Economics), Professor, Moscow, Russia

NIKITIN Sergey Vasilyevich — Head of the Department of Civil and Administrative Court Proceedings of the Lebedev Russian State University of Justice, Dr. Sci. (Law), Professor, Moscow, Russia

NOVOSELOVA Lyudmila Alexandrovna — Head of the Department of Intellectual Property Law of Kutafin Moscow State Law University (MSAL), Dr. Sci. (Law), Professor, Moscow, Russia

PLYUSHCHIKOV Vadim Gennadyevich — Director of Agrarian and Technological Institute of the Peoples' Friendship University of Russia, Dr. Sci. (Agr. Sc.), Professor, Moscow, Russia

RASSOLOV Ilya Mikhailovich — Professor of the Department of Information Law and Digital Technologies of Kutafin Moscow State Law University (MSAL), Dr. Sci. (Law), Associate Professor, Moscow, Russia

ROSA Fabrice — Professor of the Department of Labour Law at the University of Reims Champagne-Ardenne, France

ROSSINSKAYA Elena Rafailovna — Head of the Department of Forensic Examination of Kutafin Moscow State Law University (MSAL), Dr. Sci. (Law), Professor, Moscow, Russia

RYLSKAYA Marina Alexandrovna — Director of the Institute of Problems of the Efficient State and Civil Society of the Financial University under the Government of the Russia, Dr. Sci. (Law), Associate Professor, Moscow, Russia

SINYUKOV Vladimir Nikolaevich — Vice-Rector for Research of Kutafin Moscow State Law University (MSAL), Professor of

the Department of Theory of the State and Law, Dr. Sci. (Law), Professor, Moscow, Russia

SOKOLOVA Natalya Alexandrovna — Head of the Department of International Law, Academic Director of the Research Institute of Kutafin Moscow State Law University (MSAL), Dr. Sci. (Law), Professor, Moscow, Russia

USTYUKOVA Valentina Vladimirovna — Acting Head of the Sector of Environmental, Land and Agricultural Law of the Institute of the State and Law of the RAS, Dr. Sci. (Law), Professor, Moscow, Russia

TSAY TSZYUN — Director of the Law Institute of Henan University, Dr. Sci. (Law), Professor, Kaifen, the PRC

TSOPANOVA Indira Georgievna — Dean of the Law Faculty of the Russian Customs Academy, Cand. Sci. (Law), Associate Professor, Moscow, Russia

CHILSTEIN David — Professor of Law, Head of the Department of Criminal Law at the University of Paris 1 Pantheon-Sorbonne, Paris, France

SHCHEGOLEV Vitaliy Valentinovich — Vice-Rector for Research and International Cooperation of the Moscow University of Humanities and Economics, Dr. Sci. (Political Sciences), Moscow, Russia

Editor-in-Chief of the Issue:

VORONIN Vyacheslav Nikolaevich — Associate Professor of the Department of Criminal Law of the Kutafin Moscow State Law University (MSAL), Cand. Sci. (Law), Associate Professor

The Journal publishes research papers written on scientific specialties of Group 5.1 «Law» (Legal Sciences)	5.1.1. Theory and History of Law. 5.1.2. Public Law and State Law. 5.1.3. Private Law (Civil Law). 5.1.4. Criminal Law. 5.1.5. International Law.
THE CERTIFICATE OF MASS MEDIA REGISTRATION	The journal was registered by the Federal Service for Supervision of Communications, Information Technology and Mass Media (Roskomnadzor) on 5 October 2016. The Certificate of Mass Media Registration: PI No. FS77-67361
ISSN	2311-5998 (Print), 2782-6163 (Online)
PUBLICATION FREQUENCY	12 issues per year
FOUNDER AND PUBLISHER	Federal State Autonomous Educational Institution of Higher Education "Kutafin Moscow State Law University (MSAL)". Sadovaya-Kudrinskaya ul., d. 9, str. 1, Presnensky intra-urb. ter. municipal district, Moscow, Russia, 123242
EDITORIAL OFFICE. POSTAL ADDRESS	9 str. 2 Sadovaya-Kudrinskaya ul., Moscow, Russia, 125993 Tel.: +7 (499) 244-88-88 (ext. 687) E-mail: vestnik@msal.ru
SUBSCRIPTION AND DISTRIBUTION	Free price The journal is distributed through "Press of Russia" joint catalogue and the Internet catalogue of "Kniga-Servis" Agency Subscription index: 40650. Journal subscription is possible from any month
PRINTING HOUSE	Printed in Publishing Center of Kutafin Moscow State Law University (MSAL) 9 str. 2 Sadovaya-Kudrinskaya ul., Moscow, Russia, 125993
SIGNED FOR PRINTING	31.07.2025 Volume: 27,4 conventional printer's sheets (16,6 author's sheets). Format: 84×108/16. An edition of 150 copies. Digital printing. Offset paper
<i>When using published materials of the journal, reference to "Courier of the Kutafin Moscow State Law University (MSAL)" is obligatory. Full or partial use of materials is allowed only with the written permission of the authors or editors. The point of view of the Editorial Board may not coincide with the point of view of the authors of publications.</i>	
Editor L. A. Munkueva	Proof-reader S. I. Ershova
Computer layout E. G. Bulychev	

СОДЕРЖАНИЕ

СЛОВО К ЧИТАТЕЛЮ	10
УНИВЕРСИТЕТСКАЯ ХРОНИКА	12
АВТОРИТЕТНОЕ МНЕНИЕ	
Русскевич Е. А. Цифровизация уголовного законодательства: непростые последствия простых решений	26
Афанасьева О.Р., Шиян В.И. Киберпреступность в регионах России: современные тенденции и меры предупреждения	34
ВЕКТОР ЮРИДИЧЕСКОЙ НАУКИ	
Уголовно-правовое противодействие преступлениям в сфере информационных технологий	
Клепицкий И. А. Компьютерные преступления: вопросы юридической техники	48
Алёхин Д. Э. Квалификация преступлений, связанных с получением криптовалюты (майнингом)	58
Князьков А. А. Уголовно-правовая новелла за нарушение законодательства о персональных данных (ст. 272 ¹ УК РФ): особенности конструирования состава и вопросы квалификации	65
Молчанов Д. М. Информационная безопасность как объект охраны от агрессивного информационного воздействия	74
Грачева Ю. В., Чалышева Ю. В. Общественная опасность и уголовно-правовая оценка фальсификации национальной истории в компьютерных играх	84
Юрченко И. А. Теоретические и практические аспекты квалификации различных форм участия в публично демонстрируемых преступлениях против личности	93
Рубцова А. С., Устинова Т. Д. Коммерческий секс и виртуальная реальность: уголовно-правовой аспект	102
Бимбинов А. А. Уголовно-правовые риски использования приложений для заказа товаров и коммерческих услуг	112
Алтунин Т. В. Уголовно-правовая характеристика торговли алкогольной продукцией с использованием информационно-телекоммуникационных сетей, включая сеть Интернет	122
Радов В. В. Наказуемость преступлений в сфере информационных технологий ...	128

Зарубежный опыт

Воронин В. Н.

Использование искусственного интеллекта при назначении наказания в зарубежных странах и принцип справедливости 137

Антонян Е. А.

Китайский опыт борьбы с преступлениями в сфере информационных технологий 148

Хармаев Ю. В.

Современное состояние и тенденции киберпреступности в Монголии 159

Пан Дунмэй

Уголовно-правовое регулирование незаконного привлечения средств через ICO на основе технологий блокчейн 169

Криминологическое противодействие киберпреступлениям

Клещина Е. Н.

Проблемы предупреждения преступлений, совершаемых посредством информационных технологий работниками банков 181

Мочалкина И. С.

Криминологическое противодействие экономическим преступлениям, совершаемым с использованием информационно-телекоммуникационных технологий 189

Червонных Е. В.

Формирование криминогенных ситуаций в сфере социальных медиа и их влияние на процесс криминализации личности 197

Емельянов Н. С.

Пенитенциарная киберпреступность как угроза стабильного функционирования исправительного учреждения 208

Борисов А. В.

Киберпреступность на транспорте: состояние и тенденции 214

Попова Е. Э.

Применение технологии искусственного интеллекта для оценки исправления осужденных при досрочном освобождении от наказания 221

Быстрова Ю. В.

Киберпреступность в отношении несовершеннолетних: причины и направления предупреждения 228

Гришко Н. А.

Защита потенциальных жертв киберпреступлений: виктимологический подход 234

Кузнецова О. А., Маджумеев М. М.

Защита частной жизни в виртуальной реальности:
ответственность за использование дипфейк-контента
в метавселенной 244

ПРАВО В ИСТОРИЧЕСКОМ ПРЕЛОМЛЕНИИ

Из периодики прошлого

Эстрин А.

К вопросу о принципах построения системы уголовной репрессии
в пролетарском государстве (*Извлечение*) 254

ПОСТСКРИПТУМ

Воронин В. Н.

Подлинный анекдот «Петр Великий
не прощает при смертной своей болезни убийц» 260

CONTENTS

NOTE TO THE READERS	10
UNIVERSITY CHRONICLE	12
AUTHORITATIVE OPINION	
Russkevich E. A. Digitalization of Criminal Legislation: Complex Consequences of Simple Solutions	26
Afanasieva O. R., Shiyan V. I. Cybercrime in the Regions of Russia: Current Trends and Preventive Measures	34
VECTOR OF LEGAL SCIENCE РАЗДЕЛ	
Criminal Law Counteraction to Crimes in the Field of Information Technology	
Klepitskij I. A. Computer Crimes: Legal Technique Issues	48
Alekhin D. E. Qualification of crimes related to obtaining cryptocurrency (mining)	58
Knyazkov A. A. Criminal law novel for violation of the legislation on personal data (Art. 272 ¹ of the Criminal Code of Russia): design features of the composition and qualification issues	65
Molchanov D. M. Information Security as an Object of Protection from Aggressive Information Influence	74
Gracheva Ju. V., Chalysheva Ju. V. Social Danger and Criminal-Legal Assessment of Falsification of National History in Computer Games	84
Yurchenko I. A. Theoretical and Practical Aspects of Qualification of Various Forms of Participation in Publicly Demonstrated Crimes against the Person	93
Rubtsova A. S., Ustinova T. D. Commercial Sex and Virtual Reality: Criminal Law Aspect	102
Bimbinov A. A. Criminal Law Risks of Using Applications to Order Goods and Commercial Services	112
Altunin T. V. Criminal and Legal Characteristics of Alcohol Product Trade Using Information and Telecommunication Networks, Including the Internet	122
Radov V. V. Punishability of Crimes in the Field of Information Technology	128

Foreign experience

Voronin V. N.

- The Role of AI in Sentencing Decisions and the Principle of Justice:
A Cross-Jurisdictional Analysis 137

Antonyan E. A.

- China's Experience in Combating IT Crimes 148

Kharmaev Yu. V.

- Cybercrime in Mongolia. Up-to-date state and trends 159

Pang Dongmei

- Criminal Law Regulation of Illegal Funds Raising through ICO Based
on Blockchain Technology 169

Criminological Counteraction to Cybercrimes

Kleschina E. N.

- Problems of Preventing Crimes Committed by Bank Employees
Using Information Technology 181

Mochalkina I. S.

- Criminological counteraction to economic crimes committed using
information and telecommunication technologies 189

Chervonnykh E. V.

- Formation of Criminogenic Situations in the Sphere of Social Media
and their Influence on the Process of Criminalization of the Individual 197

Yemelyanov N. S.

- Penitentiary Cybercrime as a Threat to the Stable Functioning
of Correctional Institutions 208

Borisov A. V.

- Cybercrime in Transport: Status and Trends 214

Popova E. E.

- Application of Artificial Intelligence Technology to Assess
the Correction of Convicts on Early Release from Punishment 221

Bystrova Yu. V.

- Cybercrime against Minors: Causes and Directions of Prevention 228

Grishko N. A.

- Protecting Potential Victims of Cybercrime: a Victimological Approach 234

Kuznetsova O. A., Majumae M. M.

- Protection of Privacy in Virtual Reality:
Liability for the Use of Deepfake Content in the Metaverse 244

LAW IN HISTORICAL REFRACTION

From the periodicals of the past

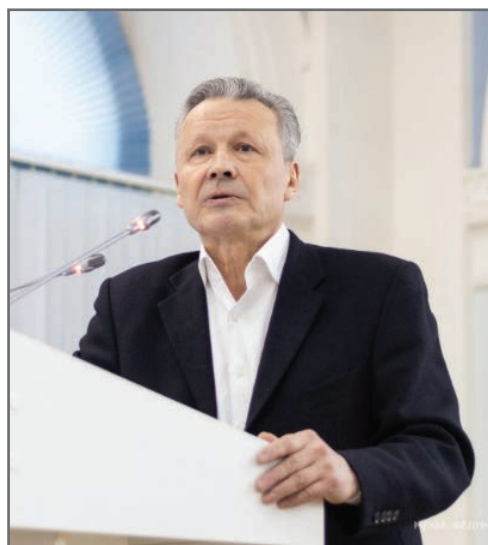
Estrin A.

On the Principles of Building a System of Criminal Repression
in a Proletarian State (Extract) 254

POSTSCRIPT

Voronin V. N.

The True Anecdote «Peter the Great Does
Not Forgive Murderers in His Deathbed» 260



Уважаемые читатели!

Предлагаем вашему вниманию выпуск журнала «Вестник Университета имени О.Е. Кутафина (МГЮА)», подготовленный совместными усилиями двух дружественных научных коллективов: кафедры криминологии и уголовно-исполнительного права имени В. Е. Эминова и кафедры уголовного права нашего Университета.

Совместный тематический номер посвящен одной из наиболее актуальных и одновременно сложных современных проблем — противодействия преступлениям в сфере информационных технологий. Бурное развитие информационных технологий не только открывает новые горизонты для социального и экономического прогресса, но и порождает качественно новые формы противоправной деятельности, требующие эффективного уголовно-правового реагирования и криминологической профилактики.

Авторы статей, опубликованных в этом номере, представляют комплексный взгляд на современные особенности цифровизации преступности. Особое внимание уделено вопросам квалификации компьютерных преступлений, анализу механизмов криминализации противоправных действий в области виртуальных валют и нарушения законодательства о персональных данных. Представлены и глубокие криминологические исследования профилактики преступлений в цифровой сфере, включая банковский сектор, и механизмов обеспечения информационной безопасности.

Очевидно, что только совместными усилиями уголовного права и криминологии можно создать эффективные стратегии и инструменты для борьбы с цифровыми преступлениями и обеспечения правопорядка в виртуальном пространстве. Интеграция теоретических концепций и практических рекомендаций, представленных в материалах выпуска журнала, имеет важное значение для

укрепления безопасности и стабильности нашего общества в условиях цифровой трансформации.

Уверены, что каждый читатель найдет в номере материалы, представляющие профессиональный интерес, а приведенные исследования вызовут живой отклик и продолжение конструктивной научной дискуссии как в периодических научных изданиях, так и в рамках научных мероприятий, проводимых на площадке Университета имени О.Е. Кутафина (МГЮА).

Е. А. Антонян,

*заведующий кафедрой криминологии
и уголовно-исполнительного права имени В. Е. Эминова
Университета имени О.Е. Кутафина (МГЮА),
доктор юридических наук, профессор*

И. Э. Звечаровский,

*заведующий кафедрой уголовного права Университета
имени О.Е. Кутафина (МГЮА),
доктор юридических наук, профессор,
заслуженный юрист России, почетный работник прокуратуры
Российской Федерации*

Университет в общественной и научной жизни страны



Заседание Совета при Президенте Российской Федерации по развитию физической культуры и спорта

Ректор Университета имени О.Е. Кутафина (МГЮА) Виктор Блажеев принял участие в заседании Совета при Президенте Российской Федерации по развитию физической культуры и спорта.

Заседание в режиме видеоконференции провел Президент России Владимир Путин. Встреча была посвящена развитию адаптивной физической культуры и адаптивного спорта.

В заседании Совета также принял участие профессор кафедры спортивного права Университета имени О.Е. Кутафина (МГЮА), председатель Комитета Государственной Думы по физической культуре и спорту Олег Матыцин.

¹ <https://msal.ru/news/>.

Церемония открытия памятника Михаилу Михайловичу Сперанскому



Ректор Университета имени О.Е. Кутафина (МГЮА) Виктор Блажеев принял участие в церемонии открытия памятника Михаилу Михайловичу Сперанскому — выдающемуся юристу, государственному и общественному деятелю.

Церемония открытия монумента состоялась 19 мая 2025 г. в Санкт-Петербурге у здания Российской национальной библиотеки в рамках мероприятий XIII Петербургского международного юридического форума. С приветственным словом на церемонии открытия выступили министр юстиции РФ Константин Чуйченко, губернатор Санкт-Петербурга Александр Беглов, председатель Ассоциации юристов России Сергей Степашин и др.

Серия мероприятий, посвященных Дню Победы

6 мая 2025 г. в Университете имени О.Е. Кутафина (МГЮА) прошел торжественный концерт, посвященный 80-летию Победы в Великой Отечественной войне.

Это событие — дань памяти героизму и мужеству тех, кто отстоял свободу и независимость нашей Родины. В рамках мероприятия участники услышали рассказы о жизненном пути героев Советского Союза, чьи имена навсегда вписаны в историю страны, а также увидели патриотические творческие номера, подготовленные студентами Университета.





С приветственным словом к участникам мероприятия обратился ректор Университета Виктор Блажеев: *«В честь празднования Великой Победы хочу подчеркнуть, что это была победа всего советского народа. Мы победили благодаря тем, кто сражался на фронтах, и тем, кто трудился в тылу. Все сплотились под единым знаменем и вместе одержали победу в этой страшной войне. Война пришла в каждый дом, унесла жизни, но принесла и будущее. Мы говорим не только о подвиге в целом, но и о судьбах конкретных людей, многие из которых работали и работают в нашем Университете. Это историческая правда, и наша задача — передавать ее следующему поколению. Важно помнить, что в Великой Отечественной войне участвовали представители всех народов Советского Союза. Борьба с нацизмом продолжается и сегодня. Мы гордимся нашими героями, которые продолжают защищать мир».*

На концерте в честь 80-й годовщины Победы вспомнили Бориса Васильевича Кравцова — Героя Советского Союза, выпускника Всесоюзного юридического заочного института. Его подвиги остаются ярким примером мужества и патриотизма для всех поколений.

На экранах Кутафинского зала были представлены имена, портреты и биографии 44 ветеранов Всесоюзного юридического заочного института, прошедших через Великую Отечественную войну. Их судьбы — пример беззаветного служения Родине. Сражаясь на фронтах и трудясь в тылу, они проявляли мужество, стойкость и веру в Победу. После войны многие из них посвятили себя развитию отечественной правовой системы.

С приветственным словом к участникам концерта обратился Герой России, участник специальной военной операции, подполковник Сергей Бойко.

Во внутреннем двореке Университета имени О.Е. Кутафина (МГЮА) работала полевая кухня. Студенты, работники и профессорско-преподавательский состав Университета смогли попробовать армейскую еду: гречку с тушенкой и морковь, черный хлеб и чай с лимоном.

Праздничные мероприятия завершились спектаклем «Завтра была война...», организованным театральным направлением «Изида» Культурно-творческого центра Ассоциации студентов.



Конференции, круглые столы, семинары



XIII Петербургский международный юридический форум

В период с 19 по 21 мая 2025 г. делегация Университета имени О.Е. Кутафина (МГЮА) принимала участие в деловой программе XIII Петербургского международного юридического форума, представляя вуз на профильных сессиях и мероприятиях, в том числе на Международном молодежном юридическом форуме.

Ректор Университета Виктор Блажеев выступил на сессии «Институт иностранного агента. Мировой опыт», которую он и проводил, и на сессии «Защита национальных интересов в сфере физической культуры и спорта». Эксперты обсудили механизмы противодействия деструктивному иностранному влиянию.

В числе спикеров сессии выступили директор Департамента информации и печати МИД России Мария Захарова, председатель Комитета Государственной Думы по развитию гражданского общества, вопросам общественных и религиозных объединений Яна Ланратова, заместитель министра юстиции РФ Олег Свириденко, а также известные пранк-журналисты Владимир Кузнецов (Вован) и Алексей Столяров (Лексус).

В работе секции «Цифровой бизнес и право» приняла участие первый проректор Университета имени О.Е. Кутафина (МГЮА) Инна Ершова.

Инна Владимировна рассказала о главных вызовах, с которыми сталкивается российское законодательство в эпоху цифровой трансформации: *«Я бы сказала, что этап нормативного регулирования цифровой экономики в целом завершен, и, по мнению многих, достаточно успешно. Это можно сравнить с периодом*





1990-х гг., когда мы только начинали формировать новую предпринимательскую экономику. Тогда мы ориентировались на зарубежный опыт, не всегда осознавая все риски, и лишь со временем начали отходить от неприемлемых для нашей системы решений. Сегодня мы наблюдаем похожую ситуацию: переход от аналоговой экономики к цифровой снова сопровождается множеством вопросов и неопределенностей. Но именно через их осмысление и решение мы сможем двигаться вперед».

Проректор по стратегическому и международному развитию Мария Мажорина приняла участие в сессии «Право в эпоху устойчивого развития: экологичная трансформация бизнеса и государства».

Эксперты обсудили вопрос переосмысления правового регулирования в связи с трансформацией экономики и ростом значимости ESG-повестки.

«Мы наблюдаем формирование новой правовой дисциплины — климатического права, которое выходит за рамки традиционного экологического регулирования и все чаще затрагивает экономические и финансовые аспекты. Это направление порождает качественно новую категорию правовых споров, связанных с ответственностью государств и корпораций за климатические последствия их деятельности. В рамках нашей исследовательской

группы при Университете за последние несколько лет мы фиксируем значительный рост интереса к климатической литигации. Мы классифицируем возникающие споры, продолжаем их изучение и стремимся к более глубокому пониманию этой стремительно развивающейся области права», — отметила Мария Мажорина.

Заведующий кафедрой конкурентного права Сергей Пузыревский и доцент кафедры Денис Гаврилов выступили спикерами на сессии «35 лет антимонопольному регулированию: результаты и перспективы».

Заведующий кафедрой нотариата Константин Корсик стал участником сессии «Развитие современных информационных технологий в сфере управления землей и недвижимостью».

Заведующий кафедрой интеллектуальных прав Людмила Новоселова участвовала в обсуждении вопросов, поднятых в рамках сессии «Правовые эксперименты: драйверы или риски?».

Заведующий кафедрой адвокатуры Светлана Володина приняла участие в дискуссии «Инновационные модели пенитенциарных учреждений».

На XIII Петербургском международном юридическом форуме ректор Университета имени О.Е. Кутафина (МГЮА) Виктор Блажеев и председатель Ассоциации юристов России Сергей Степашин подписали соглашение о проведении Всероссийского молодежного юридического форума «ЮрСлет».

Мероприятие планируется провести на площадке загородного комплекса Университета имени О.Е. Кутафина (МГЮА) «Малюшина дача».

19 мая 2025 г. в рамках XIII Петербургского международного юридического форума начала работу секция «Право в эпоху устойчивого развития: экологичная трансформация бизнеса и государства».

На площадке XIII Петербургского международного юридического форума состоялась презентация книг профессорско-преподавательского состава Университета имени О.Е. Кутафина (МГЮА).

В первый день ПМЮФ прошла презентация следующих книг:

- «Модернизация правовых и организационных режимов внешнеторговой деятельности в условиях геополитической трансформации» (автор — профессор кафедры международного частного права Бениамин Шахназаров);
- «Инновационная юриспруденция» (учебник; авторы — ректор Университета имени О.Е. Кутафина (МГЮА) Виктор Блажеев и проректор по международному и стратегическому развитию Мария Мажорина);
- «Цифровое право» (учебник; авторы — ректор Университета имени О.Е. Кутафина (МГЮА) Виктор Блажеев и профессор кафедры конкурентного права Мария Егорова);
- Law and the Real Economy in Russia (монография; авторы — первый проректор Университета имени О.Е. Кутафина (МГЮА) Инна Ершова и директор Института бизнес-права Андрей Петраков).

Во второй день ПМЮФ прошла презентация книг:

- «Семейное и женское предпринимательство в парадигме частноправового регулирования» (под редакцией первого проректора, заведующего кафедрой предпринимательского и корпоративного права Университета имени О.Е. Кутафина (МГЮА) Инны Ершовой);
- «Правовое сопровождение девелоперской деятельности» (под редакцией директора Института бизнес-права Университета имени О.Е. Кутафина (МГЮА) Андрея Петракова).



XI Летняя школа молодых ученых «Искусственный интеллект: проблемы правового регулирования»



26 мая 2025 г. в загородном комплексе Университета имени О.Е. Кутафина (МГЮА) «Малюшина дача» началась работа XI Летней школы молодых ученых «Искусственный интеллект: проблемы правового регулирования».

На протяжении пяти дней аспиранты ведущих вузов России, соискатели и кандидаты наук были погружены в вопросы регулирования искусственного интеллекта: от возможной правосубъектности ИИ до основ работы с нейросетями в образовательной и практической деятельности



Открывая XI Летнюю школу молодых ученых, первый проректор Университета Инна Ершова отметила: *«Мы наблюдаем невероятную трансформацию права: нечто подобное уже происходило в 1980—1990-е годы, когда мы переходили от одной общественно-экономической формации к другой. Тогда мы отвергли старое право, которое не подходило для рыночной экономики, и создали новое. Сегодня мы переживаем нечто похожее, если не более масштабное. Мы обсуждаем цифровизацию, цифровое право и его роль в современном мире. Говорим о правосубъектности искусственного интеллекта, и это открывает огромные возможности для дискуссий. Пройдут годы, вы станете выдающимися учеными и*

профессиональными юристами. Я уверена, что вы будете с теплотой вспоминать этот период, когда на ваших глазах формировалось новое правовое регулирование. Вы обсуждали эти вопросы, переживали вместе с нами. И, возможно, через много лет вы сможете сказать, были ли мы тогда правы или заблуждались. Но именно в этом и заключается смысл обучения — в поиске нового знания и непрекращающихся открытий. Желаю успехов!»

Со словами приветствия выступили проректор по научно-исследовательской деятельности Университета Владимир Синюков и директор Института «Аспирантура и докторантура» Мария Варлен.

«Ежегодно мы собираемся на Школе молодых ученых, не только чтобы обсуждать учебные темы, но и свободно мыслить: важно подходить к обучению не только академически, но и инновационно-творчески. Общее и высшее образование необходимы для квалификации, но, когда вы достигаете более высокого уровня, важно не только знание, но и творческое познание. Написание научных статей, диссертации — все это требует дополнительного мышления и опыта. Наука, которую вы изучаете, изменилась. Теперь она работает в режиме, где каждый может быть исследователем и мыслителем. Мы хотим,

чтобы вы вышли за рамки отраслевых задач. Это важно, потому что ни одна жизненная проблема не может быть решена без понимания ее в социальном или технологическом контексте. Обратите внимание, что Школа — это не повторение конференции или круглого стола. Здесь важна индивидуальность, мы не стремимся к большому количеству слушателей, а приглашаем тех, кто готов к глубокому погружению в тему», — отметил Владимир Синюков.

В Университете имени О.Е. Кутафина (МГЮА) обсудили наследие юриста, ученого и фронтовика — академика В. В. Лаптева

5 мая 2025 г. в Университете состоялось научно-просветительское мероприятие, приуроченное к 80-летию Победы в Великой Отечественной войне, — открытая трибуна на тему «Юрист, ученый, фронтовик — академик В. В. Лаптев». Инициаторами и организаторами события выступили кафедра предпринимательского и корпоративного права и Институт бизнес-права. Проведение открытой трибуны стало важным шагом в деле формирования ценностных ориентиров и профессиональных установок у студентов.

В центре внимания мероприятия оказалась личность выдающегося отечественного ученого-правоведа Владимира Викторовича Лаптева — советского и российского исследователя в области хозяйственного и гражданского права.

В. В. Лаптев был академиком Академии наук СССР. Под его научным руководством были изданы фундаментальные учебники по хозяйственному и предпринимательскому праву, которые до настоящего времени сохраняют свое значение для правовой науки и практики.



IV Всероссийская неделя теории государства и права

С 12 по 16 мая 2025 г. на площадке Университета имени О.Е. Кутафина (МГЮА) прошла ежегодная IV Всероссийская неделя теории государства и права, организованная совместно с Аппаратом Уполномоченного по правам человека в Российской Федерации, Общественной палатой Российской Федерации. В этом году центральной темой мероприятия стала тема «Приоритеты юридической науки и образования».

С приветственным словом к участникам и организаторам обратился заведующий кафедрой теории государства и права Университета Аркадий Корнев. Он отметил, что для ответа на ключевые вопросы о нашем прошлом,





настоящем и будущем необходимо использовать государственно-правовые формы, создающие смыслы государственного и правового развития. Проректор по научно-исследовательской деятельности Владимир Синюков в своем выступлении подчеркнул важность восстановления значения исторического и теоретического юридического знания в парадигме современного гуманитарного мышления. Также с приветственным словом к собравшимся обратился проректор по молодежной политике Александр Чанышев.

В ходе заседания выступила доктор юридических наук, профессор, заведующий кафедрой финансового права Университета Елена Грачева, которая сделала акцент на взаимосвязи отраслевых и теоретических юридических наук: *«Вы владеете сакральными знаниями о том, что происходит с нашим обществом, с нашим правом, с нашим государством. Нам, отраслевикам, эти знания сегодня необходимы. Мы с вами являемся свидетелями колоссальных преобразований. Осмысление этих процессов без вас, теоретиков, невозможно. Все то, над чем вы работаете, является ниточкой, связующей нас с такими науками, как философия, экономика, история, социология. Отраслевая наука чрезвычайно заинтересована и нуждается в современном*

осмыслении того, что же происходит в настоящее время с нашим человеческим обществом и какова роль права в регулировании этих процессов».

К участникам также обратился председатель Комитета Государственной Думы по науке и высшему образованию, профессор кафедры конституционного и муниципального права Университета Сергей Кабышев.

В рамках IV Всероссийской научной недели теории государства и права прошли онлайн-тестирование по теории государства и права, конкурс на лучшее эмпирическое исследование, мастер-классы, круглые столы, а также студенческая научная конференция «Инновационное юридическое образование и вызовы времени: каким должен быть современный юрист?».

XI Гусовские чтения

С 30 по 31 мая 2025 г. в Университете имени О.Е. Кутафина (МГЮА) прошла XI Международная научно-практическая конференция — Гусовские чтения «Национальные цели развития Российской Федерации через призму трудового права и права социального обеспечения».

На торжественном открытии с приветственным словом к участникам, гостям и организаторам конференции обратилась проректор по стратегическому и международному развитию Университета имени О.Е. Кутафина (МГЮА) Мария Мажорина: *«Сегодня мы уделяем особое внимание трансформации, изменению, развитию, технологическому лидерству и достижению национальных целей России. Каждая из этих целей основывается на людях, на человеческом капитале и тех условиях, в рамках которых осуществляется любая трудовая деятельность. Повестка конференции очень точно отражает основные направления работы научного сообщества: трудовое право и право социального обеспечения становятся фундаментом общественного прогресса во всех сферах жизни. Уверена, что дискуссии, которые пройдут в рамках конференции, помогут расширить теоретическую и практическую базу и найти новые пути для реализации потенциала каждого человека!»*



Приветствия в адрес конференции поступили также от Уполномоченного по правам человека в Российской Федерации Татьяны Москальковой и председателя Федерации независимых профсоюзов Российской Федерации Сергея Черногоаева.

Делегация Университета имени О.Е. Кутафина (МГЮА) приняла участие в Пермских чтениях

С 23 по 24 мая 2025 г. в Перми состоялась XII сессия базисного сателлитного проекта Пермского конгресса ученых-юристов «Пермские чтения по методологическим проблемам цивилистических исследований», посвященного памяти профессора М. Ю. Чельшева.

Мероприятие прошло при участии Общероссийской общественной организации «Ассоциация юристов России», издательства «Статут», региональной общественной организации «Пермское землячество», при сотрудничестве с Институтом государства и права РАН, Университетом имени О.Е. Кутафина (МГЮА), Уральским государственным юридическим университетом имени В. Ф. Яковлева, Казанским (Приволжским) федеральным университетом, Санкт-Петербургским государственным университетом, Саратовской государственной юридической академией.

Приветственный адрес участникам и организаторам Пермских чтений направил ректор Университета Виктор Блажеев.

Университет имени О.Е. Кутафина (МГЮА) представляли первый проректор, заведующий кафедрой предпринимательского и корпоративного права Инна Ершова, заведующий кафедрой гражданского права Евгений Вавилин, профессор



кафедры предпринимательского и корпоративного права Василий Лаптев и доцент кафедры интеллектуальных прав Елена Подрабинок.

Международное сотрудничество

Рабочий визит делегации Хэйлунцзянского университета



29 мая 2025 г. Университет с рабочим визитом посетила делегация Хэйлунцзянского университета. В ходе визита состоялась встреча ректора Университета имени О.Е. Кутафина (МГЮА) Виктора Блажеева с ректором Хэйлунцзянского университета Ван Цзинбо. Стороны определили направления развития сотрудничества в научной и образовательной сферах, обсудили возможность реализации совместных проектов.

В ходе встречи стороны подписали соглашение об академическом обмене. Оно предусматривает проведение совместных научных исследований и мероприятий, обмен преподавателями для чтения лекций, а также возможность направления выпускников Университета имени О.Е. Кутафина (МГЮА) в Хэйлунцзянский университет для получения ученой степени в Китае. Виктор Блажеев пригласил Хэйлунцзянский университет принять участие в XIII Московском инновационном юридическом форуме, который пройдет в марте 2026 г. в Москве.

Во встрече приняли участие со стороны Хэйлунцзянского университета начальник отдела международных дел Ху Сяофэн, директор Высшей школы перевода Сунь Чао, заместитель директора Института России Гун Нань, со стороны Университета имени О.Е. Кутафина (МГЮА) — проректор по стратегическому и международному развитию

Мария Мажорина, директор Центра международного сотрудничества Анна Драганова.



Встреча руководства Университета имени О.Е. Кутафина (МГЮА) с представителями Посольства Королевства Бахрейн в Российской Федерации

23 мая 2025 г. в Университете состоялась встреча представителей Посольства Королевства Бахрейн в Российской Федерации с руководством Университета имени О.Е. Кутафина (МГЮА).

Королевство Бахрейн на встрече представляли Генеральный секретарь Бахрейнского общества мониторинга прав человека, Генеральный секретарь

Европейского центра по правам человека в странах Залива Файсалем Фуляз. От Университета имени О.Е. Кутафина (МГЮА) во встрече приняли участие проректор по стратегическому и международному развитию Мария Мажорина, проректор по научно-исследовательской деятельности Владимир Синюков, заведующий кафедрой конституционного и муниципального права Игорь Дудко и директор Центра международного сотрудничества Анна Драганова.

Участники встречи обсудили вопросы сотрудничества в сфере защиты прав человека, организацию и проведение совместных мероприятий, а также обмен опытом между Россией и Королевством Бахрейн в данной области.



Мероприятия ректората

Очередное заседание Ученого совета

26 мая 2025 г. в Университете имени О.Е. Кутафина (МГЮА) состоялось очередное заседание Ученого совета. В ходе заседания были рассмотрены текущие кадровые вопросы, а также вопросы, связанные с деятельностью структурных подразделений.

В начале заседания была озвучена благодарность коллективу Университета имени О.Е. Кутафина (МГЮА) от командования и личного состава 810-й отдельной гвардейской орденов Жукова и Ушакова бригады морской пехоты за поддержку и оказанную помощь подразделениям бригады, находящимся на наиболее сложных участках фронта.

Ректор Университета Виктор Блажеев подчеркнул, что работа по поддержке участников специальной военной операции ведется непрерывно, и поблагодарил всех, кто вносит свой вклад в победу. Благодарственным письмом 810-й отдельной гвардейской орденов Жукова и Ушакова бригады морской пехоты были отдельно отмечены проректор по образовательной деятельности Наталья Софийчук, директор Института прокуратуры Сергей Перов и студент 2-го курса Института прокуратуры Матвей Кондратьев.

На заседании Ученого совета были озвучены имена студентов, проявивших наиболее активное участие в мероприятиях, организованных Библиотекой Университета имени О.Е. Кутафина (МГЮА).

Профессору кафедры финансового права Ольге Болтиновой в связи с юбилеем, а также за многолетнюю, плодотворную научно-педагогическую работу





и добросовестный труд была вручена почетная грамота Университета имени О.Е. Кутафина (МГЮА). Также за активное содействие и умелую организацию работы по общественно-политическому и духовно-нравственному просвещению гражданских служащих Федерального казначейства Ольга Болтинова была отмечена медалью Федерального казначейства «За Усердие и Пользу».

Коллектив Университета поздравил и других юбиляров месяца: профессора кафедры криминологии и уголовно-исполнительного права имени В. Е. Эминова Елену Клещину, доцента кафедры интеллектуальных прав Семена Михайлова, профессора кафедры уголовного права Эдуарда Жевлакова, профессора кафедры уголовно-процессуального права имени П. А. Лупинской Татьяну Вилкову, преподавателя кафедры практической юриспруденции Владимира Китсинга, профессора кафедры трудового права и права социального обеспечения Аллу Благодир.

Члены Ученого совета почтили минутой молчания память Станислава Ивановича Гридина — выдающегося ученого-административиста, кандидата юридических наук, доцента, полковника милиции в отставке, автора более 100 научных и учебно-методических работ.

Заседание Ученого совета продолжилось вручением дипломов кандидата юридических наук. Документы были вручены преподавателю кафедры международного частного права Наталии Карандашевой и ассистенту кафедры информационного права и цифровых технологий Сергею Соловкину.

Заместитель начальника Учебно-методического управления Александра Киселева рассказала о развитии внутренней системы качества образования, заведующий кафедрой гражданского права Евгений Вавилин выступил с отчетом о результатах деятельности кафедры, проректор по стратегическому и международному развитию Мария Мажорина представила месячный отчет о реализации программы стратегического академического лидерства «Приоритет-2030», национального проекта «Молодежь и дети». Она рассказала, что дорожная карта уже полностью

утверждена, все стратегические проекты запущены и по некоторым из них уже начали появляться результаты.

На Ученом совете были утверждены темы докторских и магистерских диссертаций — по данному вопросу выступила первый проректор Инна Ершова.



На заседании Ученого совета начальник Управления приемной комиссии и профориентационной работы Светлана Пола рассказала об изменениях в правилах приема, внесенных в соответствии с рекомендательными письмами Минобрнауки России.

Начальник Учебно-методического управления Ирина Комерова объяснила необходимость внесения изменений в положение о практической подготовке в части процедуры смены научного руководителя, в положение о выпускной квалификационной работе в части регистрации дипломных работ, а также рассказала об изменениях учебных планов по программе среднего профессионального образования в связи с рекомендациями Министерства просвещения РФ.

Проректор по образовательной деятельности Наталья Софийчук представила модель структуры институтов (филиалов) Университета имени О.Е. Кутафина (МГЮА) в части кафедр. Предполагается, что в институтах (филиалах) будут организованы пять основных кафедр: социальных и гуманитарных наук, публично-правовых наук, теоретико-исторических правовых наук, уголовно-правовых наук.

В завершение встречи ректор Университета имени О.Е. Кутафина (МГЮА) Виктор Блажеев объявил, что стартовала работа по подготовке Московского инновационного юридического форума 2026 г., и предложил желающим направлять свои идеи в адрес организационного комитета мероприятия.

АВТОРИТЕТНОЕ МНЕНИЕ



**Евгений
Александрович
РУСКЕВИЧ,**

профессор кафедры
уголовного права
Университета имени
О.Е. Кутафина (МГЮА),
доктор юридических наук,
доцент
russkevich@mail.ru
125993, Россия, г. Москва,
ул. Садовая-Кудринская, д. 9

Цифровизация уголовного законодательства: непростые последствия простых решений

Аннотация. В статье анализируются отдельные изменения Уголовного кодекса РФ, направленные на повышение эффективности противодействия преступлениям, совершаемым с использованием информационно-телекоммуникационных сетей, в том числе сети Интернет.

Автор отмечает, что цифровой способ совершения преступления далеко не всегда свидетельствует об увеличении общественной опасности деяния. Дополнение уголовного закона указанием на совершение преступления с использованием сети Интернет должно компенсировать реально сложившийся разрыв в степени общественной опасности между традиционной формой осуществления преступного посягательства и его цифровым аналогом. Неоправданная цифровая казуализация уголовного закона приводит к нарушению сложившихся моделей законодательного определения отдельных преступлений, а равно вступает в противоречие с доктринальными положениями, характеризующими содержание и пределы объективной стороны конкретных составов преступлений. Автор также отмечает отсутствие единого подхода к учету цифрового способа совершения преступления в рамках Особенной части УК РФ.

Ключевые слова: цифровая преступность, компьютерные преступления, преступления в сфере компьютерной информации, цифровизация уголовного закона

DOI: 10.17803/2311-5998.2025.129.5.026-033

Eugene A. RUSSKEVICH,

Professor of the Department of Criminal Law
of the Kutafin Moscow State Law University (MSAL),
Dr. Sci. (Law), Associate Professor
russkevich@mail.ru
9, ul. Sadovaya-Kudrinskaya, Moscow, Russia, 125993

Digitalization of Criminal Legislation: Complex Consequences of Simple Solutions

Abstract. The article analyzes certain amendments to the Criminal Code of the Russian Federation aimed at increasing the effectiveness of counteracting crimes committed using information and telecommunications networks, including the Internet.

The author notes that the virtual network method of committing a crime does not always indicate an increase in the social danger of the act. Supplementing the criminal law with an indication of the commission of a crime using the Internet should compensate for the real gap in the degree of social danger between the traditional form of committing a criminal offense and its digital analogue.

Unjustified digital casualization of the criminal law leads to a violation of the established models of legislative definition of individual crimes, and also contradicts the doctrinal provisions characterizing the content and limits of the objective side of specific crimes. The author also notes the lack of a unified approach to taking into account the digital method of committing a crime within the framework of the Special Part of the Criminal Code of the Russian Federation.

Keywords: *digital crime, computer crimes, crimes in the field of computer information, digitalization of criminal law*

В осмыслении проблемы противодействия цифровой преступности нельзя не учитывать то вполне очевидное обстоятельство, что сетевое пространство стало местом ежедневной социальной активности подавляющего большинства населения страны. Для современного человека взаимодействовать с другими в сети Интернет так же естественно, как и вступать в социальные интеракции в физическом пространстве. В этом смысле онлайн-коммуникация уже вряд ли требует какого-то особого отношения со стороны законодателя.

Это не означает, что право не должно меняться с учетом процессов цифровизации. Появление новых цифровых благ и отношений, построение цифровой экономики и т.п., конечно же, требуют необходимого правового регулирования и охраны. При этом в таких условиях само по себе запаздывание права является вполне ожидаемым. Отставание социального контроля от технологии и тех качественных изменений, которые она приносит как в общественно полезные, так и во вредоносные формы поведения человека, имеет естественные причины и в истории наблюдалось не единожды.

Вместе с тем, как можно легко убедиться, этого всегда достаточно для тревожных настроений в обществе. В последние годы почти на каждом научно-представительском мероприятии, посвященном проблемам борьбы с преступностью, докладчики знакомят слушателей с новыми угрозами и вызовами цифровизации, щедро употребляя при этом труднопроизносимые англицизмы. За иноплеменными словами, надо признать, зачастую скрываются традиционные и уже хорошо разработанные в науке уголовно-правовые конструкции, но производимый эффект от этого страдает мало — слушатели довольно часто проникаются убеждением о глубоком кризисе уголовного права и необходимости системных изменений в свете процессов цифровизации. Диссонансом этому попури из предложений криминализовать или как-то иначе отразить в тексте уголовного закона майнинг, треш-стриминг, буллинг, stalking, доксинг, хейтинг, флейминг, фишинг, кардинг, зумбомбинг и т.п. является справедливое утверждение о том, что «уголовное право не может идти впереди “телеги”, потому



что если новые отношения еще не сложились и не понятно о чем вообще идет речь, то и формулировать запрет в этой области весьма чревато»¹.

Думается, что, когда речь идет о правовом регулировании и совершенствовании механизма уголовно-правовой охраны, эмоциональные нарративы должны быть проигнорированы. Фиксируемое отставание права в условиях цифровизации само по себе не может выступать поводом для утверждения о глубоком кризисе и необходимости новых, соответствующих Индустрии 4.0 социальных регуляторов.

Нельзя упускать из виду, что довольно часто употребляемый тезис об экспоненциальном росте цифровых преступлений не свидетельствует об общем увеличении преступности. Речь идет о качественном изменении ее структуры, когда физический способ заменяется и вытесняется своим цифровым alter ego. Иными словами, самой преступности больше не становится, она просто меняется, оцифровывается.

На поверку также оказывается, что цифровизация мало что добавляет и без труда «укладывается» в содержание законодательных моделей подавляющего большинства составов преступлений. Кража не перестает быть тайным хищением чужого имущества, будучи совершенной посредством неправомерного доступа к банковскому мобильному приложению потерпевшего. Равно как и клевета, мошенничество, распространение порнографии и многие иные посягательства в своих цифровых проявлениях полностью вписываются в уже имеющиеся законодательные конструкции. Даже предполагаемая модель «убийства будущего», когда умышленное причинение смерти другому человеку будет осуществлено хакером дистанционно путем неправомерного воздействия на имплантированное устройство, полностью охватывается действующей редакцией ст. 105 УК РФ.

Дополнение уголовного закона указанием на совершение того или иного преступления цифровым способом должно либо восполнять имеющийся пробел в уголовно-правовой охране, либо компенсировать реально сложившийся разрыв в степени общественной опасности между традиционной формой осуществления преступного посягательства и его цифровым аналогом, как то, думается, справедливо реализовано в нормах об ответственности за отдельные преступления, связанные с оборотом запрещенных предметов и криминогенной пропагандой.

К сожалению, довольно часто информационный шум вокруг проблемы противодействия цифровым преступлениям, без оглядки на действительные потребности правоприменения с одновременным созданием либо укреплением в сознании населения в некотором роде мифических угроз, заглушает попытки удержать законодателя от очередного принятия решения по дополнению УК РФ очередным «цифровым аватаром» традиционного состава преступления в отсутствие четкого понимания, чем конкретно обусловлена оценка того или иного посягательства как обладающего более высокой степенью общественной опасности.

За прошедшие годы стал понятен общий подход законодателя к проблеме. Ответом на цифровое проявление преступного посягательства является корректировка соответствующей нормы уголовного закона указанием на совершение

¹ Хиллута В. В. Уголовное право в социальном измерении (контуры перемен и новой стратегии развития) : монография. М., 2023. С. 125.

деяния «с использованием информационно-телекоммуникационных сетей, в том числе сети Интернет». Таким образом, онлайн-коммуникация прочно вошла в систему средств дифференциации уголовной ответственности. Насколько обоснован этот подход, покажет, конечно же, время. Сейчас не может не настораживать то, что в условиях все ускоряющейся конвергенции физического и виртуального в жизни современного человека законодатель идет по пути принципиального разделения и последовательного ужесточения ответственности за цифровой способ совершения преступного посягательства. И уже можно обозначить и осмыслить непростые последствия таких решений в сфере цифровой модернизации уголовного закона.

Прежде всего надо сказать о том, что курс на адаптацию положений уголовного закона к процессам цифровизации сопряжен с нарушением сложившихся моделей законодательного описания отдельных преступлений. Ярким тому примером выступает действующая редакция нормы об ответственности за мошенничество в сфере компьютерной информации (ст. 159⁶ УК РФ). Компьютерное мошенничество, совершаемое путем неправомерного вмешательства в функционирование средств обработки, хранения и (или) передачи данных, при отсутствии признаков обмана или злоупотребления доверием, представляет собой юридический оксюморон, законотворческое недоразумение. Как известно, мошенничество немыслимо без обманного поведения либо злоупотребления доверительными отношениями. Если законодатель и желал выделить отдельную форму хищения, совершаемого исключительно путем модификации компьютерных данных, следует констатировать, что попытка эта до настоящего времени терпит неудачу и требует вполне конкретных решений. Здесь можно обратиться к опыту Республики Беларусь, где ответственность установлена именно за хищение путем модификации компьютерной информации (ст. 212 УК РБ)².

Помимо этого, учет цифрового способа вступает в противоречие с положениями (обоснованными в науке и поддержанными на уровне судебного толкования), раскрывающими содержание объективной стороны конкретных составов преступлений. Так, одним из последних решений законодателя по оцифровке Особенной части УК РФ явилось дополнение сразу многих ее норм указанием на квалифицирующий признак в виде совершения общественно опасного посягательства «с публичной демонстрацией, в том числе в средствах массовой информации или информационно-телекоммуникационных сетях (включая сеть Интернет)»³.

Начнем с того, что здесь, конечно же, представляет интерес не только цифровой аспект. Законодатель признал квалифицированным убийством или причинением вреда здоровью всякое умышленное применение насилия в отношении другого человека, совершенное публично, т.е., например, в общественном месте и в присутствии других лиц. Социально-правовые предпосылки ужесточения ответственности в таком случае, пожалуй, мало проявлены.

² URL: <https://pravo.by/document/?guid=3871&p0=hk9900275> (дата обращения: 17.03.2025).

³ Федеральный закон от 08.08.2024 № 218-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации» // СПС «КонсультантПлюс».



Указание на демонстрацию в сети Интернет сразу ставит вопрос о толковании пределов объективной стороны соответствующих преступлений. Если согласиться с подходом, согласно которому такое преступление надлежит считать юридически оконченным не с наступления конкретных общественно опасных последствий, а с момента публичного показа или размещения для публичного обозрения соответствующих видео- или фотоматериалов (размещение информации в общем доступе в сети Интернет, массовая рассылка по электронной почте и т.п.)⁴, то следует сделать вывод, что новые квалифицированные виды насильственных преступлений уже преодолели свою физическую природу и приобрели в некотором смысле виртуальное содержание.

Это, в свою очередь, приводит к постановке множества вопросов: образует ли признаки оконченного преступления, например, лишение жизни потерпевшего при несостоявшейся попытке размещения соответствующих материалов в сети Интернет? Что следует признавать местом и временем совершения такого преступления? Можно ли такое насильственное преступление считать длящимся? Можно ли признавать соисполнителем лицо, которое, хотя и не применяло насилие к потерпевшему, но осуществляло съемку совершения преступления или трансляцию в сети Интернет? И эти вопросы (подумать только — о «длящемся убийстве» (!)) нельзя не ставить. Но вот отвечать на них предстоит следователям и судьям, которые уже сейчас должны как-то применять закон в состоянии очередной правовой неопределенности.

Другим непростым последствием является то, что цифровая казуализация (создание «цифровых двойников» традиционных уголовно-правовых запретов) нарушает внутренние системные связи уголовного закона. Так, Федеральным законом от 30.11.2024 № 421-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации»⁵ глава 28 УК РФ была дополнена специальной нормой об ответственности за неправомерные действия в отношении персональных данных (ст. 272¹ УК РФ). Из ее содержания следует, что предметом преступления являются сведения, составляющие персональные данные гражданина, однако лишь в форме компьютерной информации. При этом диспозиция ст. 137 УК РФ приобрела ссылочный характер, поскольку была дополнена оговоркой о том, что она не распространяется на случаи, предусмотренные ст. 272¹ УК РФ.

В результате указанных изменений сложилась ситуация, при которой уголовно-правовое противодействие незаконным действиям в отношении персональных данных гражданина принципиально разделено по одному критерию — хранятся ли соответствующие сведения в цифровом или ином виде (например, на бумажном носителе). При этом разглашение персональных данных в телефонном разговоре образует преступление, предусмотренное ст. 137 УК РФ, а направление сообщения или фотографии с той же информацией в мессенджере уже подпадает под действие ст. 272¹ УК РФ.

Более того, поскольку в ст. 272¹ УК РФ установлена ответственность и за незаконное использование персональных данных в цифровой форме,

⁴ См.: *Шарапов Р. Д.* Квалификация преступлений, совершенных с использованием информационно-телекоммуникационных сетей // *Законность*. 2024. № 3. С. 33—38.

⁵ *Российская газета*. 06.12.2024. № 278.

то осуществление нежелательного телефонного звонка гражданину путем считывания с экрана компьютера номера телефона и сведений о фамилии, имени и отчестве абонента образует признаки преступления. Означает ли это, что теперь каждый нежелательный телефонный вызов от так называемых звонарей представляет собой факт совершения преступления, предусмотренного ст. 272¹ УК РФ? Если так, тогда мы на пороге «регистрационного апокалипсиса» по ст. 272¹ УК РФ, поскольку ежедневно миллионы граждан России получают такие звонки, причем многократно.

Важно отметить и то, что незаконное использование, равно как и хранение персональных данных не в компьютерной форме, уже преступлением не является. Искать научное или хотя бы логическое объяснение тому, почему сама цифровая форма персональных данных обуславливает наличие основания для реализации уголовной репрессии, пожалуй, не стоит.

И наконец, еще одним непростым последствием явилось отсутствие единого подхода к учету цифрового способа совершения преступления в Особенной части УК РФ. В стремлении адаптировать уголовный закон к условиям цифровой трансформации общественных отношений законодатель зачастую проявляет неоправданное усердие. Примером тому является норма об ответственности за незаконные действия в отношении особо охраняемых диких животных и водных биологических ресурсов (ст. 258¹ УК РФ). Статья привлекает внимание дублирующим содержанием квалифицирующих признаков совершения преступления «с использованием сети Интернет» и «с публичной демонстрацией в сети Интернет». Обращение к самой хронологии внесения изменений и изучение пояснительных записок к законопроектам⁶ позволяет сделать вывод, что появление двух самостоятельных цифровых способов совершения преступления не планировалось и явилось следствием реализации двух самостоятельных законотворческих инициатив.

Если подводить некий итог, можно заключить, что простые законодательные решения в области «оцифровки» УК РФ влекут далеко не простые последствия

⁶ См.: паспорт проекта федерального закона № 308781-7 «О внесении изменений в статьи 245 и 258¹ Уголовного кодекса Российской Федерации и статьи 150 и 151 Уголовно-процессуального кодекса Российской Федерации» (в целях усиления уголовной ответственности за жестокое обращение с животными) (внесен депутатами Государственной Думы ФС РФ О. В. Шеиным, В. В. Бурматовым, Е. Г. Драпеко, С. А. Вострецовым, К. Г. Слыщенко, И. В. Осиповым, Н. В. Маловым, А. Б. Выборным, О. Н. Смолиным, В. В. Белоусовым, О. А. Николаевым, О. А. Ниловым, С. М. Мироновым, А. Г. Аксаковым, А. В. Канаевым, А. Н. Грешневико) // СПС «КонсультантПлюс»; паспорт проекта федерального закона № 356397-7 «О внесении изменений в Уголовный кодекс Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации» (по вопросу совершенствования уголовного законодательства Российской Федерации в сфере противодействия преступлениям, связанным с незаконной добычей и оборотом водных биологических ресурсов, диких животных, в том числе занесенных в Красную книгу Российской Федерации) // СПС «КонсультантПлюс».



как для общего состояния уголовного закона, так и для правоприменения (оказывают дизруптивное воздействие на механизм уголовно-правовой охраны⁷).

Стоит, пожалуй, сказать и о том, что в этом можно усмотреть и очередную попытку неоправданно возложить на уголовный закон решение проблемы, которая требует системного и комплексного подхода. Противодействие цифровой преступности обладает той несомненной особенностью, что в его структуре в значительной степени преобладают организационно-технические либо сугубо технические составляющие. Предупреждение посягательств, совершаемых с компьютерной информацией и компонентами информационно-коммуникационной инфраструктуры, прежде всего реализуется за счет разработки и внедрения механизмов программно-технической защиты, в том числе от неосторожного поведения субъектов, допущенных к эксплуатации компьютерного оборудования, в том числе самих пользователей. В данном отношении крайне важным представляется обеспечение неукоснительного соблюдения установленных стандартов информационной безопасности в деятельности хозяйствующих субъектов. То, что далеко не все организации в силу объективных и (или) субъективных причин стремятся осуществлять свою деятельность на уровне последних стандартов киберзащищенности, — известный факт.

Надо обратить пристальное внимание на то, что изначально и по настоящее время коммерческий эффект (прибыль) от внедрения конкретного цифрового решения полностью превалирует над соображениями обеспечения информационной безопасности. Никто из хозяйствующих субъектов не желает отказываться от конкурентных преимуществ, которые дают технологии. Никто и не будет от них отказываться инициативно из соображений социальной ответственности. Винить в этом бизнес, пожалуй, не стоит. Бизнес должен заниматься своим делом и крепить тем самым отечественную экономику. Здесь разумное (минимально необходимое) участие в этом процессе должно проявить государство путем выработки общих правил и стандартов кибербезопасности для всех участников.

Немаловажно также государству озаботиться, наконец, тем, кто и с какими ресурсами будет бороться с современной цифровой преступностью, принимая во внимание уже давно возникший и усугубляющийся с каждым годом кадровый кризис в системе правоохранительных органов⁸.

Иными словами, простые решения по «цифровому декорированию» отечественного уголовного закона необходимо сменить на реальные меры по противодействию преступлениям, совершаемым с использованием информационно-коммуникационных технологий. Думается, что такой подход несколько поправит в целом тупиковый путь подгонки уголовно-правовых конструкций под те или иные проявления цифровизации, лишенный необходимых социальных, юридических и научных оснований.

⁷ См.: Русскевич Е. А. Уголовное право и «цифровая преступность»: проблемы и решения : монография. М., 2019. С. 20.

⁸ Глава МВД заявил о критической нехватке полицейских и следователей // РБК. 10.08.2023. URL: <https://www.rbc.ru/politics/10/08/2023/64d4d2629a7947695baea197?ysclid=m8dhdvh2q5607811322> (дата обращения: 10.03.2025).

Все вышеизложенное не следует расценивать как попытку обосновать ненужность любых изменений уголовного закона в условиях цифровизации. Речь идет лишь о том, что такие изменения должны иметь прочные и научно верифицированные предпосылки, носить не спонтанный, а тщательно выверенный характер. Так, например, давно уже назрела проблема надлежащего уголовно-правового ответа случаям так называемого криптовирусного вымогательства, когда злоумышленник, осуществив шифрование компьютерных данных пользователя, требует передать ему денежные средства как условие снятия блокировки доступа к компьютерной информации. Действующая редакция ст. 163 УК РФ не вполне пригодна для применения в таких случаях. Чтобы быть точным — неприменима в тех из них, где нет никаких признаков угрозы уничтожения или повреждения имущества, а равно шантажа.

И казалось бы, проблемных примеров — множество на практике, и обстоятельное обсуждение в научной литературе имеется, а воз и ныне там. Пожалуй, не хватает «хайпа» обозначенной проблеме, слишком она прагматична и даже приземленна. Куда уж ей до флейминга или зумбомбинга.

БИБЛИОГРАФИЯ

1. *Русскевич Е. А.* Уголовное право и «цифровая преступность»: проблемы и решения : монография. — М. : Инфра-М, 2019. — 227 с.
2. *Хилюта В. В.* Уголовное право в социальном измерении (контуры перемен и новой стратегии развития) : монография. — М. : Юрлитинформ, 2023. — 440 с.
3. *Шарапов Р. Д.* Квалификация преступлений, совершенных с использованием информационно-телекоммуникационных сетей // Законность. — 2024. — № 3. — С. 33—38.





**Ольга Романовна
АФАНАСЬЕВА,**
профессор кафедры криминологии
и уголовно-исполнительного права
имени Е. В. Эминова
Университета имени
О.Е. Кутафина (МГЮА),
доктор юридических наук, доцент
orafanaseva@msal.ru
125993, Россия, г. Москва,
ул. Садовая-Кудринская, д. 9



**Валентина Ивановна
ШИЯН,**
доцент кафедры
правового обеспечения
национальной безопасности,
законности и правопорядка
Российской академии народного
хозяйства и государственной
службы при Президенте РФ,
кандидат юридических наук,
доцент
valentina-shiyan@yandex.ru
119571, Россия, г. Москва,
просп. Вернадского,
д. 82, стр. 1

Киберпреступность в регионах России: современные тенденции и меры предупреждения¹

Аннотация. В статье представлены результаты исследования современных тенденций киберпреступности в федеральных округах и субъектах РФ. Авторы отмечают, что эффективное предупреждение киберпреступности требует исследования ее характеристик не только на общероссийском, но и на региональном уровне, что позволит определить специфику криминальной пораженности регионов, осуществить их ранжирование, обусловит выявление проблем обеспечения региональной безопасности в различных субъектах РФ и своевременную выработку научно обоснованных рекомендаций по совершенствованию мер, направленных на снижение криминальной пораженности регионов.

В числе основных современных тенденций киберпреступности авторы называют последовательный рост киберпреступлений как в целом по России, так и во всех ее федеральных округах на фоне общего снижения преступности; высокий уровень латентности и низкий уровень раскрываемости. Отмечается увеличение фактов участия в киберпреступности организованных преступных сообществ, увеличение материального ущерба киберпосягательств и появление новых форм угроз. Установлена выраженная территориальная дифференциация киберпреступности, обусловленная совокупным влиянием демографических, социокультурных, организационных и технологических факторов.

Ключевые слова: киберпреступность, криминогенная обстановка, регионы России, киберугрозы, состояние преступности, тенденции преступности, меры предупреждения, региональная безопасность

DOI: 10.17803/2311-5998.2025.129.5.034-047

¹ Данная статья подготовлена в рамках государственного задания РАНХиГС.

Olga R. AFANASIEVA,

*Professor of the Chair of Criminology and Executive Law Chair named after
E. V. Eminov of the Kutafin Moscow State Law University (MSAL),
Dr. Sci. (Law), Associate Professor
orafanaseva@msal.ru
9, ul. Sadovaya-Kudrinskaya, Moscow, Russia, 125993*

Valentina I. SHIYAN,

*Associate Professor at the Department of Legal Support of National Security,
Legality and Law and Order, Russian Presidential Academy of National Economy
and Public Administration,
Cand. Sci. (Law), Associate Professor
valentina-shiyan@yandex.ru
82/1, prosp. Vernadsky, Moscow, Russia, 119571*

Cybercrime in the Regions of Russia: Current Trends and Preventive Measures

Abstract. *The article presents the results of a study on current trends in cybercrime across federal districts and regions of the Russian Federation. The authors emphasize that effective prevention of cybercrime requires analyzing its characteristics not only at the national level but also at the regional level. This approach makes it possible to identify the specific features of criminal victimization in different regions, rank them accordingly, and uncover problems related to ensuring regional security across various parts of Russia. It also enables the timely development of scientifically grounded recommendations aimed at improving measures to reduce regional criminal victimization.*

Among the main contemporary trends in cybercrime, the authors highlight the steady increase in cybercrime rates both across Russia as a whole and in all federal districts, despite the overall decline in crime. Other noted trends include a high level of latency and a low detection rate. The study also notes an increase in the involvement of organized criminal groups in cybercrime, greater financial damage from cyberattacks, and the emergence of new threat forms. A pronounced territorial differentiation of cybercrime has been identified, driven by the combined influence of demographic, sociocultural, organizational, and technological factors.

Keywords: *cybercrime, criminogenic situation, regions of Russia, cyber threats, crime situation, crime trends, preventive measures, regional security*

На всех этапах развития общества обеспечение региональной безопасности входило в число приоритетных направлений в практике государственных органов и общественных институтов. Вместе с тем усиленное внимание ученых к особенностям региональной преступности началось лишь в конце XIX столетия. Однако этот процесс осуществлялся настолько стремительно и плодотворно, что уже в начале XX в. обусловил появление «региональной



криминологии» — самостоятельного направления в науке. Примечательно, что практически во всех криминологических трудах того времени при исследовании различных видов преступности особое внимание уделялось специфике криминальной пораженности каждой губернии, области и округа Российской империи, которые, как правило, дифференцировали на четыре или шесть типологических групп.

Бесспорной является актуальность региональных криминологических исследований, которые в большинстве своем имеют лонгитюдный характер. Результаты подобных изысканий способствуют прежде всего своевременному выявлению криминальных угроз, изучению факторов преступности и учету особенностей их проявления в конкретном регионе, а также осуществлению криминологической классификации и ранжированию регионов, определению закономерностей и специфики видов преступности в них либо фиксации ее эмерджентного характера.

В современном мире геополитическая нестабильность, многочисленные угрозы военно-политического характера, широкое использование новейших информационно-телекоммуникационных технологий во всех сферах общественной жизни, в том числе и криминальной, совершенствование новых технологий цифровизации и роботизации, интеллектуальные системы безопасности и управления обусловили появление и последовательный рост киберпреступлений во всех государствах мира.

Исходя из канонов криминологии, под киберпреступностью целесообразно понимать совокупность киберпреступлений и лиц, их совершивших, на определенной территории, за определенный период времени.

Самая лаконичная дефиниция киберпреступления содержится в Модельном законе о противодействии киберпреступности, принятом на 55-м пленарном заседании Межпарламентской Ассамблеи государств — участников Содружества Независимых Государств (постановление № 55-20 от 14.04.2023): «Киберпреступление — преступление, совершенное в киберпространстве» (ст. 2).

Полный перечень киберпреступлений представлен в указании Генпрокуратуры России и МВД России от 27.12.2024 № 952/11/3 «О введении в действие перечней статей Уголовного кодекса Российской Федерации, используемых при формировании статистической отчетности». Содержание данного нормативного правового акта наглядно свидетельствует, что киберпреступления не ограничены рамками главы 28 «Преступления в сфере компьютерной информации», а выходят далеко за ее пределы.

Рост цифровизации российского общества сопровождается резким увеличением количества и сложности киберпреступлений. Так, в 2024 г. было зарегистрировано 765 365 преступлений², совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации (киберпреступлений), что на 13,1 % выше показателя 2023 г. и в 2,59 раза больше значения 2019 г. (всего — 294 409 киберпреступлений). При

² Сводные отчеты по России «Сведения о состоянии преступности и результатах расследования преступлений» за 2019—2024 гг. ФКУ «Главный информационно-аналитический центр» Министерства внутренних дел РФ.

этом было выявлено 98 088 лиц, их совершивших, что ниже показателя 2023 г. на 6,6 % (рис. 1).



Рис. 1. Динамика количества зарегистрированных киберпреступлений и числа выявленных лиц в Российской Федерации в 2019—2024 гг.

Тенденция роста киберпреступлений наблюдается во всех федеральных округах Российской Федерации, при этом наибольшие темпы прироста, превышающие среднероссийское значение, отмечаются в Дальневосточном (+25,9 %), Приволжском (+20,6 %), Северо-Кавказском (+18,1 %) и Южном (+16,2 %) федеральных округах (рис. 2).



Рис. 2. Динамика зарегистрированных киберпреступлений в федеральных округах Российской Федерации в 2019—2024 гг.

Особенностью территориального распределения преступности в 2024 г. выступает то, что более половины всех зарегистрированных киберпреступлений



приходятся на три федеральных округа (58,7 %) и на 17 субъектов РФ (50,2 %), входящих в различные федеральные округа России (см. рис. 3, табл. 1).



Рис. 3. Киберпреступность в Федеральных округах России в 2024 г.

Таблица 1

Субъекты Российской Федерации, в которых зарегистрировано наибольшее количество киберпреступлений в 2024 г.

№ п/п	Российская Федерация и ее субъекты	Федеральный округ РФ	Количество зарегистрированных преступлений	Удельный вес, %	Удельный вес (с нарастающим итогом), %
	Россия		765 365	100	100
1	Москва	ЦФО	63 621	8,3	8,3
2	Краснодарский край	ЮФО	33 489	4,4	12,7
3	Республика Татарстан	ПФО	32 073	4,2	16,9
4	Санкт-Петербург	СЗФО	29 783	3,9	20,8
5	Республика Башкортостан	ПФО	23 823	3,1	23,9
6	Челябинская область	УФО	21 793	2,8	26,7
7	Московская область	ЦФО	19 673	2,6	29,3
8	Пермский край	ПФО	19 396	2,5	31,8

№ п/п	Российская Федерация и ее субъекты	Федеральный округ РФ	Количество зарегистрированных преступлений	Удельный вес, %	Удельный вес (с нарастающим итогом), %
9	Красноярский край	СФО	18 055	2,4	34,2
10	Ростовская область	ЮФО	17 941	2,3	36,5
11	Свердловская область	УФО	17 419	2,3	38,8
12	Самарская область	ПФО	16 868	2,2	41,0
13	Волгоградская область	ЮФО	14 396	1,9	42,9
14	Ханты-Мансийский автономный округ	УФО	14 283	1,9	44,8
15	Алтайский край	СФО	14 236	1,9	46,6
16	Нижегородская область	ПФО	13 654	1,8	48,4
17	Новосибирская область	СФО	13 454	1,8	50,2

Несмотря на сохраняющуюся общероссийскую тенденцию к росту количества зарегистрированных преступлений в сфере информационных технологий, в отдельных регионах наблюдаются признаки обратной динамики. Так, в десяти субъектах РФ в 2024 г. зафиксировано снижение числа киберпреступлений (табл. 2). Вместе с тем данное сокращение не свидетельствует об ослаблении киберугроз как таковых. Наоборот, в ряде случаев наблюдается рост степени их общественной опасности, выраженный в увеличении размера причиненного материального ущерба. Так, по данным МВД по Республике Коми, несмотря на сокращение количества зарегистрированных преступлений в сфере кибербезопасности на 20,6 %, совокупный ущерб от них возрос на 17 % и превысил 1,3 млрд рублей³. Это может свидетельствовать как о смещении фокуса киберпреступной активности в сторону более сложных, целенаправленных схем, характеризующихся высокой эффективностью и значительными экономическими последствиями, так и о деятельности правоохранительных органов по выявлению и расследованию подобных фактов преступной активности.

³ Доклад руководителя МВД Коми за 2024 год // URL: <https://uhta.bezformata.com/listnews/koми-za-2024-god/144219358/> (дата обращения: 29.03.2025).



Таблица 2

**Субъекты Российской Федерации,
в которых зафиксировано снижение количества
зарегистрированных киберпреступлений в 2024 г.**

№ п/п	Субъекты РФ	Всего	Абсолютный прирост	Темп прироста, %
1	Челябинская область	—	–936	–4,1
2	Новосибирская область	13 454	–943	–6,5
3	Кемеровская область	12 923	–670	–4,9
4	Воронежская область	9 324	–376	–3,9
5	Ленинградская область	8 071	–568	–6,6
6	Ярославская область	6 166	–365	–5,6
7	Республика Коми	5 068	–1315	–20,6
8	Смоленская область	4 990	–368	–6,9
9	Ямало-Ненецкий автономный округ	3 307	–551	–14,3
10	Орловская область	3 241	–18	–0,6

В большинстве субъектов Российской Федерации наблюдается нарастание преступной активности в сфере использования информационно-телекоммуникационных технологий или компьютерной информации. В частности, в 50 регионах страны темпы относительного прироста числа зарегистрированных преступлений, совершенных с использованием информационно-телекоммуникационных технологий, превысили среднероссийский показатель. Наиболее выраженная динамика зафиксирована в республиках Южного и Северо-Кавказского федеральных округов, а также в отдельных регионах Приволжья и Сибири.

Так, наибольшие темпы прироста в 2024 г. отмечаются в Чеченской Республике (+154,8 %), Республике Мордовия (+76,7 %), Республике Марий Эл (+67,1 %), Республике Адыгея (+60,6 %), Карачаево-Черкесской Республике (+59,7 %), Республике Дагестан (+57,3 %), Ханты-Мансийском автономном округе (+54,7 %), Республике Северная Осетия — Алания (+49,5 %), Еврейской автономной области (+43,5 %) и Псковской области (+42,0 %) (рис. 4).

Такие показатели могут свидетельствовать как о реальном росте преступной активности в указанных субъектах РФ, так и о повышении эффективности работы правоохранительных органов по выявлению киберпреступлений. Кроме того, данные тенденции требуют отдельного анализа с точки зрения факторов цифрового развития регионов, уровня интернет-проникновения и степени правовой осведомленности населения.

По итогам 2024 г. уровень криминальной нагрузки, обусловленный киберпреступностью, в Российской Федерации составил 523,68 преступления на 100 тыс. населения. Указанный показатель превышает значение 2023 г. на 13,27 % и в 2,6 раза превосходит уровневое значение 2019 г. Рост уровня киберпреступности отмечается во всех федеральных округах. Наибольшие значения уровня



*Рис. 4. Субъекты Российской Федерации
с наибольшими темпами прироста киберпреступности в 2024 г.*



*Рис. 5. Динамика уровня киберпреступности и коэффициента криминальной активности
населения в Российской Федерации в 2019—2024 гг. (на 100 тыс. населения)*

преступности, превышающие среднероссийский показатель, отмечены в Дальневосточном (623,7), Приволжском (622,8), Уральском (587,1), Северо-Западном (596,2) и Сибирском (575,9) федеральных округах (рис. 5, 6).

В 48 субъектах РФ уровень преступности превышает общероссийский, при этом в Ненецком автономном округе он выше общероссийского в два раза (1068,11 на 100 тыс. населения), в связи с чем данный регион отнесен к числу регионов с худшей криминальной ситуацией в сфере киберпреступности.

Столь высокий показатель уровня киберпреступности объясняется географической удаленностью и ограниченной доступностью традиционных форм финансового и потребительского обслуживания, высокой цифровой активностью населения, включая широкое распространение онлайн-сервисов, что, в свою очередь,



Рис. 6. Уровень киберпреступлений в федеральных округах в 2024 г. (на 100 тыс. населения)

расширяет потенциальные возможности для совершения киберпреступлений. Так, в 2024 г. в Ненецком АО уровень киберпреступлений составил (далее приведены данные на 100 тыс. населения):

- с использованием компьютеров — 423,93 преступления при среднероссийском показателе 28,97;
- с использованием сети Интернет — 1 006,54 преступления при среднероссийском показателе 444,1;
- с использованием средств мобильной связи — 532,87 преступления при среднероссийском показателе 236,76 преступления.

Негативное влияние на состояние киберпреступности может оказывать также недостаточная оснащенность правоохранительных органов региона специализированными техническими и кадровыми ресурсами для оперативного выявления и пресечения преступлений в цифровой среде.

Шесть регионов (Республика Марий Эл (977,53), Республика Карелия (952,17), Томская область (923,53), Новгородская область (907,69), Республика Удмуртия (888,43) и Кировская область (870,4)) образуют группу с высоким уровнем киберпреступности. Высокие показатели коэффициента киберпреступности, зафиксированные в таких субъектах РФ, требуют комплексного анализа с учетом социально-экономических, демографических, организационных и технологических факторов. Между тем возможно предположить, что одной из причин высокого уровня регистрируемых киберпреступлений является активное распространение цифровых технологий в условиях слабой цифровой гигиены и недостаточной правовой грамотности населения. Кроме того, в таких регионах, как Республика Удмуртия и Томская область, функционируют крупные промышленные и образовательные центры, что обеспечивает высокий уровень интернет-активности и широкой вовлеченности населения в дистанционные формы занятости, обучения и потребления.

Отмеченные значения уровня преступности могут быть следствием высокой активности органов внутренних дел по выявлению и регистрации киберпреступлений, в том числе благодаря функционированию специализированных подразделений в региональных управлениях МВД России.

В группу регионов с уровнем преступности выше среднего входят десять субъектов РФ: Мурманская область (837,7), Ханты-Мансийский автономный округ (811,82), Республики Татарстан (801,22) и Мордовия (798,28), Архангельская область (796,57), Пермский край (777,31), Амурская область (760,71), Еврейская автономная область (737,3), Псковская область (726,67) и Республика Коми (703,3).

61 субъект РФ образует группу регионов со средним уровнем киберпреступности. Это преимущественно субъекты РФ, входящие в состав Центрального, Приволжского, Северо-Западного и Южного федеральных округов.

Группу регионов с коэффициентом преступности ниже среднего значения составляют четыре субъекта РФ: Кабардино-Балкарская Республика (317,4), Рязанская область (286,4), Республика Тыва (271,7) и Московская область (227,4).

К регионам с низким коэффициентом преступности отнесены Республики Ингушетия (82,1), Дагестан (64,6) и Чеченская (27,6). Между тем в 2024 г. в Чеченской Республике отмечается наибольший темп прироста киберпреступности. Сложившаяся криминальная ситуация, существенно отличающаяся от среднероссийских значений, может быть интерпретирована посредством анализа влияния демографических, социокультурных и институциональных факторов.

Прежде всего необходимо учитывать ограниченный уровень цифровизации и относительно низкую вовлеченность населения данных регионов в электронную коммерцию, онлайн-сервисы и дистанционные формы социальной активности. Несмотря на активное развитие инфраструктуры связи, в отмеченных республиках сохраняются низкие показатели охвата населения Интернетом по сравнению с другими субъектами РФ, особенно в сельских и горных районах регионов. Это объективно снижает как потенциальную вовлеченность в цифровую среду, так и возможности для реализации преступных схем с использованием информационных технологий.

На состояние преступности оказывают влияние также социокультурные особенности и высокая степень семейной и общинной сплоченности, характерная для республик Северного Кавказа. В таких условиях преступления, особенно в отношении местных жителей, зачастую регулируются внеформальными механизмами социальной регуляции, что, безусловно, сказывается на показателях регистрируемой преступности.

О повышенной степени общественной опасности киберпреступлений свидетельствует широкое использование информационно-телекоммуникационных технологий в деятельности организованных групп, преступных сообществ (преступных организаций), что позволяет говорить о ее наукоемкости. По итогам 2024 г. только число преступлений в сфере компьютерной информации, совершенных организованными группами или преступными сообществами (преступными организациями), увеличилось в 9,5 раза, прирост составил +853,8 %.

Все чаще достижения научно-технического прогресса применяются при совершении преступлений экономической направленности, преступлений террористического характера, в сфере незаконного оборота наркотиков.



Глобализация информационных процессов обусловила появление новых форм терроризма и экстремизма — кибертерроризма и киберэкстремизма.

Отметим, что данные официальной статистики не отражают реальное состояние киберпреступлений, поскольку исследуемый вид преступности продолжает оставаться высоклатентным. По мнению экспертов, этот показатель составляет от 60 % и даже более⁴.

Думается, что латентизация киберпреступлений обусловлена анонимностью интернет-пользователей, т.е. возможностью создавать скрытые ресурсы на псевдодоменах, транснациональным характером, скоротечностью, отсутствием материальных следов и другими обстоятельствами. В результате латентности и низкой раскрываемости (в 2024 г. было раскрыто 23,2 % киберпреступлений, в 2023 г. — 26,6 %) невозможно говорить о надлежащей реализации принципа неотвратимой ответственности и эффективной деятельности по предупреждению этого вида преступлений.

В криминологической науке традиционно низкую раскрываемость связывают с латентным характером киберпреступлений. Справедливости ради необходимо отметить, что на уровне ряда регионов раскрываемость киберпреступлений выше общероссийского показателя. В частности, в Республике Дагестан раскрываемость в 2024 г. составляла 48,6 %, в Свердловской области — 37,6 %, в Республике Ингушетия — 36,8 %, в Чеченской Республике — 34,0 %, в Рязанской области — 32,9 %, в Тамбовской области — 32,3 %, в Брянской области — 32,2 %, в Кемеровской области — Кузбассе — 31,7 %, в Московской области — 31,3 %, в Кабардино-Балкарской Республике — 31,1 %.

Соответственно, в указанных субъектах РФ в большинстве случаев растет количество лиц, выявленных за совершение киберпреступлений, и отмечается увеличение уровня (коэффициента) исследуемого вида преступности.

Например, в 2024 г. по сравнению с 2023 г. на территории Республики Дагестан раскрываемость киберпреступлений повысилась на 0,3 %, уровень (коэффициент) — на 23,2, темпы прироста количества лиц, выявленных за совершение киберпреступлений, увеличились на 46,2 %. Высокая раскрываемость обусловила рост последних двух показателей в Московской области, соответственно, на 33,7 и 4,2 %, в Чеченской Республике — на 16,0 и 123,3 %.

Самое низкое значение раскрываемости киберпреступлений зарегистрировано в Ненецком автономном округе — 9,6 %.

⁴ См., например: Латентность киберпреступности превысила 60 % — Сидоренко // РАПСИ — Российское агентство правовой и судебной информации. URL: https://rapsinews.ru/digital_law_news/20240424/309839280.html (дата обращения: 29.03.2025) ; Линников А. С. Экономические последствия расширения масштабов киберпреступности в России и мире // Банковское право. 2017. № 5. С. 19—29 ; Бойко О. А., Унукович А. С. Детерминанты латентных преступлений, совершаемых с использованием информационно-коммуникационных технологий // Юридический вестник Самарского университета. 2020. Т. 6. № 3. С. 53—59 ; Ki Hong (Steve) Chon. Cybercrime Precursors: Towards a Model of Offender Resources // The Australian National University Journal. 2018. № 1. P. 66—81.

В качестве сравнения обозначим, что раскрываемость преступлений экономической направленности зафиксирована на отметке 80,9 %, экстремистской направленности — 92,7 %, коррупционной направленности — 97,2 %.

Результаты проведенного исследования позволяют констатировать, что в целях обеспечения региональной безопасности осуществляется реализация комплекса следующих мер. В соответствии с поручением Президента России В. В. Путина ФСБ России и МВД России были разработаны дополнительные меры по блокировке телефонных вызовов, осуществляемых с территорий Украины и других недружественных иностранных государств в преступных целях, а также иные необходимые меры по защите прав и законных интересов граждан Российской Федерации от преступных посягательств, совершаемых с использованием современных информационно-коммуникационных технологий⁵. В результате значительно сократилось количество мошеннических звонков россиянам⁶.

Распоряжением Правительства РФ от 30.12.2024 № 4154-р была утверждена Концепция государственной системы противодействия противоправным деяниям, совершаемым с использованием информационно-коммуникационных технологий. Настоящий документ определяет принципы, цели, задачи и функции государственной системы противодействия противоправным деяниям, совершаемым с использованием информационно-коммуникационных технологий, а также нормативно-правовое, научно-техническое, информационно-аналитическое, кадровое, организационно-штатное и финансовое обеспечение ее создания и функционирования.

Особый акцент сделан на создании государственной системы противодействия киберпреступлениям, на взаимодействии федеральных государственных органов и органов государственной власти субъектов РФ, Центрального банка РФ, финансовых и иных организаций в сфере противодействия киберпреступности, на прогнозировании и выявлении противоправных деяний, совершенствовании инструментов и механизмов противодействия киберпреступлениям, развитии цифровой грамотности населения, правосознания граждан, на укреплении международного сотрудничества и др.

К сожалению, указанная Концепция не имеет нормативного характера, поскольку в соответствии со ст. 5 Федерального конституционного закона от 06.11.2020 № 4-ФКЗ «О Правительстве Российской Федерации» «акты Правительства Российской Федерации, имеющие нормативный характер, издаются в форме постановлений Правительства Российской Федерации. Акты по оперативным и другим текущим вопросам, не имеющие нормативного характера, издаются в форме распоряжений Правительства Российской Федерации».

Особое внимание уделяется укреплению кадрового потенциала подразделений, осуществляющих противодействие киберпреступности, их обучению и переподготовке, которые проводятся на базе Краснодарского университета МВД

⁵ Перечень поручений по итогам заседания Совета по развитию гражданского общества и правам человека (утв. Президентом РФ 14.01.2024 № Пр-64) // URL: <http://www.kremlin.ru/acts/assignments/orders/73277> (дата обращения: 10.03.2025).

⁶ Сбёр: число звонков мошенников россиянам удалось уменьшить до 6—7 млн в сутки // URL: <https://tass.ru/ekonomika/21775745> (дата обращения: 10.03.2025).



России (создан профильный факультет) и Московского университета МВД России имени В. Я. Кикотя (создана профильная кафедра).

Учитывая современные тенденции киберпреступности, можно констатировать, что, несмотря на принимаемые превентивные меры, повышение эффективности деятельности органов внутренних дел в рассматриваемой сфере, говорить о полной результативности и достаточности пока не приходится.

Проведенное исследование позволяет заключить, что киберпреступность в Российской Федерации в период с 2019 по 2024 г. демонстрирует устойчивую тенденцию к росту при низких значениях выявляемости виновных лиц и раскрываемости преступности. При этом киберпреступность охватывает все федеральные округа, проявляясь с разной степенью интенсивности на уровне субъектов РФ. Установлена выраженная территориальная дифференциация уровня киберпреступности, обусловленная совокупным влиянием демографических, социокультурных, организационных и технологических факторов.

Характерной особенностью современного этапа является не только количественный рост зарегистрированных преступлений, совершенных с использованием информационно-телекоммуникационных технологий, но и повышение их качественной сложности, наукоемкости и степени общественной опасности. Это проявляется в усилении участия организованных преступных сообществ, возрастании финансовых последствий киберпосягательств и появлении новых форм угроз, таких как кибертерроризм и киберэкстремизм.

Особую озабоченность вызывает высокая латентность и низкий уровень раскрываемости киберпреступлений (менее 25 %), что указывает на сохраняющуюся неэффективность существующих механизмов уголовно-правового реагирования и превентивной деятельности. Вместе с тем зафиксированы отдельные позитивные сдвиги, выражающиеся в разработке государственной концепции противодействия преступлениям в ИКТ-среде, росте кадрового обеспечения и развитии цифровой грамотности населения.

Однако, учитывая отсутствие нормативного характера утвержденных стратегических документов и сохраняющиеся пробелы в межведомственном взаимодействии, можно заключить, что предпринимаемые меры по предупреждению киберпреступности на текущем этапе являются недостаточно эффективными, что требует комплексной корректировки подходов как на федеральном, так и региональном уровне.

БИБЛИОГРАФИЯ

1. Бойко О. А., Унукович А. С. Детерминанты латентных преступлений, совершаемых с использованием информационно-коммуникационных технологий // Юридический вестник Самарского университета. — 2020. — Т. 6. — № 3. — С. 53—59.
2. Доклад руководителя МВД Коми за 2024 год // URL: <https://uhta.bezformata.com/listnews/komi-za-2024-god/144219358/> (дата обращения: 29.03.2025).

3. Латентность киберпреступности превысила 60 % — Сидоренко // РАПСИ — Российское агентство правовой и судебной информации. URL: https://rapsinews.ru/digital_law_news/20240424/309839280.html (дата обращения: 29.03.2025).
4. *Линников А. С.* Экономические последствия расширения масштабов киберпреступности в России и мире // Банковское право. — 2017. — № 5. — С. 19—29.
5. Сбер: число звонков мошенников россиянам удалось уменьшить до 6—7 млн в сутки // URL: <https://tass.ru/ekonomika/21775745> (дата обращения: 10.03.2025).
6. *Ki Hong (Steve) Chon.* Cybercrime Precursors: Towards a Model of Offender Resources // The Australian National University Journal. — 2018. — № 1. — P. 66—81.

Уголовно-правовое противодействие преступлениям в сфере информационных технологий



Компьютерные преступления: вопросы юридической техники

Аннотация. Статьи действующего УК РФ, предусматривающие уголовную ответственность за компьютерные преступления, не совершенны как в контексте юридической техники, так и в смысле уголовной политики. Признаки преступлений определены казуистично, что существенно усложняет применение закона. Последствия преступлений определены без учета их объекта и причиняемого этими преступлениями вреда. Понятие неправомерности содеянного не раскрыто в законе, на практике также нет единообразия в его понимании, что влечет необоснованное расширение репрессии. При этом люди не осознают преступности содеянного, что негативно в контексте уголовной политики. Предложены изменения в действующий уголовный закон: составы преступлений сконструировать как формальные; определить неправомерность доступа к компьютерной информации как доступ к ней без разрешения хозяина компьютера; определить вредоносность компьютерной программы как предназначение для неразрешенного внесения изменений в информацию в чужом компьютере.

Ключевые слова: уголовное право; юридическая техника; уголовная политика; анония; компьютерные преступления; неправомерный доступ к компьютерной информации; вредоносные программы

**Иван Анатольевич
КЛЕПИЦКИЙ,**
профессор кафедры
уголовного права
Университета имени
О.Е. Кутафина (МГЮА),
доктор юридических наук,
профессор
iaklepitskij@msal.ru
125993, Россия, г. Москва,
ул. Садовая-Кудринская, д. 9

DOI: 10.17803/2311-5998.2025.129.5.048-057

Ivan A. KLEPITSKIJ,

*Professor of the Department of Criminal Law
of the Kutafin Moscow State Law University (MSAL),*

Dr. Sci. (Law), Professor

iaklepitskij@msal.ru

9, ul. Sadovaya-Kudrinskaya, Moscow, Russia, 125993

Computer Crimes: Legal Technique Issues

Abstract. *The articles of the Criminal Code of the Russian Federation that provide for criminal liability for computer crimes are imperfect both in the context of legal technique and in terms of criminal policy. The elements of crimes are defined casuistically, which significantly complicates the application of the law. The consequences of crimes are defined without taking into account the social values protected by law and the harm caused by these crimes. The definition of the illegality of the act is not disclosed in the law, in practice there is also no uniformity in its interpretation, which results in an unjustified expansion of repression. People do not realize the criminality of their actions, which is negative in the context of criminal policy. Changes to the current criminal law are proposed: to construct the elements of crimes as formal (conduct crimes); to define the illegality of access to computer information as access to it without the permission of the computer owner; to define the harmfulness of a computer program as the purpose of making unauthorized changes to information on a computer belonging to another person.*

Keywords: *criminal law; legal technique; criminal policy; anomie; computer crimes; unauthorized access to computer information; virus programs*

В середине 90-х гг. прошлого века во время разработки проекта действующего Уголовного кодекса в России был небольшой опыт моделирования законодательства о компьютерных преступлениях. Сама необходимость в особых нормах о компьютерных преступлениях была под вопросом, к примеру, считалось, что норма о хищении охватывает все возможные формы хищений, поэтому потребность относительно нормы о компьютерном мошенничестве отсутствует, в результате в первой редакции действующего УК РФ такой нормы не было. Сомнения относительно социальной обусловленности норм о компьютерных преступлениях побудили законодателя к конструированию материальных составов компьютерных преступлений, при этом неверное понимание объекта этих преступлений имело следствием казуистичное и небесспорное определение последствий.

Федеральным законом от 7 декабря 2011 г. № 420-ФЗ¹ нормы о компьютерных преступлениях были изложены в новой редакции, но эта редакция мало отличалась от старой, из закона исчезло упоминание электронно-вычислительной машины (ЭВМ), было дано законодательное определение компьютерной информации. Также были дополнены квалифицирующие признаки (крупный ущерб, корыстный

¹ СЗ РФ. 2011. № 50. Ст. 7362.



мотив, тяжкие последствия и угроза их наступления), соответственно, наказание стало более строгим. Дальнейшая эволюция норм о компьютерных преступлениях выразилась в криминализации Федеральным законом от 29 ноября 2012 г. № 207-ФЗ² компьютерного мошенничества. Федеральным законом от 26 июля 2017 г. № 194-ФЗ³ усилено наказание за посягательства на критическую информационную инфраструктуру России (ст. 274¹ УК РФ). Федеральным законом от 23 апреля 2018 г. № 111-ФЗ⁴ изложена в новой редакции норма о мошенничестве с использованием электронных средств платежа (ст. 159³ УК РФ), тем же законом в норму о краже добавлен квалифицирующий признак «кража... с банковского счета, а равно в отношении электронных денежных средств» (п. «г» ч. 3 ст. 158 УК РФ), усилено наказание за компьютерное мошенничество. Федеральным законом от 14 июля 2022 г. № 260-ФЗ⁵ защищена система противодействия угрозам функционированию в России сети Интернет и сети связи общего пользования (ст. 274² УК РФ). Федеральным законом от 30 ноября 2024 г. № 421-ФЗ⁶ введена уголовная ответственность за незаконный оборот компьютерной информации, содержащей персональные данные.

Обобщив развитие российского законодательства о компьютерных преступлениях, можно отметить тенденцию к усилению наказаний, можно также упомянуть о появлении новых норм о компьютерном преступлении против порядка управления (в части защиты системы противодействия угрозам функционированию сетей) и о защите персональных данных. В течение последнего десятилетия появились и новые проблемы, в законе не отраженные, связанные с правовой охраной прав и законных интересов относительно различных виртуальных ценностей, начиная с криптовалют и заканчивая предметами компьютерных игр. В целом тенденции эти разумны и предсказуемы, проблемы решаемы. Но остаются нерешенными проблемы с юридической техникой, изначально заложенные в ранних редакциях действующего УК РФ. Более того, проблемы эти воспроизводятся в новых законах.

Ключевым понятием для норм о компьютерных преступлениях является «компьютерная информация», воздействуя на которую, лицо совершает преступление. В первоначальной редакции ст. 272 УК РФ речь шла об «информации на машинном носителе, в... ЭВМ, системе ЭВМ или их сети». В действующем законе под компьютерной информацией «понимаются сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи» (п. 1 примечаний к ст. 272 УК РФ). Первоначальная редакция рождала сомнения относительно понимания в качестве компьютерной информации любой информации на машинном носителе, проблема это решалась путем понимания машинного носителя как предназначенного для ЭВМ. В итоге было ясно, что информация на диске или жестком диске, предназначенных для работы с ЭВМ, — это компьютерная информация, неправомерный доступ к которой уголовно наказуем. В то же время незаконное пользование чужой стиральной

² СЗ РФ. 2012. № 49. Ст. 6752.

³ СЗ РФ. 2017. № 31 (ч. I). Ст. 4743.

⁴ СЗ РФ. 2018. № 18. Ст. 2581.

⁵ СЗ РФ. 2022. № 29 (ч. II). Ст. 5227.

⁶ СЗ РФ. 2024. № 49 (ч. IV). Ст. 7412.

машиной, радио или телевизором, хотя и может быть предосудительным, но не образует состава преступления, предусмотренного ст. 272 УК РФ. В действующей редакции закона такой вывод сделать уже затруднительно, поскольку компьютерной признается любая информация, «представленная в форме электрических сигналов». Это определение изначально неверное, так как, с одной стороны, компьютерная информация представлена не в форме электрических сигналов, а в виде их записи в разных формах на разных носителях (магнитных, оптических и иных). Отключение электричества не влечет утрату компьютерной информации. С другой стороны, в форме электрических сигналов информация обрабатывается не только в компьютере, но почти в любом электронном устройстве, например в калькуляторе, стиральной машине, радио, телевизоре, хлебопечке⁷. В мозге человека и животных информация также обрабатывается в форме электрических сигналов, что было известно нейробиологу Ч. С. Шеррингтону уже в XIX веке⁸. Если узкий специалист в области компьютерных технологий вправе не знать этого, то законодатель не может позволить себе такую узость познаний в определении признаков преступления. Ввиду отсутствия пригодного для практики легального понятия компьютерной информации правильным представляется руководствоваться здравым смыслом и исходить из того, что компьютерной является информация, существующая на технических носителях, специально предназначенных для ввода и обработки информации в ЭВМ. Законодатель уже движется в этом направлении, вновь упомянув ЭВМ в ч. 6 ст. 272¹ УК РФ, введенной Федеральным законом от 30 ноября 2024 г. № 421-ФЗ. Норма эта казуистична в определении предмета преступления, но казуистичность объясняется несовершенством имеющегося обобщенного понятия.

Для правильного понимания компьютерной информации нужно уяснить объект преступлений, предусмотренных гл. 28 УК РФ. В конце прошлого века в связи с внедрением компьютерных технологий в разные отрасли общественной жизни появился новый компонент общественной безопасности — компьютерная безопасность. Неправомерное вторжение в работу систем, использующих такие технологии, чревато серьезными угрозами для человека, общества и государства. В результате такого вторжения серьезные риски создаются для неприкосновенности частной жизни, для имущественных прав и интересов, для безопасности транспорта и связи, для иных требующих уголовно-правовой охраны частных, общественных и государственных интересов. В наше время человек доверил компьютерам много рутинной работы, в результате жизнь человека стала комфортнее, многие полезные системы стали работать быстрее, эффективнее и даже

⁷ Поэтому и определение, данное в п. 2 постановления Пленума Верховного Суда РФ от 15 декабря 2022 г. № 37 «О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть Интернет» представляется слишком широким: «...к числу компьютерных устройств могут быть отнесены любые электронные устройства, способные выполнять функции по приему, обработке, хранению и передаче информации, закодированной в форме электрических сигналов».

⁸ См.: Шеперд Г. Нейробиология : в 2 т. М., 1987. Т. 1. С. 105 и след.



безопаснее. Но эффективность и безопасность зависят от соблюдения людьми определенных правил, что и объясняет криминализацию неправомерного воздействия на компьютерную информацию.

При этом кажущаяся сложность информационных технологий влечет неоправданную казуистичность в определении объективных признаков компьютерных преступлений. Так, альтернативный обману способ хищения при компьютерном мошенничестве определяется в законе как «ввод, удаление, блокирование, модификация компьютерной информации либо иное вмешательство в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей» (ст. 159⁶ УК РФ). На самом деле мошенничество — это корыстное имущественное преступление. Потребность в криминализации компьютерного мошенничества возникла в связи с тем, что компьютер заменил человека в принятии технических решений относительно передачи имущества, что прежде всего относится к банковским технологиям, распоряжению денежными средствами на счетах в банках. До реформы 2012 г. к компьютерным мошенничествам применялась норма об обычном мошенничестве, при этом обман трактовался очень широко, на грани аналогии, в уголовном праве запрещенной. На деле есть только один способ «обмануть» компьютер и фальсифицировать решение о передаче имущества — нужно идентифицироваться (правомерно или ложно) от имени клиента или работника (менеджера, кассира-операциониста, технического специалиста) финансовой или иной организации и провести операцию. Для этого вполне достаточно ввода информации, всю прочую работу выполнит компьютер. Правильно было бы указать, что ввод этот должен быть неправомерным, или в целом обобщить способ хищения как «неправомерное воздействие на компьютерную информацию». При этом, даже если идентификация честная, например, ворует сотрудник банка, используя свой доступ к информации, воздействие на информацию будет неправомерным уже в силу того, что оно нарушает имущественное право потерпевшего⁹.

Не менее казуистично определяются и последствия компьютерных преступлений. Так, описание способа компьютерного мошенничества заимствовано в норме о неправомерном доступе к компьютерной информации (ст. 272 УК РФ), где «уничтожение, блокирование, модификация и копирование информации» описаны не в качестве способа, а в качестве последствий. Там широкое определение последствий в отличие от компьютерного мошенничества можно было бы считать оправданным, поскольку это преступление не имущественное, а посягательство на общественную безопасность. Но являются ли «уничтожение, блокирование, модификация и копирование информации» вредным последствием, или это неоправданно сложное описание деяния? Второй вариант представляется в большей мере соответствующим действительности, причем это казуистичное описание с претензией на наукообразность неточное. Так, «модификация» информации — термин не технический, а юридический. В гражданском праве различают модификацию и адаптацию программного обеспечения (ст. 1270 ГК

⁹ См.: *Щепельков В. Ф.* О квалификации преступлений в сфере компьютерной информации (в свете разъяснений Пленума Верховного Суда РФ) // Уголовное право. 2023. № 6. С. 70—79.

РФ). Исключительное право на модификацию (переработку) программы имеет правообладатель, предоставивший лицензию. Адаптацию же программы, ее приспособление для работы на устройстве пользователя и с его конкретными программами, пользователь вправе произвести самостоятельно без разрешения правообладателя. Например, он вправе прописать в реестре операционной системы драйвер приобретенного им устройства. Какого-либо разумного основания использовать термин «модификация» в ст. 272 (а затем и в других статьях УК РФ) не было, можно было использовать термин «изменение». В итоге смысл термина «модификация» при применении уголовного закона пришлось изменить, указав, что под модификацией нужно понимать любое изменение информации¹⁰.

Были сложности и с толкованием слова «копирование», под копированием предлагалось понимать исключительно выполнение команды операционной системой, но и здесь здравый смысл со временем возобладал, «переписывание от руки» также стало пониматься в качестве копирования¹¹. Неясно только, можно ли считать копированием простое считывание информации с экрана, ведь нельзя считать существенным такое обстоятельство, как переписал ли хакер информацию на бумаге или запомнил ее. Впрочем, вопрос о том, возможен ли доступ к компьютерной информации без изменения компьютерной информации, — риторический. При загрузке любого файла и выводе на экран любого изображения компьютерная информация в машине меняется. При таких обстоятельствах искусственная конструкция материального состава неоправданна, она вводит в заблуждение относительно того, что не всякий неправомерный доступ к компьютерной информации наказуем.

На заре криминализации компьютерных преступлений, когда важность охраны компьютерной безопасности осознавалась еще не в полной мере, материальные составы преступлений конструировались чаще, чем в наше время, но при этом указывались не придуманные последствия, учитывались охраняемые законом объекты за рамками компьютерной безопасности. В качестве примера можно привести германский Второй закон о борьбе с хозяйственной преступностью от 15 мая 1986 г.¹² Этим законом уголовная ответственность была установлена, в частности, за нарушение неприкосновенности частной жизни и конфиденциальности (компьютерный шпионаж, совершенный с преодолением защиты информации, — StGB, § 202a), имущественные преступления (компьютерное мошенничество — § 263a; злоупотребление с чеками и кредитными картами — § 266b; незаконное изменение данных, дополнившее норму об уничтожении

¹⁰ См.: Генеральная прокуратура Российской Федерации. Методические рекомендации по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации. 2013 // URL: <https://epp.genproc.gov.ru/web/gprf/documents/scientific-materials?item=4900252> (дата обращения: 22.02.2025). Эта позиция была поддержана и в п. 28 постановления Пленума Верховного Суда РФ от 15 декабря 2022 г. № 37.

¹¹ Методические рекомендации по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации. 2013.

¹² Zweites Gesetz zur Bekämpfung der Wirtschaftskriminalität (2.WiKG) vom 15.05.1986 // BGBl. I 1986, Nr. 21 vom 23.05.1986, S. 721.



имущества, — § 303а, компьютерный саботаж, квалифицированный состав в отношении § 303а, а также иное существенное нарушение обработки данных — § 303b), преступления, сходные с подлогом (фальсификация данных на электронных носителях, имеющих удостоверительное значение, — § 269; обман в правовых отношениях при обработке данных — § 270). Российский законодатель выбрал другой путь, изначально отнеся главу о компьютерных преступлениях к разделу о преступлениях против общественной безопасности, но не учел ни специфику объекта этих преступлений, ни механизм причинения вреда.

Наряду с казуистичным определением способов и последствий компьютерных преступлений проблемы связаны и с пониманием признака «неправомерности» доступа в ст. 272 и его «несанкционированности» в ст. 273 УК РФ. Может ли доступ человека к своему собственному компьютеру быть преступным посягательством на информационную безопасность? Примеры: чип-тюнинг бортового компьютера собственного автомобиля или чужого автомобиля по просьбе его хозяина; очистка памяти кассового аппарата; взлом защиты компьютерной программы от неправомерного использования. На практике были случаи квалификации подобных деяний в качестве компьютерных преступлений. Вместе с тем общественная безопасность от подобных деяний не страдает. Человек вправе уничтожить любую информацию в своем компьютере, он вправе и сам свой компьютер уничтожить со всей информацией в нем. Важной особенностью неправомерного доступа и вредоносных программ является то, что речь идет о неправомерном воздействии или угрозе неправомерного воздействия на чужие компьютеры, которые лицу не принадлежат. В качестве варианта посягательством на компьютерную безопасность может быть и воздействие на собственный компьютер в нарушение прав и законных интересов пользователя, если доступ к компьютеру предоставлен другому пользователю (например, он имеет учетную запись в системе), а доступ хозяина ограничен. Например, лицо, предоставляющее услугу в виде пользования электронной почтой, социальной сетью или мессенджером, может взломать чужой аккаунт, нарушив тем самым тайну связи или неправомерно распространяв информацию от чужого имени.

В случае чип-тюнинга двигателя собственного автомобиля страдает не компьютерная безопасность, может пострадать экологическая. Административная ответственность за эксплуатацию автомобиля с превышением нормативов содержания загрязняющих веществ в выбросах предусмотрена ст. 8.23 КоАП РФ, при этом не должно иметь существенного значения, перепрошьет ли водитель бортовой компьютер или разгонит мотор иным способом. Очистка памяти собственного кассового аппарата — нарушение экономическое, финансовое, за такое деяние предусмотрена административная ответственность ч. 4 ст. 14.5 КоАП РФ, не исключена и налоговая, и уголовная ответственность за уклонение от уплаты налогов, компьютерная безопасность при этом не страдает. Использование контрафактного экземпляра компьютерной программы, в том числе со взломом защиты от пиратского копирования, — это нарушение авторских прав, за которое также установлены гражданско-правовая, административная или уголовная ответственность.

Случаи вменения в качестве вредоносных программ программного обеспечения для перепрошивки бортовых компьютеров автомобилей в свежей практике

последних лет (изучены приговоры с 1 января 2023 г.) мною не обнаружены. Что же касается взлома защиты компьютерной информации — тут тенденция иная¹³. Федеральным законом от 7 декабря 2011 г. № 420-ФЗ в ст. 273 УК РФ в качестве вредоносной программы прямо названа программа, предназначенная для нейтрализации средств защиты компьютерной информации.

Рассмотрим типичную ситуацию. Гражданин продал смарт-карту со встроенным микрочипом, содержащим компьютерную программу, предназначенную для нейтрализации системы шифрования сигнала спутникового телевидения «Триколор», что позволяет просматривать платные каналы без оплаты, осужден по ч. 2 ст. 273 УК РФ за распространение компьютерных программ, заведомо предназначенных для несанкционированного копирования компьютерной информации и нейтрализации средств защиты компьютерной информации, совершенное из корыстной заинтересованности, за преступление средней тяжести назначено наказание в виде одного года лишения свободы условно¹⁴. Законность приговора сомнений не вызывает, небесспорной представляется социальная обусловленность закона.

Действительно, имеет место нарушение исключительных прав спутниковой компании и ее лицензиаров, но страдает ли в подобной ситуации общественная безопасность, имеет ли место серьезная угроза интересам неопределенного широкого круга лиц? Представляется, что такой угрозы нет. При этом уголовная ответственность по ст. 273 УК РФ возможна с возраста 16 лет, наказание в ч. 1 этой статьи — до 4 лет лишения свободы, значительно более строгое, чем наказание за простую кражу. Уголовная ответственность предусмотрена не только за создание и распространение вредоносных программ, но и за их использование. В России миллионы подростков регулярно используют программы, предназначенные для нейтрализации средств защиты компьютерной информации от пиратского копирования, устанавливая пиратские копии программ, в основном — компьютерных игр. Практика при этом соответствует здравому смыслу, по ч. 1 ст. 273 УК РФ в 2023 г. осуждено всего 12 человек. В действительности осуждают по ч. 1 ст. 273 людей за преступления достаточно серьезные. Гражданин создал программное обеспечение для шифрования данных на компьютерах неопределенного круга иностранных организаций с целью блокирования доступа к ним¹⁵. Другой использовал

¹³ В 2018 г. Е. А. Рускевич отмечал, что в судебно-следственной практике наибольшее распространение получило признание в качестве вредоносных программ, предназначенных для генерации серийного номера и кода активации при установке пиратских копий программного обеспечения (см.: *Рускевич Е. А.* Понятие вредоносной компьютерной программы // Актуальные проблемы российского права. 2018. № 11. С. 207—215). Сейчас к «лекарствам» для взлома защиты лицензионного программного обеспечения добавилась информация на смарт-картах, позволяющая просматривать спутниковое телевидение без оплаты. И в том, и в другом случае никаких изменений в информацию в чужом компьютере не вносится, имеет место приготовление к нарушению авторских прав.

¹⁴ Приговор Люблинского районного суда города Москвы от 18 декабря 2018 г. по делу № 1-861/2018.

¹⁵ Приговор Центрального районного суда города Калининграда от 25 декабря 2024 г. по делу № 1-375/2024.



и распространял универсальную программную платформу, предназначенную для получения несанкционированного доступа к различным электронным сервисам, платежным системам, средствам онлайн-коммуникаций, профилям социальных сетей и т.п., «реализация функционала которой осуществляется путем скрытого “заражения”»¹⁶. Третий атаковал ПАО «Тамбовский завод “Электроприбор”»¹⁷.

Фактически детей не привлекают к ответственности за взлом защиты компьютерных игр от пиратского копирования. Тем не менее совершеннолетний гражданин осужден за то, что незаконно модифицировал программное обеспечение в собственной игровой приставке, что сделало возможным ее использование для компьютерных игр без лицензии. Осужден по совокупности статей 172 (за модификацию программного обеспечения в собственной приставке) и 173 УК РФ (за использование при этом вредоносной программы, скачанной в сети Интернет)¹⁸. Корыстный мотив осужденному не вменили, хотя он пытался продать приставку, прямо указав в объявлении о продаже, что приставка «прошита». При таком подходе заправку чипированного картриджа для принтера нужно квалифицировать по совокупности ч. 3 ст. 172 и ч. 2 ст. 173, так как заправка картриджами — услуга платная, при этом такая деятельность осуществляется, как правило, в виде промысла организованными группами лиц. Если на «Авито» вбить в строку поиска «прошитая игровая приставка» — можно увидеть много предложений. Складывается впечатление, что люди не осознают преступности своих деяний.

Проблема в том, что деяние, которое не рассматривается в обществе в качестве серьезного проступка, в уголовном законе рассматривается в качестве серьезного (средней тяжести) преступления, что негативно сказывается на народном правосознании, в частности, развращает молодежь, подрывает авторитет права как такового. Совершение преступлений не должно быть массовым обыденным поведением. Представляется, что при таких обстоятельствах административной и гражданско-правовой ответственности за нарушение авторских прав достаточно, в уголовном же законе признаки составов компьютерных преступлений целесообразно уточнить, сохранив уголовную ответственность за реально опасные для общества деяния. Это позволит и правоохранительным органам сосредоточиться на реально полезной работе. Возможно, по мере развития народного правосознания санкции за нарушения авторских прав можно будет сделать более строгими, но время для этого еще не пришло. Пока же представляется целесообразным изложить нормы о компьютерных преступлениях (гл. 28 УК РФ) в уточненной редакции:

«Статья 272. Неправомерный доступ к компьютерной информации

1. Неправомерный доступ к компьютерной информации в чужом компьютере или в нарушение прав владельца этой информации — наказывается штрафом или лишением свободы на срок до пяти лет.
2. То же деяние, если оно повлекло тяжкие последствия, — наказывается лишением свободы на срок до 7 лет.

¹⁶ Приговор Свердловского районного суда города Костромы от 22 октября 2024 г. № 1-333/2024.

¹⁷ Приговор Советского районного суда города Тамбова от 21 августа 2024 г. № 1-337/2024.

¹⁸ Приговор Тамбовского районного суда Тамбовской области от 8 февраля 2023 г. по делу № 1-46/2023.

Примечания.

1. Компьютерной признается информация, существующая на технических носителях, специально предназначенных для ввода и обработки информации в компьютере.

2. Под нарушением прав владельца информации понимается деяние хозяина компьютера, предоставившего владельцу информации право использовать свой компьютер с ограничением доступа хозяина компьютера к этой информации в силу закона или договора.

Статья 273. Вредоносные программы

1. Создание, распространение или использование компьютерных программ, заведомо предназначенных для неразрешенного изменения информации в чужом компьютере, —

наказываются штрафом или лишением свободы на срок до пяти лет.

2. Те же деяния, если они повлекли тяжкие последствия, —

наказываются лишением свободы на срок до семи лет.

Статья 274. Нарушение правил пользования компьютерной информацией

Нарушение правил пользования компьютерной информацией или компьютерным оборудованием, если это повлекло по неосторожности тяжкие последствия, а равно умышленное причинение вреда лицом, имеющим доступ к компьютерной информации, злоупотребившим этим доступом, —

наказывается штрафом или лишением свободы на срок до пяти лет.

Статья 274¹. Неправомерное воздействие на критическую информационную инфраструктуру

Деяния, предусмотренные статьями 272—274, совершенные с целью неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации, —

наказываются штрафом или лишением свободы на срок до десяти лет.

Статья 274². Нарушение законодательства о персональных данных

1. Нарушение законодательства о персональных данных, сопряженное с хранением компьютерной информации, содержащей персональные данные, полученной незаконным путем, —

наказывается штрафом или лишением свободы на срок до пяти лет.

2. То же деяние, сопряженное с передачей персональных данных иностранцу, иностранному государству, иностранной или международной организации, — наказывается штрафом или лишением свободы на срок до десяти лет».

БИБЛИОГРАФИЯ

1. Русскевич Е. А. Понятие вредоносной компьютерной программы // Актуальные проблемы российского права. — 2018. — № 11. — С. 207—215.
2. Щепельков В. Ф. О квалификации преступлений в сфере компьютерной информации (в свете разъяснений Пленума Верховного Суда РФ) // Уголовное право. — 2023. — № 6. — С. 70—79.
3. Шеперд Г. Нейробиология : в 2 т. — М., 1987. — Т. 1. — 454 с.





**Денис Эдуардович
АЛЁХИН,**

партнер,
руководитель практики
Московской коллегии
адвокатов «Grad»,
alekhin@gradfirm.ru
105005, Россия, г. Москва,
ул. Бауманская,
д. 33/2, стр. 1

Квалификация преступлений, связанных с получением криптовалюты (майнингом)

Аннотация. Правовой статус майнинга в России остается одним из самых спорных вопросов. Основная сложность связана с отсутствием четкого подхода к правовому регулированию этого процесса, который заключается в создании новых единиц криптовалюты. Тем не менее принятые в прошлом году нормативные правовые акты подчеркивают актуальность и важность анализируемой темы.

В данной статье рассматриваются проблемы квалификации преступлений, связанных с получением криптовалюты, в том числе посредством майнинга. Анализируется правовой статус криптовалют в российском законодательстве, выявляются пробелы в правовом регулировании и особенности их правоприменения. Особое внимание уделено квалификации незаконного майнинга как формы незаконного предпринимательства, а также преступлениям, связанным с хищением электроэнергии, мошенничеством, вымогательством и легализацией доходов, полученных преступным путем. Исследуются актуальные судебные решения и проблемы доказывания в уголовных делах, связанных с цифровыми активами. Выделяются ключевые направления для развития уголовно-правового регулирования в отношении преступлений, связанных с криптовалютами.

Ключевые слова: криптовалюта, майнинг, преступление, уголовная ответственность, мошенничество, незаконное предпринимательство, легализация, киберпреступность

DOI: 10.17803/2311-5998.2025.129.5.058-064

Denis E. ALEKHIN,

Partner, Head of Practice
Moscow Bar Association "Grad"
alekhin@gradfirm.ru

33/2, str. 1, ul. Baumanskaya, Moscow, Russia, 105005

Qualification of crimes related to obtaining cryptocurrency (mining)

Abstract. The legal status of mining in Russia remains one of the most controversial issues. The main difficulty is related to the lack of a clear approach to the legal regulation of this process, which is the creation of new units of cryptocurrency. Nevertheless, the regulatory legal acts adopted last year emphasize the relevance and importance of the analyzed topic.

The article examines the problems of qualifying crimes related to obtaining cryptocurrency, including mining. The legal status of cryptocurrencies in Russian and international legislation is analyzed, identifying gaps in regulation and enforcement. Special attention is given to the qualification of illegal mining as a form of unlawful business, as well as crimes related to electricity theft, fraud, extortion, and money laundering. The study explores relevant court rulings and evidentiary issues in criminal cases involving digital assets. International experiences in cryptocurrency regulation are reviewed, and suggestions for improving Russian legislation are provided. Key directions for the development of criminal law policy concerning cryptocurrency-related crimes are highlighted.

Keywords: cryptocurrency, mining, crime, criminal liability, fraud, illegal business, legalization, cybercrime

Введение

В современном мире криптовалюта стала неотъемлемой частью цифровой экономики, что повлекло за собой рост преступлений, связанных с ее получением, использованием и оборотом. В отличие от традиционных финансовых инструментов, криптовалюта функционирует в децентрализованных системах, что усложняет государственный контроль и правоприменительную практику. Это создает почву для различных правонарушений, таких как мошенничество, отмывание денег, финансирование незаконной деятельности, уклонение от уплаты налогов и другие преступления.

За последний год в Российской Федерации произошли значительные изменения в законодательстве, касающемся криптовалют и майнинга. С 01.11.2024 вступил в силу Федеральный закон от 08.08.2024 № 221-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации»¹, который легализовал деятельность по добыче цифровых валют и установил ряд новых требований и ограничений для участников этого рынка. Закон вводит официальные определения таких терминов, как «майнинг», «майнинг-пул» и «оператор майнингowej инфраструктуры».

В статье 1 вышеуказанного Закона дается определение майнинга цифровой валюты: «...деятельность по проведению математических вычислений с использованием технических средств для внесения записей в информационную систему, использующую технологию распределенного реестра, с целью получения вознаграждения в цифровой валюте за подтверждение записей в этой системе».

Для осуществления майнинга юридические лица и индивидуальные предприниматели (ИП) обязаны зарегистрироваться в специальном реестре, который с 2025 г. перешел под управление ФНС России. Операторы майнингowej инфраструктуры также подлежат включению в этот реестр. Физические лица могут

¹ URL: https://www.consultant.ru/document/cons_doc_law_482417/.



заниматься майнингом без регистрации, если их потребление электроэнергии не превышает установленные лимиты.

Государство вправе запрещать майнинг в отдельных регионах, особенно в энергодефицитных зонах. Согласно постановлению Правительства РФ от 23.12.2024 № 1869 «Об установлении запрета на осуществление майнинга цифровой валюты (в том числе участие в майнинг-пуле) в отдельных субъектах Российской Федерации и на отдельных территориях субъектов Российской Федерации»² с 01.01.2025 по 15.03.2031 добывать криптовалюту, включая участие в майнинг-пулах, запрещено в 13 субъектах РФ: Иркутской области, Бурятии, Забайкальском крае, Дагестане, Ингушетии, Кабардино-Балкарии, Карачаево-Черкесии, Северной Осетии, Чечне, ДНР, ЛНР, Запорожской и Херсонской областях.

ФНС планирует двухэтапное налогообложение майнинга: первый — при зачислении криптовалюты, второй — при ее продаже.

В данной статье рассматриваются исключительно преступления, связанные с майнингом криптовалюты. Этот процесс, предполагающий использование вычислительных мощностей для подтверждения транзакций и генерации новых блоков в блокчейне, может применяться в незаконных целях. Наиболее распространенными преступлениями, связанными с майнингом, являются незаконное потребление электроэнергии, использование чужих вычислительных мощностей без согласия владельцев (криптоджекинг), нарушение налогового законодательства при добыче криптовалюты, а также неправомерное использование государственного оборудования для личного обогащения. При этом следует отметить, что правоприменительная практика по таким преступлениям пока остается фрагментарной.

Незаконный майнинг

1. Криптоджекинг представляет собой незаконное использование чужих вычислительных мощностей для майнинга криптовалюты. Чаще всего он осуществляется через заражение компьютеров, мобильных устройств или серверов вредоносным программным обеспечением, которое скрытно использует ресурсы устройства для добычи криптовалюты, не осведомляя владельцев этих устройств. Вредоносные программы, такие как криптоджеки, могут внедряться на устройства через фишинговые сайты, зараженные веб-страницы, вредоносные электронные письма или через уязвимости в программном обеспечении.

Особенность криптоджекинга заключается в том, что он может происходить на массовом уровне, затрагивая сотни и тысячи устройств. Это создает значительное финансовое бремя для владельцев зараженных устройств, так как майнинг криптовалюты требует больших вычислительных мощностей и приводит к увеличению потребления электроэнергии, что может вызвать повышение расходов на электричество и даже повреждение оборудования из-за перегрева.

С точки зрения уголовного права такие действия могут квалифицироваться как неправомерный доступ к компьютерной информации (ст. 272 УК РФ) или создание,

² URL: https://www.consultant.ru/document/cons_doc_law_494125/92d969e26a4326c5d02fa79b8f9cf4994ee5633b/.

использование и распространение вредоносных программ (ст. 273 УК РФ). Кроме того, при выявлении кражи личных данных в процессе криптоджекинга возможно применение статей, касающихся нарушения частной жизни (ст. 137 УК РФ).

Стоит также отметить, что криптоджекинг является не только нарушением законов об информационной безопасности, но и активно используется в коммерческих целях, когда злоумышленники с помощью массовых заражений пытаются сгенерировать криптовалюту для получения прибыли. Сложность выявления криптоджекинга связана с тем, что подобные вредоносные программы часто действуют скрытно и не заметны для обычных пользователей, что затрудняет оперативное обнаружение и пресечение таких преступлений.

2. Незаконное потребление электроэнергии — одна из наиболее распространенных форм преступной деятельности в сфере майнинга криптовалют. Процесс майнинга требует значительных затрат энергии, что делает его экономически невыгодным без использования дешевых или бесплатных источников энергии. Некоторые майнеры, стремясь снизить издержки, подключаются к электросетям незаконным способом, используя различные методы обхода счетчиков, установку «косых» проводок или даже подключение к электросетям без ведома владельцев имущества.

Такое незаконное потребление энергии может иметь серьезные последствия, включая увеличение нагрузки на энергосистемы, снижение качества электроснабжения и даже возникновение аварийных ситуаций. В некоторых случаях эти действия могут привести к существенным убыткам для энергетических компаний, поскольку они обязаны компенсировать недополученные доходы, а также затраты на восстановление сетевого оборудования, поврежденного из-за перегрузок.

С юридической точки зрения такие действия могут подпадать под статью 165 «Причинение имущественного ущерба путем обмана или злоупотребления доверием» УК РФ, если злоумышленники обманывают энергетические компании или владельцев объектов с целью незаконного подключения.

Использование краденых или незаконно подключенных ресурсов также может квалифицироваться как кража электроэнергии, что подпадает под статью 158 УК РФ.

Более того, если незаконное подключение связано с причинением серьезных материальных убытков или значительным ущербом для энергоснабжения, возможны более тяжелые наказания, включая лишение свободы на длительные сроки. Проблема незаконного потребления электроэнергии особенно актуальна для регионов, где майнинг криптовалюты активно развивается, а законодательство и контроль за энергетическими системами остаются недостаточно строгими.

Отмывание преступных доходов через майнинг

Майнинг криптовалюты может стать инструментом для отмывания преступных доходов. Преступники, получившие деньги или криптовалюту незаконным путем (например, через кражу, мошенничество или другие противоправные действия), могут использовать майнинг как способ легализации этих средств. В данном контексте майнинг служит каналом для преобразования «грязных»



активов в «чистые», что в дальнейшем позволяет преступникам использовать их в легальной экономике.

Майнинг криптовалюты предоставляет относительную анонимность и позволяет скрывать истинный источник средств. Полученные таким образом криптовалюты могут быть использованы для покупки товаров или услуг, обменены на фиатные деньги через криптовалютные биржи или использованы в качестве вложений, что затрудняет их отслеживание.

В таких случаях преступники могут столкнуться с уголовной ответственностью по ст. 174 «Легализация (отмывание) денежных средств или иного имущества, приобретенных лицом в результате совершения им преступления» УК РФ, которая предусматривает наказание за действия, направленные на легализацию доходов, полученных незаконным путем. Законодательство в сфере криптовалюты, однако, не всегда содержит достаточно четкие механизмы для отслеживания и пресечения таких схем.

С целью борьбы с отмыванием преступных доходов через майнинг необходимо усилить мониторинг и контроль криптовалютных операций.

Нарушение налогового законодательства

С увеличением популярности криптовалют правительства многих стран начали активно регулировать криптовалютные операции, включая обязательство декларировать доходы от криптовалют. В России, например, в последние годы были приняты изменения в законодательство, направленные на установление правил для налогообложения цифровых финансовых активов (ЦФА)³. Это означает, что даже если доходы от майнинга получены в виде криптовалюты, они должны быть задекларированы, а налоги, в том числе налог на прибыль, уплачены в соответствии с действующим Налоговым кодексом.

Таким образом, с 01.11.2024 майнинг криптовалюты, как и любой другой вид доходной деятельности, подлежит налогообложению. Однако многие майнеры, особенно в условиях анонимности, присущей криптовалютам, часто уклоняются от декларирования полученных доходов, что может привести к налоговым правонарушениям. В частности, если субъект майнит криптовалюту и не декларирует полученные доходы, он может быть привлечен к ответственности за уклонение от уплаты налогов в соответствии со статьями 198 и 199 УК РФ.

Статья 198 «Уклонение физического лица от уплаты налогов, сборов и (или) физического лица — плательщика страховых взносов от уплаты страховых взносов» УК РФ предусматривает ответственность за неуплату налогов физическим лицом, если сумма неуплаченных налогов превышает определенный порог. В случае с майнингом это может касаться как доходов от продажи криптовалюты, так и самой добычи, которая также рассматривается как доход. Уклонение от декларирования и уплаты налога на прибыль может повлечь за собой как штрафы, так и уголовное наказание в виде лишения свободы.

³ Сидоренко Э. Л. Криминальное использование криптовалюты: международные оценки // Международное уголовное право и международная юстиция. 2016. № 6. С. 8.

Статья 199 «Уклонение от уплаты налогов, сборов, подлежащих уплате организацией, и (или) страховых взносов, подлежащих уплате организацией — плательщиком страховых взносов» УК РФ может быть применена, если майнинг осуществляется через юридическое лицо, которое не уплачивает налоги с доходов от деятельности по майнингу.

Для налоговых органов важно выявлять случаи уклонения от налогообложения в сфере криптовалют, что ставит перед ними задачу отслеживания операций майнеров, их доходов и проверку корректности налоговых деклараций. Важно также, что для минимизации рисков налоговых нарушений майнерам следует соблюдать требования законодательства, в том числе по декларированию и уплате налогов с доходов от криптовалют, а также участвовать в системе учета ЦФА, предлагающей налоговую отчетность для криптовалютных операций.

Судебная практика

Судебная практика в области незаконного майнинга и криптовалюты развивается, и уже существует несколько примеров уголовных дел, касающихся преступлений в этой сфере.

Уголовное дело по факту незаконной предпринимательской деятельности. В 2021 г. в одном из российских регионов был задержан гражданин, который занимался майнингом криптовалюты без регистрации в качестве предпринимателя. Суд признал его виновным по ст. 171 «Незаконное предпринимательство» УК РФ, и он был оштрафован на 500 000 рублей.

Уголовное дело по факту нарушения безопасности в аэропорту. В 2017 г. сотрудники ФСБ задержали системного администратора аэропорта «Внуково» за создание фермы для майнинга криптовалюты в Московском центре управления воздушным движением. Его действия создавали угрозу безопасности аэропорта и могли привести к серьезным последствиям, таким как крушение самолетов. В данном случае действия злоумышленника были квалифицированы как нарушение должностных обязанностей и угроза безопасности полетов.

Приведенные примеры показывают, что майнинг криптовалюты может быть связан с различными уголовными правонарушениями, включая незаконное предпринимательство, мошенничество, кражу, нарушение правил безопасности и даже государственную измену. Важно отметить, что уголовные дела в этой сфере часто сталкиваются с юридическими сложностями, такими как определение ущерба и правомерность квалификации криптовалюты как имущества⁴. В связи с этим правовая охрана криптовалюты требует дальнейшего развития и адаптации законодательства для учета особенностей цифровых активов.

⁴ Файзуллина Л. Э. Пробелы уголовно-правового регулирования криптовалюты в российском законодательстве. Проблемы квалификации киберпреступлений и оценки доказательств // URL: https://zakon.ru/blog/2024/3/26/probely_ugolovno-pravovogo_regulirovaniya_kriptovalyuty_v_rossijskom_zakonodatelstve_problemy_kvalif.



Заключение

Преступления, связанные с майнингом криптовалют, становятся важной частью уголовно-правовой практики в условиях стремительно развивающейся цифровой экономики. С учетом растущей популярности криптовалют и их использования в различных сферах жизни, включая финансовые, коммерческие и личные операции, правовая охрана этой области приобретает все более актуальное значение.

В работе рассмотрены основные правонарушения, включая незаконное использование вычислительных мощностей, кражу электроэнергии и незаконное предпринимательство. Несмотря на имеющуюся судебную практику, правоприменительная деятельность сталкивается с проблемами квалификации преступлений и оценки ущерба.

Анализ законодательства показал необходимость его адаптации к специфике цифровых активов. Недавние изменения в правовом регулировании криптовалют и майнинга направлены на борьбу с теневыми схемами и незаконным оборотом цифровых активов. Однако требуется дальнейшее совершенствование норм и механизмов их применения.

Развитие судебной практики, совершенствование законодательства и повышение правовой осведомленности пользователей криптовалют — важные шаги для эффективного противодействия преступлениям в цифровой сфере.

БИБЛИОГРАФИЯ

1. *Аджиев Н. Б.* Криптовалюта как предмет преступлений против собственности // Международный научно-исследовательский журнал. — 2023. — № 8 (134).
2. *Долгиева М. М.* Операции с криптовалютами: актуальные проблемы теории и практики применения уголовного законодательства // Актуальные проблемы российского права. — 2019. — № 4. — С. 128—139.
3. Криптовалюты: тренды, риски, меры : доклад для общественных консультаций // Банк России. — URL: https://cbr.ru/Content/Document/File/132241/Consultation_Paper_20012022.pdf (дата обращения: 29.03.2025).
4. *Сидоренко Э. Л.* Криминальное использование криптовалюты: международные оценки // Международное уголовное право и международная юстиция. — 2016. — № 6.
5. *Смоляров М. В.* Уголовно-правовые последствия хищения токенов криптовалюты и гражданско-правовые механизмы защиты прав потерпевшего // СПС «Гарант».
6. Уголовное право. Общая часть : учебник для вузов / А. В. Наумов [и др.] ; отв. ред. А. В. Наумов, А. Г. Кибальник. — 6-е изд., перераб. и доп. — М. : Юрайт, 2024. — 448 с.
7. *Файзуллина Л. Э.* Пробелы уголовно-правового регулирования криптовалюты в российском законодательстве. Проблемы квалификации киберпреступлений и оценки доказательств. — URL: https://zakon.ru/blog/2024/3/26/probely_ugolovno-pravovogo_regulirovaniya_kriptovalyuty_v_rossijskom_zakonodatelstve_problemy_kvalif (дата обращения: 27.03.2025).

Уголовно-правовая новелла за нарушение законодательства о персональных данных (ст. 272¹ УК РФ): особенности конструирования состава и вопросы квалификации

Аннотация. В статье рассматриваются различные аспекты технико-юридического совершенствования ст. 272¹, внесенной в уголовное законодательство Федеральным законом от 30.11.2024 № 421-ФЗ. Представляется, что достаточных криминологических оснований для расширения криминализации главы о компьютерных преступлениях путем конструирования самостоятельного состава преступления не имелось. С появлением ст. 272¹ УК РФ возникает конкуренция со ст. 137 УК РФ и ст. 13.11 КоАП РФ. Самостоятельная криминализация хранения персональных данных в электронной форме в качестве деяния средней тяжести не соответствует характеру и степени общественной опасности деяния. Отсутствие нормативно-правового регулирования в сфере противодействия незаконному обороту программ, предназначенных для незаконного оборота компьютерной информации, содержащей персональные данные, затрудняет возможность эффективного правоприменения, для чего необходимо внесение изменений в действующее законодательство криминального цикла и об оперативно-разыскной деятельности. Методологическая база исследования построена на диалектическом методе познания, общенаучных и частнонаучных методах исследования. Автор использует системный подход к анализу проблемы, что позволяет рассмотреть ее в комплексе.

Ключевые слова: персональные данные, компьютерная информация, биометрические персональные данные, трансграничная передача информации, телеграм-боты



**Александр Александрович
КНЯЗЬКОВ,**

доцент кафедры
уголовного права
Университета имени
О.Е. Кутафина (МГЮА),
кандидат юридических наук
aaknyazkov@msal.ru
125993, Россия, г. Москва,
ул. Садовая-Кудринская, д. 9

DOI: 10.17803/2311-5998.2025.129.5.065-073

Alexander A. KNYAZKOV,

Associate Professor, Department of Criminal Law
of the Kutafin Moscow State Law University (MSAL),
Cand. Sci. (Law)

aaknyazkov@msal.ru

9, ul. Sadovaya-Kudrinskaya, Moscow, Russia, 125993

**Criminal law novel for violation of the legislation
on personal data (Art. 272¹ of the Criminal Code of Russia):
design features of the composition and qualification issues**

Abstract. *The article examines various aspects of the technical and legal perfection of the novel of Article 272¹ of the Criminal Code, introduced into criminal law by Federal Law No. 421-FZ dated 11/30/2024. It seems that there were no sufficient criminological grounds for expanding the criminalization of the chapter on computer crimes by constructing an independent corpus delicti. With the advent of Article 272¹ of the Criminal Code, competition arose with Article 137 of the Criminal Code and Article 13.11 of the Administrative Code of the Russian Federation. The independent criminalization of storing personal data in electronic form as an act of moderate severity does not correspond to the nature and degree of public danger of the act. The lack of regulatory and legal regulation in the field of countering the illicit trafficking of programs designed for the illicit trafficking of computer information containing personal data makes it difficult to effectively enforce law enforcement, which requires amendments to the current legislation on the criminal cycle and operational investigative activities.*

Keywords: *personal data, computer information, biometric personal data, cross-border information transfer, telegram bots*

В России Интернетом пользуются в настоящее время не менее 130 млн человек, включая более 106 млн пользователей социальных сетей¹, куда они, в том числе по требованию соответствующих платформ, загружают свои различные персональные данные. Кроме того, по состоянию на ноябрь 2024 г. порядка 84 % граждан пользуются услугами маркетплейсов (Ozon, Wildberries и др.)², что также предполагает введение и сохранение персональных данных пользователей в электронном виде.

Фактически без персональных данных в настоящее время полноценное пользование сетью Интернет значительно ограничивается в своем функционале — персональные данные требуются для верификации пользователя, дающей дополнительные возможности проверки его платежеспособности и т.д. В этой связи все более актуальными становятся проблемы надлежащего обеспечения

¹ URL: <https://blog.manufact.pro/2024/07/01/digital-russia-2024/> (дата обращения: 23.03.2025).

² URL: <https://1prime.ru/20241112/marketpleys-852766679.html> (дата обращения: 23.03.2025).

уголовно-правовой защиты таких данных, недопустимости их несанкционированного распространения и использования в криминальных целях.

В последние годы на федеральном уровне предпринимаются определенные шаги по нормативному решению указанной проблемы. Так, в конце 2023 г. ужесточена ответственность за утечку персональных данных путем повышения размера административного штрафа для должностных и юридических лиц (ч. 1 ст. 13.11 КоАП РФ). В октябре 2024 г. в Совет Федерации Всероссийским союзом страховщиков направлен проект концепции добровольного страхования рисков неправомерной утечки персональных данных, предусматривающий возможность получения компенсации морального ущерба, вреда имуществу и здоровью³.

Несмотря на усилия федерального законодателя и правоохранительных органов, черный рынок оборота персональных данных процветает, чему способствуют и сами недобросовестные работники организаций, предоставляющие персональные данные клиентов на безвозмездной или возмездной основе для последующего неправомерного использования.

Длительное время применение уголовной ответственности за преступления, связанные с незаконным использованием персональных данных, являлось малоэффективным. Имеющиеся составы уголовно-наказуемых деяний (ст. 137, 183, 272 УК РФ) не позволяли добиваться неотвратимости ответственности и соразмерного наказания.

Как следствие, Федеральным законом от 30.11.2024 № 421-ФЗ криминализирован незаконный оборот персональных данных⁴. С 11.12.2024 в российском уголовном законе появилась ст. 272¹, предусматривающая два самостоятельных состава преступления, представленных в шести частях с различными квалифицирующими признаками.

Не оспаривая необходимость ужесточения уголовно-правового противодействия соответствующему виду общественно опасного посягательства, отметим ряд технико-юридических недостатков при конструировании нового состава в тексте уголовного закона.

1. Законодатель при проектировании рассматриваемой новеллы допустил существенную ошибку, выразившуюся в подмене объекта и предмета преступления ст. 272¹, что следует из текста пояснительной записки к законопроекту о внесении изменений в УК РФ. Так авторы-разработчики безосновательно определили компьютерную информацию, содержащую персональные данные, как объект преступления⁵. Речь в данном случае не идет о какой-то незначительной оплошности; по нашему убеждению, именно указанный сбой законодательной техники свидетельствует об ошибочности введения в гл. 28 УК нового состава преступления, что вряд ли будет отвечать потребностям правоприменительной практики и криминологическим реалиям.

³ Страховщики запустят возмещения от утечек данных до конца 2025 года // URL: <https://www.rbc.ru/finances/12/11/2024/6731fa139a79475b4427e441> (дата обращения: 23.03.2025).

⁴ Российская газета. 06.12.2024.

⁵ Пояснительная записка к проекту федерального закона «О внесении изменений в Уголовный кодекс Российской Федерации» // URL: <https://sozd.duma.gov.ru/download/e55ce1c8-6725-497a-af16-e20265a80eed> (дата обращения: 23.03.2025).



Анализ изменений гл. 28 УК РФ свидетельствует, что отечественный законодатель своими точечными и не до конца проработанными поправками продолжил политику экспериментирования с нормами о компьютерных преступлениях. Так, несмотря на относительную устойчивость гл. 28 УК к нормотворческим реформам, законодатель сначала криминализировал неправомерное воздействие на критическую информационную инфраструктуру в 2017 г. (ст. 274¹ УК), что встретило преимущественно неодобрительную оценку в доктрине уголовного права по причине значительного количества технико-юридических дефектов данной нормы⁶. Следом законодатель добавил в гл. 28 УК в 2022 г. новый состав с административной преюдицией с весьма громоздкой диспозицией, перенасыщенной узкоспециализированной терминологией, по непонятным причинам снабженный дублирующим определением понятия должностного лица (в примечании к ст. 274² УК). Оценить эффективность ст. 274¹ УК пока не представляется возможным, поскольку новый состав преступления еще не применялся в правоприменительной практике.

Анализируемую нами ст. 272¹ УК РФ, введенную в конце 2024 г., также вряд ли обоснованно характеризовать в качестве необходимой правотворческой меры, поскольку данное преступление существенно не отличается по степени общественной опасности от основных составов преступлений в сфере компьютерной информации (ст. 272, 273), что могло бы оправдать конструирование специальной нормы⁷. В данном конкретном случае мы такого не наблюдаем, так как законодатель мог бы пойти по пути углубления дифференциации уголовной ответственности за указанные выше «компьютерные» преступления, добавив в соответствующие составы гл. 28 УК квалифицирующий признак «в отношении компьютерной информации, составляющей персональные данные», что не требовало бы включения в уголовный закон нового состава преступления.

2. Законодатель описывает диспозицию ст. 272¹ посредством указания на три способа совершения преступления путем (1) неправомерного доступа к средствам обработки компьютерной информации с персональными данными, (2) хранения или иного вмешательства в их функционирование либо (3) иным незаконным путем.

Если первые два описанных в законе способа не встречают существенных нареканий, то последний из них обоснованно вызывает вопросы. Пока в отсутствие какой-либо судебной практики складывается предположение, что указанный законодателем «иной незаконный путь» будет приравняться правоприменителем к не установленному (не доказанному) органами следствия пути, чем будет неизбежно допускаться расширительное толкование закона с

⁶ См., например: Бражник С. Д. Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации (статья 274.1 УК РФ): о некоторых проблемах дифференциации ответственности // Актуальные проблемы уголовного права на современном этапе (вопросы дифференциации ответственности и законодательной техники). 2020. № 9. С. 92—101.

⁷ Князьков А. А. Освобождение от уголовной ответственности по делам об экономических преступлениях (гл. 22 УК РФ): вопросы дифференциации и законодательной техники : дис. ... канд. юрид. наук. 2015. С. 27.

упрощением процесса доказывания и квалификации содеянного, что, в свою очередь, будет являться нарушением права обвиняемого на защиту от такого неконкретизированного обвинения в совершении преступления средней тяжести (ч. 1, 2 и 6) или тяжкого (ч. 3, 4 и 5 ст. 272¹ УК РФ) преступления.

Думается, что практика может сложиться иным путем, отличающимся от устоявшейся позиции Пленума Верховного Суда РФ применительно к ст. 272 УК РФ. Так, высшая судебная инстанция указала, что по уголовным делам о преступлениях, предусмотренных ст. 272 УК, неправомерным доступом к компьютерной информации является получение или использование такой информации в нарушение установленного нормативными правовыми актами порядка независимо от формы такого доступа⁸.

И если в целях применения ст. 272 УК Пленум Верховного Суда РФ раскрыл неправомерный доступ посредством бланкетного приема, то по ст. 272¹ УК имеются разумные основания прогнозировать практику упрощения квалификации содеянного, исходя из того, что если лицо изначально не могло получить доступ к персональным данным законным путем, следовательно, презюмируется уголовная противоправность по ст. 272¹ УК, т.е. получение субъектом доступа к информации с персональными данными незаконным путем.

При этом такой подход может быть удобен правоприменителю и избавит его от обязанности доказывать криминообразующий признак состава преступления, что не будет законным и не соответствует криминологическим реалиям⁹, поскольку по новой статье наказуемым является уже сам по себе факт хранения компьютерной информации, содержащей персональные данные, а не ее хранение в целях, например, последующего сбыта либо иного использования, что было бы допустимым.

Так, содеянное по ч. 1 рассматриваемой статьи образует состав преступления средней тяжести с санкцией в виде лишения свободы до 4 лет, что сопоставимо с хранением особо ценных диких животных и водных биологических ресурсов, занесенных в Красную книгу России (ч. 1 ст. 258¹ УК), и даже строже по наказанию, чем хранение наркотиков (ч. 1 ст. 228 УК), либо психотропных веществ (ч. 1 ст. 228³ УК), что вряд ли оправданно с точки зрения характера и степени общественной опасности сопоставляемых деяний. В этой связи мы не можем

⁸ Постановление Пленума Верховного Суда РФ от 15.12.2022 № 37 «О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть Интернет». П. 15 // СПС «КонсультантПлюс».

⁹ Вместе с тем подобная порочная практика встречается по другим категориям дел, в частности о незаконном обороте наркотиков. Так, например, суд указал, что «вывод суда первой инстанции о бланкетном характере диспозиции инкриминируемого ФИО1 преступления противоречит тексту уголовного закона, поскольку часть 1 статьи 228 УК РФ не содержит ссылки на нарушение или несоблюдение норм и правил, утверждаемых иными нормативными актами» (апелляционное постановление Ленинградского областного суда от 10.01.2025 № 22-146/2025 // СПС «КонсультантПлюс»). С данным подходом суда согласиться не представляется возможным.



согласиться с авторами — разработчиками законопроекта о введении ст. 272¹ УК¹⁰, которые, по нашему мнению, не обосновали необходимость конструирования основного состава преступления в виде преступления средней тяжести. Ссылки на увеличение сроков давности уголовного преследования и погашения судимости не являются гарантией эффективного уголовно-правового противодействия криминальному обороту персональных данных.

3. Характеризуя норму ст. 272¹ УК, нам приходится затронуть проблематику установления содержания понятия «персональные данные» и его соотношения с предметом преступления, предусмотренного ст. 137 УК.

В связи с введением в УК ст. 272¹ криминализация незаконного оборота персональных данных в компьютерной (электронной) форме охватывается гл. 28 УК; в том же случае, если субъект совершает противоправные действия (собираение или распространение) сведений, образующих личную тайну гражданина в «бумажной» форме, то уголовная ответственность будет наступать по ст. 137 УК. Во избежание возможной конкуренции составов указанных преступлений одновременно с внесением поправок в гл. 28 УК законодатель поправил диспозицию ст. 137 УК.

Согласно судебной статистике за 2023 г., по ч. 1 ст. 137 УК было осуждено 224 человека¹¹. С учетом внесенных законодателем вышеуказанных изменений в гл. 28 УК можно прогнозировать, что дальнейшее применение ст. 137 УК будет неуклонно снижаться. До введения в УК ст. 272.1 уголовные дела в отношении посягательств на персональные данные, как правило, возбуждались по ст. 137 УК. Однако частная жизнь по смыслу ст. 137 УК не охватывает всего объема персональных данных.

Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» (далее — Закон № 152-ФЗ) определяет персональные данные как любую информацию, которая относится к прямо или косвенно определенному или определяемому физическому лицу¹². Несмотря на то что данное определение было изначально сформулировано законодателем и не менялось на протяжении всего периода применения Закона № 152-ФЗ, в доктрине и на практике толкование содержания понятия персональных данных всегда сопровождалось дискуссиями.

Следует заметить, что статьей 13.11 КоАП РФ, предусматривающей административную ответственность за нарушения требований законодательства в области персональных данных, в том числе связанных с обработкой таких данных, охватываются незаконные сбор, хранение, использование и передача как самих персональных данных, так и баз, включающих такие данные.

В то же время в диспозиции ч. 1 ст. 272¹ УК отсутствуют конститутивные признаки, позволяющие четко отграничивать преступление от административного правонарушения по ст. 13.11 КоАП, что неизбежно приведет к конкуренции указанных норм и рассогласованию практики их применения.

¹⁰ Пояснительная записка к проекту федерального закона «О внесении изменений в Уголовный кодекс Российской Федерации».

¹¹ URL: <https://stat.ani-пресс.рф/stats/ug/t/14/s/17> (дата обращения: 23.03.2025).

¹² СПС «КонсультантПлюс».

4. Квалифицированный вид преступления, установленный ч. 2 ст. 272¹ УК, предусматривает ответственность за деяние, совершенное в отношении компьютерной информации, содержащей персональные данные несовершеннолетних лиц, специальные категории персональных данных или биометрические персональные данные.

Повышенная общественная опасность незаконного оборота указанных видов персональных данных очевидна и не вызывает сомнений, поскольку презюмируется наступление негативных последствий для лица при их несанкционированном использовании. Так, к специальной категории персональных данных относятся данные о расе, национальности, состоянии здоровья, об интимной жизни, о политических взглядах, религиозных или философских убеждениях (ч. 1 ст. 10 Закона № 152-ФЗ).

Перечень типов персональных данных, отнесенных к категории специальных, является в силу закона закрытым. Однако отнесение той или иной информации к данной категории персональных данных может быть сопряжено с рядом квалификационных сложностей. Например, фотография индивида может выявлять его расовую или этническую принадлежность, а в некоторых случаях — и политические убеждения при наличии соответствующего контекста¹³.

К числу биометрических персональных данных, указанных в ч. 2 ст. 272¹ УК, закон относит сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность (ч. 1 ст. 11 Закона № 152-ФЗ), например, фотографическое изображение и иные сведения, используемые для обеспечения однократного и (или) многократного прохода на охраняемую территорию и установления личности гражданина¹⁴.

5. Квалифицированные составы ст. 272¹ УК влекут повышенную уголовную ответственность, в частности, за деяния, сопряженные с трансграничной передачей компьютерной информации, содержащей персональные данные, или трансграничным перемещением носителей информации, содержащих персональные данные (ч. 4). Очевидно, что конструирование данного особо квалифицирующего признака рассчитано на применение в отношении облачных сервисов и серверов на территории иностранных (так называемых недружественных) государств.

Также предусмотрена уголовная ответственность за создание или обеспечение функционирования информационного ресурса, заведомо предназначенного для незаконных хранения, передачи (распространения, предоставления, доступа) компьютерной информации, содержащей персональные данные, полученной незаконным путем (ч. 6).

6. В силу прямого указания закона действие новой статьи УК РФ не распространяется на случаи обработки персональных данных физическими лицами исключительно для личных и семейных нужд.

¹³ Савельев А. И. Научно-практический постатейный комментарий к Федеральному закону «О персональных данных». М. : Статут, 2021. С. 300.

¹⁴ Письмо Минцифры России от 17.07.2020 № ОП-П24-070-19433 «О рассмотрении обращения» // СПС «КонсультантПлюс».



Очевидно, что это примечание к статье было обусловлено необходимостью избежать чрезмерно расширительного и произвольного толкования, как было, например, при оценке действий родителя, использующего мобильное приложение родительского контроля, позволяющего слышать происходящее в непосредственной близости от ребенка, для чего потребовалось вмешательство Конституционного Суда РФ с корректировкой сложившейся правоприменительной практики¹⁵, или же привлечение к уголовной ответственности фермеров по ст. 138¹ УК за использование технических средств контроля за домашними животными и скотом¹⁶.

Здесь возникает вопрос об уголовно-правовой оценке деяния в случае, если персональные данные требуются для иной, заведомо некриминальной цели, например, при необходимости установления идентификаторов истца или ответчика при подаче искового заявления в суд, перечисленных в п. 2—3 ч. 2 ст. 131 ГПК РФ.

На наш взгляд, по духу закона сбор таких сведений не должен квалифицироваться по ст. 137 УК РФ ввиду отсутствия субъективной стороны данного состава преступления, однако позиция судебной практики складывается иначе. Так, Пленум Верховного Суда РФ указывает, что не влечет уголовную ответственность собирание или распространение таких сведений лишь в государственных, общественных или иных публичных интересах¹⁷. Из этого разъяснения следует, что незаконный сбор идентификаторов участников судопроизводства не может сводиться к вышеперечисленным интересам, поскольку преследует личный интерес по судебной защите нарушенных прав и законных интересов.

7. Частью 6 ст. 272.1 УК РФ криминализировано создание и (или) обеспечение функционирования информационного ресурса, заведомо предназначенного для незаконных хранения, передачи (распространения, предоставления, доступа) компьютерной информации, содержащей персональные данные, полученной незаконным путем.

Фактически речь идет о введении уголовной ответственности за создание различных программ-роботов, телеграм-ботов и т.п., позволяющих получить всю необходимую персональную информацию преимущественно на возмездной основе путем автоматизированной обработки компьютерной информации в Интернете, не требующей человеческого участия, с существенной экономией времени на обработку информации, содержащей персональные данные.

Примеры следственно-судебной практики применения ст. 273 УК РФ в отношении вредоносного программного обеспечения показывают, что создателей таких

¹⁵ Постановление Конституционного Суда РФ от 18.01.2024 № 2-П «По делу о проверке конституционности части первой статьи 137 Уголовного кодекса Российской Федерации в связи с жалобой гражданина П. О. Вильке» // СПС «КонсультантПлюс».

¹⁶ Абдулин Р. С. Страсти по «Закону о сборе валежника»: от теории к практике // Уголовное судопроизводство. 2021. № 1. С. 31.

¹⁷ Постановление Пленума Верховного Суда РФ от 25.12.2018 № 46 «О некоторых вопросах судебной практики по делам о преступлениях против конституционных прав и свобод человека и гражданина (статьи 137, 138, 138.1, 139, 144.1, 145, 145¹ Уголовного кодекса Российской Федерации)». Абз. 2 п. 2 // СПС «КонсультантПлюс».

роботов и программ-ботов будет сложно не только выявлять, но и привлекать к уголовной ответственности ввиду недостаточной регламентированности этой процедуры на законодательном уровне (в первую очередь в нормах Закона об оперативно-разыскной деятельности) и отсутствия организационных мероприятий, направленных на совершенствование системы выявления, раскрытия и противодействия преступлениям в сфере незаконного оборота персональных данных.

БИБЛИОГРАФИЯ

1. *Абдулин Р. С.* Страсти по «Закону о сборе валежника»: от теории к практике // Уголовное судопроизводство. — 2021. — № 1. — С. 27—31.
2. *Бражник С. Д.* Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации (статья 274.1 УК РФ): о некоторых проблемах дифференциации ответственности // Актуальные проблемы уголовного права на современном этапе (вопросы дифференциации ответственности и законодательной техники). — 2020. — № 9. — С. 92—101.
3. *Князьков А. А.* Освобождение от уголовной ответственности по делам об экономических преступлениях (гл. 22 УК РФ): вопросы дифференциации и законодательной техники : дис. ... канд. юрид. наук. — 2015. — 219 с.
4. *Савельев А. И.* Научно-практический постатейный комментарий к Федеральному закону «О персональных данных». — М. : Статут, 2021. — 468 с.





**Дмитрий Михайлович
МОЛЧАНОВ,**

доцент кафедры
уголовного права

Университета имени
О.Е. Кутафина (МГЮА),
кандидат юридических
наук, доцент

dmmolchanov@msal.ru

125993, Россия, г. Москва,
ул. Садовая-Кудринская,
д. 9

Информационная безопасность как объект охраны от агрессивного информационного воздействия

Аннотация. В статье предлагается рассматривать информационную безопасность как трехсоставной объект, который включает в себя защищенность полезной информации от внешнего воздействия; доступность достоверной информации для обеспечения нормального функционирования государственных институтов и жизнедеятельности граждан; защищенность человека от агрессивного или деструктивного информационного воздействия. Основное внимание уделяется последнему аспекту. Существуют два механизма защиты: личный информационный фильтр, основанный на верном понимании ценностной иерархии, и принудительное ограничение информационных потоков со стороны государства. Ни тот ни другой механизм в настоящее время полноценно не работает: субъективная ценностная иерархия большого числа людей не соответствует объективной картине мира, а государство пока не научилось ни контролировать, ни ограничивать информационные потоки. Информационная среда в России очень неоднородна, огромное количество деструктивной информации находится в открытом доступе. Возможность генерирования и распространения такой информации почти не ограничена. Но осознание проблемы уже появилось и попытки выстраивания информационных барьеров как в направлении воспитания верных нравственных ориентиров, так и в направлении контроля и регулирования информационных потоков в России предпринимаются.

Ключевые слова: информационная безопасность, агрессивная информационная среда, ценностная иерархия, информационное воздействие, информационные фильтры, традиционные духовно-нравственные ценности, защищенность от информации, адресное информационное воздействие, публичное информационное воздействие, информационная атака

DOI: 10.17803/2311-5998.2025.129.5.074-083

Dmitry M. MOLCHANOV,

Associate Professor of the Department of Criminal Law
of the Kutafin Moscow State Law University (MSAL),
Cand. Sci. (Law), Associate Professor
dmmolchanov@msal.ru
9, ul. Sadovaya-Kudrinskaya, Moscow, Russia, 125993

Information Security as an Object of Protection from Aggressive Information Influence

Abstract. The article proposes to consider information security as a three-component object, which includes the protection of useful information from external influence, the availability of reliable information to ensure the normal functioning of state institutions and the life of citizens, and the protection of a person from aggressive or destructive information impact. The main attention is paid to the last aspect. There are two mechanisms of protection: a personal information filter based on the correct understanding of the value hierarchy and forced restriction of information flows by the state. Neither mechanism is currently fully operational: the subjective value hierarchy of a large number of people does not correspond to the objective picture of the world, and the state has not yet learned to either control or limit information flows. The information environment in Russia is very heterogeneous, a huge amount of destructive information is in the public domain. The possibility of generating and disseminating such information is almost unlimited. But awareness of the problem has already appeared and attempts to build information barriers both in the direction of educating the correct moral guidelines and in the direction of control and regulation of information flows in Russia are being undertaken.

Keywords: information security, aggressive information environment, value hierarchy, information impact, information filters, traditional spiritual and moral values, protection from information, targeted information impact, public information impact, information attac

В начале было Слово, и Слово было у Бога,
и Слово было Бог.

Ин. 1:1

И сказал Бог: да будет свет. И стал свет.

Быт. 1:3

Стоящие эпиграфом к данному исследованию слова из Евангелия от Иоанна и Книги Бытия имеют онтологический смысл и не требуют подробного анализа в этой работе, поскольку мы изучаем проблематику более низкого уровня, однако они могут являться камертоном, позволяющим настроиться на понимание масштаба исследуемых проблем: разрушительная сила слова может быть колоссальна. Словом созданный стройный порядок мироздания разрушается человеческими словами и возвращается к первобытному доисторическому состоянию хаоса: таков масштаб. Та информация, то слово, которое является



предметом изучения, образно и метко описано Н. С. Гумилевым в последнем четверостишии его одноименного стихотворения:

Мы ему поставили пределом
Скучные пределы естества.
И, как пчелы в улье опустелом,
Дурно пахнут мертвые слова.

О мертвых словах, об информации, разрушающей сознание, а вслед за этим и все окружающее, и пойдет речь в данной статье.

Безопасность в уголовном праве традиционно понимается как состояние защищенности. Применительно к информационной безопасности можно выделить минимум три аспекта: защищенность информации, защищенность от информации и защищенность права обладания достоверной информацией, имеющей жизненно важное (в широком смысле) значение для конкретного человека или нормальной деятельности государственных органов Российской Федерации. В первом случае речь идет об обеспечении безопасности ценной информации от деструктивного внешнего воздействия, во втором — о защите от деструктивного внешнего воздействия самой информации¹ на человека, в третьем — о защите права на обладание жизненно необходимой достоверной информацией, которая утаивается.

Необходимость охраны информации для законодателя очевидна, поэтому в УК РФ в зависимости от специфики охраняемой информации нормы о ее защите обособляются самим законодателем либо в отдельную группу в одной главе (например, преступления в сфере компьютерной информации), либо в группу, хотя и не обособленную, но помещенную в одну главу наряду с иными преступлениями (например, преступления, посягающие на сохранность государственной тайны). Защита права на обладание достоверной информацией обеспечивается несколькими нормами УК РФ, в которых устанавливается ответственность за непредоставление информации или за предоставление недостоверной информации.

Однако право на обладание достоверной информацией не рассматривается ни законодателем, ни доктриной уголовного права в качестве составной части более общего объекта охраны: информационной безопасности. Да и само право на обладание достоверной информацией в большинстве случаев является дополнительным объектом, однако и эта характеристика состава зачастую в доктрине игнорируется². Исключение составляют ст. 140 и 287 УК РФ.

¹ В теории дается различное толкование термина «информация». См., например: Кузьмин В. П. Понятие и юридическая сущность информации // Информационное право. 2009. № 2. С. 6.

² Например, в Комментариях к УК РФ под редакцией В. М. Лебедева для ст. 237 УК РФ право граждан на получение достоверной информации указывается как дополнительный объект, а в других комментариях наличие дополнительного объекта игнорируется (см., например: Комментарий к Уголовному кодексу Российской Федерации : в 4 т. М. : Юрайт, 2017. Т. 3 : Особенная часть / отв. ред. В. М. Лебедев. С. 122 ; Комментарий к Уголовному кодексу Российской Федерации (постатейный) / под ред. А. И. Чучаева. 3-е изд., испр. и доп. М. : Контракт, 2011. С. 349.

Конституционно закрепленное право (ст. 24 Конституции РФ) на обладание достоверной информацией, содержащейся в документах и материалах, непосредственно затрагивающих права и свободы человека, является основным непосредственным объектом нормы, закрепленной в ст. 140 УК РФ. Непосредственным объектом нормы, закрепленной в ст. 287 УК РФ, являются общественные отношения в области полноценного информационного обеспечения Федерального Собрания РФ и Счетной палаты РФ. Криминализация деяний, закрепленных в остальных нормах УК РФ, устанавливающих запрет на непредоставление информации или предоставление недостоверной информации, обуславливается необходимостью охраны иных объектов: интересов инвесторов (ст. 185¹), интересов кредиторов (ст. 195), общественной безопасности в широком смысле (ст. 207¹), общественной безопасности в части охраны жизни и здоровья граждан (ст. 207²), здоровья населения (ст. 237).

В отношении непосредственного объекта уголовно-правовой охраны нормы, закрепленной в ст. 237 УК РФ, следует отметить, что он выходит за пределы видового объекта гл. 25 УК РФ, поскольку название статьи определяет, что сокрытие информации создает опасность не только для здоровья, но и для жизни людей (видовой объект гл. 24 УК РФ), а диспозиция статьи позволяет говорить и о том, что непосредственный объект вторгается в пределы видового объекта гл. 26 УК РФ, поскольку указывает на угрозу наступления негативных последствий для окружающей среды.

Следовательно, можно утверждать, что это своего рода межвидовая норма, которая соответствует объему родового объекта, но выходит за пределы трех видовых объектов глав 24, 25 и 26 УК РФ. Кратко стоит упомянуть и о том, что место информационной безопасности как объекта уголовно-правовой охраны этой нормы не всегда верно понимается в теории. Так, в комментарии к УК РФ под редакцией профессора А. В. Бриллиантова можно встретить утверждение, что основным непосредственным объектом являются «общественные отношения, обеспечивающие право гражданина на получение достоверной информации об обстоятельствах, создающих опасность для жизни или здоровья», а факультативным объектом — «отношения по охране здоровья, окружающей природной среды»³.

Согласиться с этой позицией нельзя, поскольку общественная безопасность в части защищенности жизни людей, здоровья населения и безопасной окружающей среды является не факультативным, а основным непосредственным объектом данной нормы. Именно создание угрозы этому объекту обуславливает возможность наступления уголовной ответственности. А в механизм возможного причинения вреда основному объекту включается объект дополнительный: информационная безопасность в части осведомленности населения о фактах и обстоятельствах, угрожающих экологии, жизни и здоровью людей. В ряде доктринальных источников мы находим именно такое понимание непосредственного и дополнительного объектов⁴.

³ Комментарий к Уголовному кодексу Российской Федерации (постатейный) / под ред. А. В. Бриллиантова : в 2 т. 2-е изд. М. : Проспект, 2015. Т. 2. С. 130.

⁴ См., например: Комментарий к Уголовному кодексу Российской Федерации : в 4 т. Т. 3. С. 122.



Значимость достоверной информации для обеспечения безопасности населения существенно возрастает при появлении дополнительных угроз. Например, военные действия, которые Российская Федерация вынужденно вела на своей территории в Курской области, являются ответом на возникшую угрозу территориальной целостности и жизни населения России. А предоставление несвоевременной и недостоверной информации о возникшей угрозе в самом начале ее появления, в том числе в средствах массовой информации, создало препятствие в принятии мер по своевременной эвакуации населения, что повлекло тяжкие последствия для оставшегося на оккупированной территории населения, в отношении которого представителями вооруженных сил противника совершались различные преступления: убийства, причинение различной тяжести вреда здоровью, изнасилования, грабежи, разбои.

Изучение судебной практики (если такая имеется), в связи с вышеизложенными обстоятельствами, о привлечении каких-либо лиц к уголовной ответственности по статьям 207¹ или 207² УК РФ могло бы быть основой отдельного научного исследования. Если такой практики нет, то это хороший повод для исследования другой проблемы: пробелов в УК РФ в части установления уголовной ответственности за несвоевременное и недостоверное информирование населения об угрозах, возникающих вследствие военных действий.

Столь длинный экскурс по объекту исследования потребовался нам по той причине, что в доктрине уголовного права России пока еще не устоялось понимание информационной безопасности как трехсоставного объекта⁵.

Обратимся к теоретическим и практическим аспектам информационной безопасности как объекта охраны от деструктивного информационного воздействия. Какие угрозы информационной безопасности в этой сфере существуют? Есть ли эффективные уголовно-правовые механизмы борьбы с этими угрозами? Что собой представляет информационная безопасность как объект охраны в этой сфере?

Как выглядит проблема глазами законодателя? Во-первых, в Особенной части УК РФ есть ряд норм, прямо запрещающих распространение деструктивной информации⁶; во-вторых, законодатель усиливает ответственность за ряд

⁵ В доктрине уголовного права представлены в основном многочисленные попытки осмысления отдельных частей этого объекта. См., например: Чеботарева А. А. Обеспечение информационной безопасности личности в Интернете: история и проблемы развития законодательства // История государства и права. 2010. № 11. С. 30—33; Ефремова М. А. Информационная безопасность как объект уголовно-правовой охраны // Информационное право. 2014. № 5. С. 21—25.

⁶ Например, эти нормы закреплены в следующих статьях УК РФ: ст. 110² «Организация деятельности, направленной на побуждение к совершению самоубийства»; ст. 205² «Публичные призывы к осуществлению террористической деятельности, публичное оправдание терроризма или пропаганда терроризма»; ст. 280 «Публичные призывы к осуществлению экстремистской деятельности»; ст. 280¹ «Публичные призывы к осуществлению действий, направленных на нарушение территориальной целостности Российской Федерации»; ст. 280⁴ «Публичные призывы к осуществлению деятельности, направленной против безопасности государства»; ст. 282⁴ «Неоднократная пропаганда

преступлений, которые сами по себе не несут угрозы информационной безопасности, однако в сочетании с инструментами по распространению информации создают качественно новую угрозу, поскольку демонстративно выставляются напоказ неограниченно широкой аудитории сети Интернет. Большое число статей УК РФ, предусматривающих ответственность за насильственные преступления (например, п. «о» ч. 2 ст. 105, п. «и» ч. 2 ст. 111, п. «д» ч. 2 ст. 115, п. «и» ч. 2 ст. 126, п. «з» ч. 2 ст. 127 УК РФ), дополнено квалифицирующим признаком следующего содержания: «совершенное с публичной демонстрацией, в том числе в средствах массовой информации или информационно-телекоммуникационных сетях (включая сеть Интернет)».

В-третьих, в ряде норм, которые относятся к квалифицированным составам, в качестве квалифицирующего признака указывается на совершение этого преступления с использованием такого информационного инструмента, как сеть Интернет (например, в п. «б» ч. 3 ст. 133 ; п. «в» ч. 3 ст. 222 ; п. «б» ч. 2 ст. 228¹ УК РФ). Информационную безопасность в таких случаях вполне уместно считать дополнительным объектом, поскольку именно легкий доступ к информации создает предпосылки для огромного спектра негативных последствий, которые появляются у лица, подвергшегося информационному воздействию. Возможность обезличенного общения через Интернет создает «рабочие места» для посредников в сбыте или приобретении оружия или наркотиков, создает комфортные условия для приобретения запрещенных предметов без опасения быть привлеченным к уголовной ответственности.

И главной точкой приложения усилий со стороны государства для борьбы с этими преступлениями могло бы быть пресечение беспрепятственного обмена информацией в этой сфере. Следует отметить и явную недооценку степени общественной опасности преступлений, совершаемых с использованием сети Интернет: на основе опыта так называемых цветных революций можно было бы сделать однозначный вывод о том, что данный квалифицирующий признак необходим в ст. 212 УК РФ, предусматривающей ответственность за организацию массовых беспорядков, но такого признака нет.

На основе анализа судебной практики можно сделать вывод о том, что огромное число преступлений, предусмотренных ст. 135 УК РФ, совершается с использованием сети Интернет, но такого признака и здесь нет. Исходя из многофункциональности сети Интернет как средства передачи информации, можно было бы учитывать его использование как обстоятельство,отягчающее наказание, но ст. 63 УК ограничивается усилением ответственности лишь за один вариант его использования: для публичной демонстрации совершаемого преступления. Объяснить это можно тем, что пока государство находится в самом начале пути осознания глобальности угроз для всех сфер жизнедеятельности государства, создаваемых возможностью неконтролируемого информационного воздействия.

либо публичное демонстрирование нацистской атрибутики или символики, либо атрибутики или символики экстремистских организаций, либо иных атрибутики или символики, пропаганда либо публичное демонстрирование которых запрещены федеральными законами»; ст. 354 «Публичные призывы к развязыванию агрессивной войны».



Потенциально нормы УК РФ, запрещающие противоправное информационное воздействие, наряду с теми объектами, которые закладываются в них законодателем и легко считываются при обычном подходе к толкованию исходя из места нормы в структуре Особенной части УК, охраняют и информационную безопасность. Например, норма, устанавливающая уголовно-правовой запрет на клевету (ст. 128¹ УК РФ), вряд ли воспринимается как норма, защищающая информационную безопасность. Традиционно принято считать, что клевета посягает на такие объекты уголовно-правовой охраны, как честь и достоинство. Это, конечно же, верно, однако ни законодатель, ни правоприменитель, ни доктрина уголовного права не учитывают тот факт, что ложная информация, порочащая честь и достоинство другого человека, не менее разрушительно действует и на людей, которые воспринимают такую информацию, поскольку они становятся носителями негативного отношения к другим людям, осуждают их, испытывают негативные эмоции, может быть, даже проявляют готовность порвать или рвут социальные связи в самых различных сферах (семейные, творческие, деловые и пр.), хотя никаких оснований для этого нет, поскольку информация, которой они поверили, не соответствует действительности. Вряд ли законодатель учитывал эти угрозы. Но они существуют, и дальнейшая теоретическая разработка этой темы позволит и законодателю учитывать все грани общественной опасности деструктивной информации.

Необходимо отметить, что деструктивное информационное воздействие может быть адресным, а может носить публичный характер. К адресному воздействию на ограниченный круг субъектов можно отнести те случаи, когда одно лицо побуждает другое лицо к совершению какого-либо преступления. Такие действия могут получить оценку как соучастие в виде подстрекательства, а могут рассматриваться законодателем в качестве самостоятельного преступления в статьях Особенной части⁷.

Адресное воздействие, побуждающее совершить то или иное негативное действие, может быть самостоятельным преступлением, не являясь аналогом соучастия (ст. 150, 151 УК РФ). На примере ст. 150 УК РФ можно уяснить интересную закономерность: по смыслу данной статьи вовлекаемый в совершение преступления несовершеннолетний является потерпевшим, что не исключает возможности привлечения его самого к уголовной ответственности в качестве соучастника того преступления, в которое его вовлекли. Взрослый человек, которого подстрекатель вовлек в совершение преступления, сделав своим соучастником, в юридическом смысле, конечно же, не может признаваться потерпевшим, но, рассматривая действия подстрекателя в контексте нарушения информационной безопасности, вполне можно утверждать, что подстрекаемый — именно жертва деструктивного информационного воздействия. Потерпевшие же в буквальном смысле слова могут подвергаться агрессивному информационному воздействию различной направленности. Например, мошенничество, развратные действия, склонение к потреблению наркотических средств — это те преступления, которые невозможно совершить без оказания деструктивного информационного воздействия на потерпевшего.

⁷ См., например: УК РФ. Ч. 1 и 1¹ ст. 205¹.

Массовое информационное воздействие может быть следующих видов: 1) массовое воздействие, побуждающее к противоправным действиям (в том числе к преступлениям); 2) массовое воздействие, направленное на нравственное разрушение человеческой личности или причинение иного вреда, причем направленность в данном случае может являться объективной характеристикой, которая может и не осознаваться самим преступником. Возможно сочетание адресного и массового воздействия, когда информационная атака, хотя и носит адресный характер (например, при мошенничестве), однако совершается на постоянной основе в отношении большого количества потерпевших (например, массовый обзвон).

Опасность деструктивного информационного воздействия обусловлена тем, что в человеческой природе заложена склонность к информационному взаимодействию друг с другом и естественной реакцией является доверие. Это особенно ярко проявляется в детях, которые без сомнения воспринимают все, что слышат от родителей. С возрастом у человека появляется навык критического мышления, и всякая новая информация воспринимается избирательно, в зависимости от той схемы информационных фильтров, которая в человеке сформирована. Главная проблема заключается в том, что схема фильтрации изначально у большинства людей сформирована с изъянами и может работать в обратном направлении: нужную и жизненно важную для человека информацию отвергать, а разрушительную и негативную воспринимать как полезную.

Этим словам более 2 700 лет, но с тех пор люди не изменились⁸: «Горе тем, которые зло называют добром, и добро — злом, тьму почитают светом, и свет — тьмою, горькое почитают сладким, и сладкое — горьким! Горе тем, которые мудры в своих глазах и разумны пред самими собою!» (Ис. 5:20—21). Полная неадекватность в восприятии информации встречается, наверное, редко, а возможно, вообще не встречается, если только речь не идет о психических патологиях. А вот частичное смещение ориентиров в большей или меньшей степени — явление повсеместное. Это обуславливается в первую очередь тем, что ценностная иерархия большинства людей не имеет объективной основы: добро и зло воспринимаются как понятия относительные.

Это означает, что большинство людей представляют группу повышенного риска: неспособность отделить зерна от плевел позволяет деструктивной информации завладеть сознанием человека и в первую очередь разрушать его изнутри, а затем побуждать его нести разрушительную энергию во внешний мир в виде самых разнообразных преступлений. В какую именно брешь проникнет информация, зависит от индивидуальной деформации: кого-то можно убедить в национальной исключительности, кого-то в бессмысленности жизни и необходимости покончить жизнь самоубийством, кого-то — в том, что необходимо бороться за права сексуальных меньшинств. В случае, если внутренние информационные

⁸ Люди не изменились, но очень сильно изменились внешние условия, изменилось информационное поле. Если раньше человек жил в пустыне своего разума и ему попадались лишь информационные ручейки с возможностью выбора, из какого попить, то сегодня он живет в море информации, в которое впадают тысячи рек, большая часть которых — сточные каналы.



фильтры работают с правильной настройкой (на основе объективно верной системы ценностей), вероятность воздействия деструктивной информации остается, но является низкой.

Углубляться в детальное рассмотрение субъективной картины мира конкретного человека, максимально приближенной к объективной ценностной реальности, в рамках данной статьи мы не можем, но можем проиллюстрировать, как работает механизм защиты в этом случае, на частном примере. Например, ст. 282⁴ УК РФ запрещает пропаганду либо публичное демонстрирование нацистской атрибутики или символики, поскольку существует риск закрепления в сознании людей таких знаков и символов как положительных, с дальнейшим перенесением этих характеристик символов на их носителей как людей «сильных, твердых, решительных», однако для выживших узников концлагерей такая символика не может вызывать ничего, кроме отвращения, поскольку они имели опыт реального общения с этими «сильными, твердыми и решительными» людьми, носившими подобную атрибутику.

Но такая информационная защита может работать и априорно (без переживания негативного личного опыта), на основе тех знаний о должном и недолжном, которые заложены в сознание человека с детства. Например, у некоторых людей сознание совершенно закрыто от восприятия матерной брани и возможность внутреннего воздействия на них такой информации равна нулю⁹, поскольку такая информация активно отторгается почти на физиологическом уровне (как неприятие тухлой пищи). У подавляющего же большинства людей такие защитные механизмы отсутствуют по очень большому спектру информационных угроз, а потому информационная безопасность требует активного участия государства в ее обеспечении.

С началом военных действий стало появляться смутное и не вполне оформившееся понимание масштаба информационных угроз, а потому государство предпринимает попытки борьбы с ними. Есть верное понимание, что эффективная борьба требует усилия в двух направлениях: формирование сознания на основе правильной ценностной иерархии и меры контроля и ограничения в отношении источников информации. Но делается это все на скорую руку и без глубокого осмысления, поэтому пока усилия в этих направлениях напоминают хаотичные телодвижения человека, который, почувствовав угрозу, начинает размахивать руками, пытаясь от нее защититься. А надо не махать руками, а прицельно стрелять.

Указ Президента РФ от 09.11.2022 № 809 «Об утверждении Основ государственной политики по сохранению и укреплению традиционных российских духовно-нравственных ценностей» можно назвать одним из шагов на пути к обеспечению информационной безопасности. Но пока это шаг человека, который пытается найти верное направление, но движется в темноте на ощупь. Проиллюстрируем сказанное всего одним примером. Если в п. 5 этого Указа первой ценностью провозглашается жизнь, а по статистике за 2023 г. в России сделано 467 тысяч аборт¹⁰, значит «жизнь», о которой говорится в Указе, всего лишь термин,

⁹ Возможно лишь внешнее воздействие, от которого человеку становится противно, как от неприятного запаха или вида разлагающегося трупа, например.

¹⁰ URL: <https://www.kommersant.ru/doc/7497492> (дата обращения: 31.03.2025).

не наполненный содержанием. В контексте информационной безопасности можно предложить рассмотреть два сценария: 1) государство будет активно защищать в информационном пространстве право женщин на прерывание беременности; 2) государство будет активно участвовать в информационном противодействии такому решению беременных женщин. Какой из этих сценариев соответствует интересам обеспечения информационной безопасности?

В заключение — краткие соображения по второму направлению обеспечения информационной безопасности: контроль информационных потоков и ответственность за распространение деструктивной информации. В этом направлении успех возможен лишь в том случае, если:

- 1) информационные ресурсы физически находятся в пределах досягаемости российских правоохранительных органов;
- 2) существует возможность блокировки информации из источников, находящихся вне такого контроля;
- 3) для владельцев информационных ресурсов, которые сами не распространяют информацию, устанавливается обязанность самоцензуры всех материалов, которые размещены на той или иной информационной платформе.

БИБЛИОГРАФИЯ

1. *Ефремова М. А.* Информационная безопасность как объект уголовно-правовой охраны // Информационное право. — 2014. — № 5.
2. *Гумилев Н. С.* Полное собрание сочинений : в 10 т. — М. : Воскресенье, 1998. — Т. 3 : Стихотворения. Поэмы / ред. колл. : Н. Н. Скотов (гл. ред.) [и др.] ; РАН. Ин-т рус. лит. (Пушк. дом.).
3. Комментарий к Уголовному кодексу Российской Федерации : в 4 т. — М. : Юрайт, 2017. — Т. 3 : Особенная часть / отв. ред. В. М. Лебедев.
4. Комментарий к Уголовному кодексу Российской Федерации (постатейный) / под ред. А. В. Бриллиантова : в 2 т. — 2-е изд. — М. : Проспект, 2015. — Т. 2.
5. Комментарий к Уголовному кодексу Российской Федерации (постатейный) / под ред. А. И. Чучаева. — 3-е изд., испр. и доп. — М. : Контракт, 2011.
6. *Кузьмин В. П.* Понятие и юридическая сущность информации // Информационное право. — 2009. — № 2.
7. *Чеботарева А. А.* Обеспечение информационной безопасности личности в Интернете: история и проблемы развития законодательства // История государства и права. — 2010. — № 11.





**Юлия Викторовна
ГРАЧЕВА,**

профессор кафедры
уголовного права
Университета имени
О.Е. Кутафина (МГЮА),
доктор юридических наук,
профессор

jvgracheva@msal.ru
125993, Россия, г. Москва,
ул. Садовая-Кудринская, д. 9



**Юлия Владимировна
ЧАЛЫШЕВА,**

аспирант кафедры
уголовного права
Университета имени
О.Е. Кутафина (МГЮА),
первый заместитель
председателя Совета
молодых ученых МГЮА
chalysheva011@mail.ru
125993, Россия, г. Москва,
ул. Садовая-Кудринская, д. 9

Общественная опасность и уголовно-правовая оценка фальсификации национальной истории в компьютерных играх

Аннотация. Статья посвящена уголовно-правовой оценке фальсификации истории в компьютерных играх, которые сегодня наряду с социальными сетями, интернет-порталами, видеохостингами, новостными сайтами стали дополнительной коммуникационной площадкой для обмена данными среди пользователей информационных технологий. Согласно исследованиям международных компаний, количество игроков постоянно увеличивается, охватывая разные возрастные группы и регионы, что подтверждает массовый характер игровой индустрии. Особо распространены среди молодого поколения компьютерные игры, сюжет которых связан с событиями Второй мировой войны и Великой Отечественной войны. В этой связи в статье сформулированы предложения по квалификации действий, фальсифицирующих исторические факты, содержащиеся в компьютерных играх. Обращается внимание на неопределенность правовой природы компьютерных игр, отсутствие регламентации разработки и определения содержания игровых продуктов, что порождает сложности уголовно-правовой оценки искажения информации об исторических событиях в играх.

Сохранение исторической памяти является стратегическим интересом России, обеспечить который позволит только комплексный подход, включающий уголовно-правовой механизм противодействия фальсификации истории.

Ключевые слова: политика памяти, фальсификация истории, реабилитация нацизма, компьютерные игры, фейк, историческая правда, национальная безопасность, уголовно-правовая оценка

DOI: 10.17803/2311-5998.2025.129.5.084-092

Julia V. GRACHEVA,

*Professor of the Department of Criminal Law
of the Kutafin Moscow State Law University (MSAL),*

Dr. Sci. (Law), Professor

jvgracheva@msal.ru

9, ul. Sadovaya-Kudrinskaya, Moscow, Russia, 125993

Julia V. CHALYSHEVA,

*Postgraduate student of the Department of Criminal law
of the Kutafin Moscow State Law University (MSAL),*

first deputy Chairman of the Council of young scientists of MSAL

chalysheva011@mail.ru

9, ul. Sadovaya-Kudrinskaya, Moscow, Russia, 125993

Social Danger and Criminal-Legal Assessment of Falsification of National History in Computer Games

Abstract. *The article is devoted to the criminal-legal assessment of the falsification of history in computer games, which today, along with social networks, Internet portals, video hosting sites, news sites have become an additional communication platform for the exchange of data among users of information technology. According to research by international companies, the number of players is constantly increasing, covering different age groups and regions, which confirms the mass character of the gaming industry. Computer games whose plots are connected with the events of World War II and the Great Patriotic War are especially widespread among the younger generation. In this regard, the article formulates proposals for the qualification of actions that falsify historical facts contained in computer games. Attention is drawn to the uncertainty of the legal nature of computer games, the lack of regulation of the development and definition of the content of game products, which gives rise to difficulties in the criminal-legal assessment of the distortion of information about historical events in games.*

Preservation of historical memory is a strategic interest of Russia, which can only be ensured by a comprehensive approach, including a criminal-legal mechanism to combat the falsification of history.

Keywords: *memory policy, falsification of history, rehabilitation of Nazism, computer games, fakes, historical truth, national security, criminal law assessment*

Согласно последнему опубликованному отчету мировой аналитической компании DFC Intelligence за 2023 г., число потребителей компьютерных игр выросло до 3,7 млрд человек¹. В представленное количество входят

¹ Global Video Game Audience Reaches 3.7 Billion // URL: <https://www.dfciint.com/global-video-game-audience-reaches-3-7-billion/> (дата обращения: 04.03.2025).



пользователи различной степени вовлеченности: одни играют систематически, на постоянной основе, а другие — лишь изредка. В этой связи некоторые аналитики отмечают, что геймерами можно назвать только 10 % от общего количества вовлеченных в игровую индустрию, т.е. около 300 млн человек². Говоря о целевой аудитории, необходимо обратить внимание на то, что большая часть игроков — молодые люди в возрасте от 18 до 24 лет³.

Указанные данные подтверждают массовый характер распространенности компьютерных игр, что позволяет рассматривать их в качестве определенного средства воздействия на общественное сознание, в том числе на мировоззрение молодого поколения. С. И. Белов справедливо отмечает, что настало время, когда компьютерные игры, выступающие в роли нового инструмента формирования представлений о событиях прошлого, начинают конкурировать со школьными учебниками по истории⁴. Вместе с тем сохранение исторической памяти в Стратегии национальной безопасности Российской Федерации определено в качестве национального приоритета⁵.

В современном мире к индустрии компьютерных игр сложилось двойственное отношение. Так, с одной стороны, ее развитие может способствовать созданию уникального прибыльного сектора экономики, образовательного компонента для молодежной аудитории, а с другой — через сюжет игровых продуктов может происходить влияние на сознание человека, его мировоззрение, что не исключает возникновения других рисков и угроз для национальной безопасности⁶. В этой связи А. Н. Лушин обращает внимание на то, что одной из глобальных проблем является фальсификация истории, которая оказывает пагубное воздействие на историческую память народа, в конечном счете способствует ее утрате, что может привести к потере молодого поколения⁷. Таким образом, искажение исторических фактов посредством компьютерных игр может оказать негативное воздействие на

² Исследование показало, что почти половина населения Земли играет в игры // URL: <https://www.gazeta.ru/tech/news/2023/04/12/20197243.shtml> (дата обращения: 04.03.2025).

³ Видеоигры — и кто в них играет? // URL: <https://wciom.ru/analytical-reviews/analiticheskii-obzor/videoigry-i-cto-v-nikh-igraet> (дата обращения: 04.03.2025).

⁴ См.: *Белов С. И.* Компьютерные игры как инструмент реализации политики памяти (на примере отображения событий Великой Отечественной войны в видеоиграх) // Вестник Российского университета дружбы народов. Серия : Политология. 2018. Т. 20. № 1. С. 96—104.

⁵ Указ Президента РФ от 02.07.2021 № 400 «О Стратегии национальной безопасности Российской Федерации» // СЗ РФ. 2021. № 27 (ч. II). Ст. 5351.

⁶ См.: *Федорченко С. Н., Тедиков Д. О., Теслюк К. В., Маркарян Р. А.* Сетевые компьютерные игры в эпоху цифровизации: новые угрозы или потенциалы для реализации политики памяти? // Вестник Московского государственного областного университета (электронный журнал). 2019. № 3. С. 73—78.

⁷ См.: *Лушин А. Н.* Фальсификация истории: теоретический подход к проблеме (на примере России) // Вестник Нижегородской академии МВД России. 2013. № 23. С. 24.

население страны. Это обстоятельство дает основание рассматривать игровые продукты в качестве инструмента «мягкой силы»⁸.

В России с учетом новых угроз, вызванных полномасштабной цифровой трансформацией, на федеральном уровне реализуются разнообразные меры организационного и законодательного характера, направленные на создание системы, обеспечивающей защиту исторической правды. Государство заинтересовано в институционализации противодействия фальсификации истории любого рода, в том числе в компьютерных играх. В этих целях была образована Межведомственная комиссия по историческому просвещению⁹, создан Национальный центр исторической памяти при Президенте Российской Федерации¹⁰. О. В. Дамаскин, В. В. Красинский указывают, что «важным элементом борьбы с фальсификацией истории и реабилитации нацизма выступает информационная политика, основанная на использовании современных информационно-коммуникационных технологий и задействовании средств массовой коммуникации»¹¹.

Законодательного понятия исторической правды в правовой системе России не сформулировано, в доктринальных разработках под рассматриваемым термином понимают достоверную информацию о событиях прошлого, подтвержденную конкретными фактами, которая обладает социальной значимостью для общества и нуждается в защите от искажений¹².

В этой связи искажение (фальсификация) истории представляет собой процесс изменения, переписывания или неправильной интерпретации исторических фактов, событий таким образом, чтобы они соответствовали образам и определенным целям, идеям заинтересованных субъектов.

Многие исследователи отмечают, что активная деятельность нашего государства по нормативному закреплению различных аспектов сохранения памяти о прошлом началась совсем недавно и связана по большей части с принятием конституционных поправок¹³. Так, в 2020 г. Конституция РФ дополнена статьей 67.1, ч. 3 которой содержит норму о недопустимости умаления значения подвига народа при защите Отечества, а также закрепляет тезис о том, что в Российской Федерации обеспечивается защита исторической правды. До принятия указанной конституционной нормы в рамках «политики памяти»

⁸ В Кремле считают, что компьютерные игры становятся инструментом мягкой силы // URL: <https://tass.ru/obschestvo/15100395> (дата обращения: 17.03.2025).

⁹ Указ Президента РФ от 30.07.2021 № 442 «О Межведомственной комиссии по историческому просвещению» // СЗ РФ. 2021. № 31. Ст. 5896.

¹⁰ Указ Президента РФ от 02.11.2023 № 817 «О создании автономной некоммерческой организации «Национальный центр исторической памяти при Президенте Российской Федерации»» // СЗ РФ. 2023. № 45. Ст. 8034.

¹¹ Дамаскин О. В., Красинский В. В. Информационное противодействие фальсификации истории и реабилитации нацизма // Государство и право. 2021. № 6. С. 154.

¹² Москалев Г. Л. Охрана исторической правды: новая задача российского права // Журнал Сибирского федерального университета. Гуманитарные науки. 2022. № 15 (8). С. 1077.

¹³ См.: Воронова О. Е. Историческая политика Российской Федерации // Вопросы истории. 2021. № 11–3. С. 286.



также было сделано немало. Начиная с 1990-х гг. постепенно формируются правовые основы, в которых нашли отражение сведения о памятных датах, закрепление получили основные формы увековечения памяти о воинах России и др.¹⁴ Позже были сформулированы нормы об административной и уголовной ответственности за нарушение общественных отношений, складывающихся по вопросу сохранения исторической правды.

На сегодняшний день нормативную основу защиты исторической памяти составляют более 30 правовых акта, среди которых немаловажную роль играют документы стратегического планирования. Так, в 2024 г. был подписан Указ Президента РФ, в котором обоснована необходимость создания механизма государственного контроля за рынком компьютерных игр в целях исключения распространения продуктов, формирующих искаженное представление об истории нашей страны¹⁵.

В 2020 г. в Государственную Думу был внесен законопроект, предусматривающий установление уголовной ответственности за фальсификацию исторических фактов о причинах и итогах Второй мировой войны¹⁶. Данная инициатива была отклонена, так как предполагаемая ст. 354² УК РФ во многом совпадала с уже существующей ст. 354¹ УК РФ.

Кроме того, историческая память в соответствии с Указом Президента РФ признается традиционной ценностью российского общества¹⁷. Таким образом, все перечисленные инициативы и конкретные решения в рамках внутренней политики государства подчеркивают, что вопрос сохранения исторической правды является стратегически важной задачей для любой страны.

Достаточно популярным жанром компьютерных игр являются именно исторические, в которых неотъемлемым сюжетным компонентом выступают отдельные исторические периоды или события. Разработчики, создавая игровые продукты, зачастую искажают исторические факты, что формирует неправильное представление о прошлом.

И. Б. Кабыткина и А. Я. Володина называют следующие основные направления, в рамках которых фальсифицируются исторические факты: «Отрицание

¹⁴ Федеральный закон от 13.03.1995 № 32-ФЗ «О днях воинской славы и памятных датах России» // СЗ РФ. 1995. № 11. Ст. 943 ; Федеральный закон от 19.05.1995 № 80-ФЗ «Об увековечении Победы советского народа в Великой Отечественной войне 1941—1945 годов» // СЗ РФ. 1995. № 21. Ст. 1928 ; Федеральный закон от 12.01.1995 № 5-ФЗ «О ветеранах» // СЗ РФ. 1995. № 3. Ст. 168.

¹⁵ Указ Президента РФ от 08.05.2024 № 314 «Об утверждении Основ государственной политики Российской Федерации в области исторического просвещения» // СЗ РФ. 2024. № 20. Ст. 2587.

¹⁶ Проект федерального закона № 963440-7 «О внесении изменений в Уголовный кодекс Российской Федерации» (об установлении уголовной ответственности за фальсификацию исторических фактов о причинах и итогах Второй мировой войны) // URL: <https://sozd.duma.gov.ru/bill/963440-7> (дата обращения: 20.03.2025).

¹⁷ Указ Президента РФ от 09.11.2022 № 809 «Об утверждении Основ государственной политики по сохранению и укреплению традиционных российских духовно-нравственных ценностей» // СЗ РФ. 2022. № 46. Ст. 7977.

освободительного характера Великой Отечественной войны; умаление роли СССР в победе над фашизмом на территории Европы; обвинение России (как правопреемницы СССР) в разжигании Второй мировой войны» и др.¹⁸

Случаи недостоверной интерпретации исторических фактов были зафиксированы в серии игр Call of Duty, а также Company of Heroes 2, Commandos 3: Destination Berlin и др. Исследователи отмечают¹⁹, что наиболее фальсифицируемыми являются факты, относящиеся к периоду Второй мировой войны, а также конкретные события Великой Отечественной войны. В качестве примера приведем игру Command & Conquer: Red Alert, по сюжету которой наступление на Европу начинает не Гитлер, а Сталин, в процессе игры Советский Союз позиционируется в качестве врага²⁰. Роскомнадзор заблокировал данный игровой продукт на территории России.

Участившиеся случаи искажений сведений исторической памяти ставят вопрос о необходимости правовой оценки таких деяний.

Нормы об уголовной ответственности за фальсификацию истории появлялись в законодательстве РФ постепенно. В 2014 г. в УК РФ была введена ст. 354.1, которая должна была способствовать охране исторической памяти ввиду обострившихся политических событий, происходящих в Украине²¹. Однако технико-юридическое изложение этой нормы несовершенно. Например, проблемным аспектом при квалификации деяний, фальсифицирующих национальную историю в компьютерных играх, выступает вопрос об определении предмета преступления, а именно — заведомо ложных сведений о деятельности СССР в годы Второй мировой войны. В тексте уголовного закона не указаны признаки такой деятельности, т.е., по сути, она может включать в себя не только военные действия, но и внутреннюю, и внешнюю политику государства того периода. В этой связи также не в полной мере очевидно и само содержание ложных сведений.

Объективная сторона состава преступления описана в УК РФ следующими альтернативными действиями:

¹⁸ Кабыткина И. Б., Володина А. Я. Историческая правда как предмет фальсификации в современных политических условиях // Международный научно-исследовательский журнал. 2023. № 5 (131). С. 3.

¹⁹ См.: Белов С. И., Кротова А. А. Компьютерные игры как ресурс реализации политики памяти: практический опыт и скрытые возможности (на материалах позиционирования событий Великой Отечественной войны) // Вестник Московского государственного областного университета. Серия: История и политические науки. 2020. № 1. С. 54—63; Грибан И. В., Грибан О. Н. Играя в прошлое: репрезентация Второй мировой войны в компьютерных играх и проблема сохранения исторической памяти // Преподавание истории в школе. 2020. № 5. С. 41—47.

²⁰ См.: Федорченко С. Н. Интерпретация событий Великой Отечественной войны в компьютерных играх: риски и перспективы легитимации режима через политику памяти // Постсоветские исследования. 2020. Т. 3. № 5. С. 433.

²¹ Пошелов П. В. Уголовно-правовая оценка реабилитации нацизма : дис. ... канд. юрид. наук. Омск, 2023. С. 6.



а) отрицание фактов, установленных приговором Международного военного трибунала для суда и наказания главных военных преступников европейских стран оси;

б) одобрение преступлений, установленных указанным приговором;

в) распространение заведомо ложных сведений о деятельности СССР в годы Второй мировой войны, о ветеранах Великой Отечественной войны.

В теории уголовного права нет единства по определению правовой природы компьютерных игр. Так, одними юристами они признаются в качестве результата интеллектуальной деятельности; другими рассматриваются как информация; некоторыми — как средство коммуникации и, наконец, — как предмет игрового характера²².

Давая правовую оценку рассматриваемых деяний, необходимо обратить внимание на два момента. Во-первых, сама по себе компьютерная игра в рамках сюжета может содержать заведомо ложные сведения, что дает основание понимать ее в качестве информационного продукта. Во-вторых, осуществление действий по фальсификации истории может происходить в чатах компьютерных игр, что характеризуется в качестве способа совершения преступления.

С точки зрения уголовного права игровой продукт лучше понимать как способ подачи информации, но не информацию как таковую. Обязательным условием наступления уголовной ответственности по ч. 1 ст. 354¹ УК РФ является признак публичности. Пленум Верховного Суда РФ ориентирует правоприменителя при установлении публичности учитывать место, способ, обстановку и другие обстоятельства дела (обращения к группе людей в общественных местах, на собраниях, митингах, демонстрациях, распространение листовок, вывешивание плакатов, распространение обращений путем массовой рассылки сообщений абонентам мобильной связи и т.п.). Некоторые исследователи применительно к социальным сетям отмечают, что «криминализация способов обмена информацией обусловлена таким их свойством, как публичность»²³.

Если же фальсифицированные сведения распространяются в чатах компьютерных игр, то игры признаются средством коммуникации пользователей, что дает основание рассматривать их в качестве разновидности мессенджеров. В данном случае уголовно-правовую оценку можно основывать на п. «в» ч. 2 ст. 354¹ УК РФ.

Пока не сложилось практики привлечения к уголовной ответственности за фальсификацию национальной истории в компьютерных играх, что во многом связано с несформированным правовым регулированием компьютерной индустрии в России. На наш взгляд, трудностью также является и то, что

²² Архипов В. В., Васильев А. А., Андреев Н. Ю., Печатнова Ю. В. Компьютерные игры в юридических исследованиях: к вопросу о предпосылках модели регулирования // Вестник Санкт-Петербургского университета. Право. 2023. Т. 14. № 1. С. 12.

²³ Пестерева Ю. С., Пошелов П. В., Рагозина И. Г., Чекмезова Е. И. Уголовно-правовая характеристика способов обмена информацией в социальных сетях на примере статей 148, 282, 354¹ УК РФ // Вестник Томского государственного университета. Право. 2020. № 35. С. 118.

большинство компьютерных игр создано зарубежными студиями, чем обусловлено решение данной проблемы путем блокировки противоправного контента.

Сейчас в Государственной Думе находится законопроект, который нацелен на регулирование общественных отношений, возникающих в связи с разработкой и распространением видеоигр на территории Российской Федерации, а также на установление ограничений осуществления данной деятельности. Кроме того, предлагаемый законопроект включает регламентацию требований как к организаторам сервисов распространения компьютерных игр, так и к лицам, их распространяющим²⁴. Таким образом, появление у разработчиков определенных обязанностей может способствовать применению уголовно-правовых средств в данной сфере.

Подводя итог, отметим, что участвовавшие случаи фальсификации истории в компьютерных играх ставят вопрос о правовой оценке таких действий. Связано это с тем, что компьютерные игры рассматриваются не только как сегмент развлекательной индустрии, но и как сильнейший транслятор ценностей, идей, культурных установок. Искажение исторических фактов может привести к формированию неверных представлений о прошлом, нарушению исторической памяти народа и обострению межнациональных конфликтов.

На данный момент до конца не решен вопрос о правовой природе компьютерных игр, что, на наш взгляд, мешает реализации потенциала уголовно-правовых норм, охраняющих историческую память.

Таким образом, необходимо выработать подход, при котором право способствовало бы созданию качественных игровых продуктов, а не становилось барьером для развития отрасли компьютерных игр в целом.

БИБЛИОГРАФИЯ

1. *Архипов В. В., Васильев А. А., Андреев Н. Ю., Печатнова Ю. В.* Компьютерные игры в юридических исследованиях: к вопросу о предпосылках модели регулирования // Вестник Санкт-Петербургского университета. — Право. — 2023. — Т. 14. — № 1. — С. 5—21.
2. *Белов С. И.* Компьютерные игры как инструмент реализации политики памяти (на примере отображения событий Великой Отечественной войны в видеоиграх) // Вестник Российского университета дружбы народов. — Серия : Политология. — 2018. — Т. 20. — № 1. — С. 96—104.
3. *Белов С. И., Кретьова А. А.* Компьютерные игры как ресурс реализации политики памяти: практический опыт и скрытые возможности (на материалах позиционирования событий Великой Отечественной войны) // Вестник Московского государственного областного университета. — 2020. — № 1. — С. 54—63.
4. *Воронова О. Е.* Историческая политика Российской Федерации // Вопросы истории. — 2021. — № 11—3. — С. 282—287.

²⁴ Проект федерального закона № 795581-8 «О деятельности по разработке и распространению видеоигр на территории Российской Федерации» // URL: <https://sozd.duma.gov.ru/bill/795581-8?ysclid=m8v5zi5vpn682752673> (дата обращения: 29.03.2025).



5. *Грибан И. В., Грибан О. Н.* Играя в прошлое: репрезентация Второй мировой войны в компьютерных играх и проблема сохранения исторической памяти // Преподавание истории в школе. — 2020. — № 5. — С. 41—47.
6. *Дамаскин О. В., Красинский В. В.* Информационное противодействие фальсификации истории и реабилитации нацизма // Государство и право. — 2021. — № 6. — С. 147—157.
7. *Кабыткина И. Б., Володина А. Я.* Историческая правда как предмет фальсификации в современных политических условиях // Международный научно-исследовательский журнал. — 2023. — № 5 (131). — С. 1—4.
8. *Лушин А. Н.* Фальсификация истории: теоретический подход к проблеме (на примере России) // Вестник Нижегородской академии МВД России. — 2013. — № 23. — С. 21—25.
9. *Москалев Г. Л.* Охрана исторической правды: новая задача российского права // Журнал Сибирского федерального университета. — Гуманитарные науки. — 2022. — № 15 (8). — С. 1070—1081.
10. *Пестерева Ю. С., Пошелов П. В., Рагозина И. Г., Чекмезова Е. И.* Уголовно-правовая характеристика способов обмена информацией в социальных сетях на примере статей 148, 282, 3541 УК РФ // Вестник Томского государственного университета. — Право. — 2020. — № 35. — С. 112—121.
11. *Пошелов П. В.* Уголовно-правовая оценка реабилитации нацизма : дис. ... канд. юрид. наук. — Омск, 2023. — 193 с.
12. *Федорченко С. Н.* Интерпретация событий Великой Отечественной войны в компьютерных играх: риски и перспективы легитимации режима через политику памяти // Постсоветские исследования. — 2020. — Т. 3. — № 5. — С. 427—438.
13. *Федорченко С. Н., Тедиков Д. О., Теслюк К. В., Маркарян Р. А.* Сетевые компьютерные игры в эпоху цифровизации: новые угрозы или потенциалы для реализации политики памяти? // Вестник Московского государственного областного университета (электронный журнал). — 2019. — № 3. — С. 73—78.

Теоретические и практические аспекты квалификации различных форм участия в публично демонстрируемых преступлениях против личности

Аннотация. В статье разработаны концептуальные основы уголовно-правовой квалификации общественно опасных деяний зрителей онлайн-трансляций преступлений против личности. В структуре аудитории деструктивного контента, демонстрируемого в режиме реального времени, автором выделяются три группы лиц: активные спонсоры, интерактивные зрители и пассивные («теневые») наблюдатели. Делается вывод, что пользователи стриминговых сервисов, осуществляющие материальное стимулирование в форме донатов создателя запрещенного онлайн-контента, должны привлекаться к уголовной ответственности в качестве подстрекателей к преступлению; участники виртуальной трансляции преступления, проявляющие пользовательскую активность в виде положительной обратной связи, рассматриваемые как пособники общественно опасного посягательства, пассивных («теневых») наблюдателей, увеличивающих охват интернет-трансляций противоправных действий, необходимо наказывать в уголовно-правовом порядке за несообщение о преступлении против личности или за оставление в опасности. В настоящем исследовании предложено восстановить институт прикосновенности к преступлению в российском законодательстве, расширить субъектный состав уголовно-правовой нормы об оставлении в опасности, включить признак публичной демонстрации противоправных действий в ст. 125 УК РФ. Данные изменения направлены на повышение социальной ответственности граждан и предотвращение преступных посягательств против личности.

Ключевые слова: публичная демонстрация, онлайн-трансляция, треш-стрим, донаты, подстрекательство к преступлению, пособничество в преступлении, преступления против личности, оставление в опасности, прикосновенность к преступлению, несообщение о преступлении



Ирина Александровна ЮРЧЕНКО,
доцент кафедры
уголовного права
Университета имени
О.Е. Кутафина (МГЮА),
кандидат юридических
наук, доцент
iajurchenko@msal.ru
125993, Россия, г. Москва,
ул. Садовая-Кудринская,
д. 9

DOI: 10.17803/2311-5998.2025.129.5.093-101

Irina A. YURCHENKO,

Associate Professor of the Chair of Criminal Law
of the Kutafin Moscow State Law University (MSAL),

Cand. Sci. (Law), Associate Professor

iajurchenko@msal.ru

9, ul. Sadovaya-Kudrinskaya, Moscow, Russia, 125993

Theoretical and Practical Aspects of Qualification of Various Forms of Participation in Publicly Demonstrated Crimes against the Person

Abstract. *The article develops conceptual bases of criminal-legal qualification of socially dangerous acts of viewers online-broadcasts of crimes against personality. In the structure of the audience of destructive content, shown in real time, the author distinguishes three groups of persons: active sponsors, interactive viewers and passive («shadow») observers. It is concluded that streaming service users who materially incentivize the creator of prohibited online content in the form of donates should be held criminally liable as instigators of crime, participants of the virtual broadcast of the crime, showing user activity in the form of positive feedback, are considered as accomplices of socially dangerous assault, passive («shady») observers, increasing Internet coverage the transmission of unlawful acts, it is necessary to punish in criminal law for failure to report a crime against the person or for leaving in danger. In the present study it is proposed to restore the institution of touch to a crime in Russian legislation, to expand the subject-matter of criminal law rules on putting at risk, to include the feature of public demonstration of unlawful acts in article 125 CC. These changes are aimed at increasing the social responsibility of citizens and preventing criminal attacks against the person.*

Keywords: *public demonstration, online broadcast, trash-streaming, donations, incitement to a crime, aiding and abetting a crime, crimes against the person, leaving in danger, involvement in a crime, failure to report a crime*

В 1984 г. суд города Нью-Бедфорда штата Массачусетс рассмотрел дело о групповом изнасиловании, совершенном в баре «Большой Дэн» на глазах многочисленных посетителей. Потерпевшей была двадцатидвухлетняя местная жительница Шерил Араужо, согласно показаниям которой 6 марта 1983 г. около девяти вечера, оставив дома двух малолетних детей, она пришла в бар, чтобы купить сигареты. В баре находилось около десяти мужчин, двое из которых предложили отвезти ее домой. После отказа молодую женщину сбили с ног, отнесли на бильярдный стол, раздели и неоднократно изнасиловали. Присутствующие при этом зрители так или иначе высказывали одобрение происходящему путем одобрительных криков, аплодисментов, свиста и т.п. Изнасилование осуществлялось в течение двух часов. Никто из очевидцев преступления, которые находились в заведении, не вызвал полицию и не пресек преступные действия.

Попытки бармена позвонить в полицию пресекались двумя посетителями, которые выкрикивали в адрес насильников указания продолжать сексуальные действия в отношении потерпевшей. Было установлено, что свидетелями изнасилования стали также лица, которые заглядывали в окна бара, чтобы узнать причину шума, но в само заведение не заходили. Около полуночи женщине удалось выбежать из бара, остановить проезжающую машину и попросить помощи¹.

Таким образом, лиц, причастных к публичному изнасилованию Шерил Араужо, можно разделить на несколько групп: 1) непосредственные исполнители преступления (активные участники, основные фигуранты); 2) соучастники преступления, поддерживающие действия исполнителей (второстепенные фигуранты); 3) наблюдатели (бездействующие свидетели преступления); 4) мимолетные очевидцы (случайные свидетели).

Из-за отсутствия должной правовой регламентации состава изнасилования и ответственности за несообщение о преступлении в качестве обвиняемых были привлечены только шестеро мужчин, из которых четверо были признаны присяжными заседателями виновными в совершении квалифицированного изнасилования, а двое, блокировавших доступ к телефону, оправданы ввиду отсутствия достаточных доказательств их соучастия. В ходе судебного следствия было установлено, что только один из четырех осужденных совершил естественное половое сношение с потерпевшей, еще двое совершили половой контакт в извращенной форме, а четвертый помогал трем путем удерживания потерпевшей силой².

В обществе вердикт суда был воспринят неоднозначно в связи с рядом нетипичных обстоятельств дела:

- судебный процесс об изнасиловании впервые в истории США транслировался по телевидению;
- персональные данные потерпевшей Шерил Араужо были оглашены в прямом эфире одной из сторон, участвующей в деле, что в дальнейшем привело к ее травле;
- обвиняемые имели португальское происхождение, что широко освещалось в средствах массовой информации и вызвало у американского населения антипортугальские настроения (призывы выслать португальцев в Европу, не поддерживать материально их бизнес и т.п.), в связи с чем португальская диаспора Нью-Бедфорда сочла необходимым встать на защиту обвиняемых;
- потерпевшая Шерил Араужо также имела португальское происхождение, но в отношении нее публика и члены португальской общины были настроены отрицательно из-за ее аморального образа жизни и виктимного поведения в день совершения преступления;
- сразу после изнасилования Шерил Араужо женские организации оказали поддержку потерпевшей, организовав перед мэрией Нью-Бедфорда марш протеста, участники которого несли плакат «Изнасилование — это не зрелищный вид спорта»;

¹ Chancer Lynn S. New Bedford, Massachusetts, March 6, 1983 — March 22, 1984: The «Before and after» of a Group Rape // *Gender and Society*. 1987. Vol. 1. № 3. P. 239—240, 245.

² Chancer Lynn S. Op. cit. P. 245—250.



— после вынесения приговора произошли массовые протесты в поддержку осужденных, участники которых сочли назначенное наказание слишком суровым по причине их этнического происхождения³.

В 1986 г. Шерил Араужо, находясь в состоянии опьянения, не справилась с управлением и погибла в автокатастрофе⁴. В 1987 г. Верховный суд штата Массачусетс отклонил апелляцию осужденных за изнасилование в баре «Большой Дэн», оставив вынесенный приговор в силе. Из четырех трое виновных подлежали наказанию в виде тюремного заключения в диапазоне от 9 до 12 лет, а один — в диапазоне от 6 до 8 лет⁵. Мировую известность делу об изнасиловании в местном баре принес снятый в 1988 г. художественный фильм «Обвиняемые» с Джо-ди Фостер в главной роли, которая получила за нее премию «Оскар». Слоганом фильма стала фраза: «Первый крик был о помощи. Второй — о справедливости»⁶.

Дело об изнасиловании Шерил Араужо стало одним из первых мейнстримовых дел, получившим широкую огласку благодаря его освещению средствами массовой информации в режиме реального времени. Оно также поставило вопросы об уголовной ответственности свидетелей, которые наблюдали за совершением преступления или поощряли его. В 1983 г. законодательная конструкция состава изнасилования, ответственность за которое предусмотрена в § 22 гл. 265 Закона штата Массачусетс об изнасилованиях и преступлениях на сексуальной почве⁷, соответствовала современному описанию, закрепленному в ст. 131 УК РФ (потерпевшей может быть только женщина, субъектом преступления — мужчина, половое сношение совершается без согласия жертвы и только в естественной форме, насилие применяется по отношению к потерпевшей).

Публичное судебное разбирательство дела об изнасиловании Шерил Араужо дало толчок к реформированию данной уголовно-правовой нормы, и в настоящее время состав изнасилования включает в себя не только естественную, но и противоестественную насильственную половую связь. Также была усовершенствована норма о соучастии в преступлении и несообщении о преступлении.

Примечательным является обстоятельство, что в том же 1984 г., когда проходил судебный процесс по делу Шерил Араужо, была создана открытая, но пока только для образовательных учреждений, сеть NSFNET, ставшая предвестником Интернета, появление которого привело к возникновению ранее неизвестных проблем, в частности, возможности совместного совершения преступлений на расстоянии без необходимости личного контакта между соучастниками, проведение домашних лайв-трансляций треш-контента, зрителями которых может быть неопределенный круг лиц. Через 35 лет на платформе Netflix состоялась премьера документального сериала Trial by Media («Суд над Медиа»), снятого под руководством исполнительного продюсера Джорджа Клуни, в пятом эпизоде

³ Chancer Lynn S. Op. cit. P. 239—240, 248—253.

⁴ New Bedford Rape Victim Dies // Off Our Backs. 1987. Vol. 17. № 2. P. 7.

⁵ New Bedford Rapists Lose Appeal // Off Our Backs. 1988. Vol. 18. № 4. P. 8.

⁶ The Accused // URL: <https://www.imdb.com/title/tt0094608/> (дата обращения: 2 апреля 2025 г.).

⁷ Massachusetts law about rape and sex crimes // URL: <https://www.mass.gov/info-details/mass-general-laws-c265-ss-22> (дата обращения: 2 апреля 2025 г.).

которого на примере дела об изнасиловании в 1983 г. Шерил Араужо в баре «Большой Дэн» обсуждалась проблема этичности использования средствами массовой информации онлайн-трансляций шокирующего контента для расширения своей аудитории⁸.

В российском уголовном законодательстве признак совершения преступления против личности с его публичной демонстрацией, в том числе в средствах массовой информации или информационно-телекоммуникационных сетях (включая сеть Интернет), появился в 2024 г. в целях противодействия распространению в информационном пространстве деструктивного контента в виде треш-стримов⁹. В этой связи необходимо определить, какой смысл законодатель придает указанному признаку. Согласно буквальному толкованию, преступление может совершаться с его публичной демонстрацией и без использования средств массовой информации, а также информационно-телекоммуникационных сетей, включая сеть Интернет.

Примером может служить ч. 2 ст. 128¹ УК РФ в случае совершения клеветы в публично демонстрирующемся произведении. Но вряд ли квалифицирующий признак публичной демонстрации применительно к преступлениям против личности подразумевает их совершение в обычном общественном пространстве, например на улице. В пояснительной записке к проекту федерального закона «О внесении изменений в Уголовный кодекс Российской Федерации» признак «совершение преступления с публичной демонстрацией, в том числе в средствах массовой информации или информационно-телекоммуникационных сетях (включая сеть Интернет)» понимается в узком смысле, как совершение общественно опасного деяния исключительно в цифровом пространстве.

Применительно к ст. 242 и 242¹ УК РФ Верховный Суд РФ разъяснил, что публичная демонстрация с использованием электронных или информационно-телекоммуникационных сетей, включая сеть Интернет, может иметь две формы: онлайн-показ и размещение запрещенной законом информации (материалов, сведений) на личных страницах и на страницах групп пользователей (в социальных сетях или на интернет-страницах)¹⁰.

Некоторые авторы распространяют данное понятие и на ситуации публичной демонстрации преступлений против личности¹¹. Представляется, что публич-

⁸ Trial by Media: a troubling Netflix series on press coverage of the courtroom // URL: <https://www.theguardian.com/tv-and-radio/2020/may/11/trial-by-media-troubling-netflix-series-press-coverage-courtroom> (дата обращения: 03.04.2025).

⁹ Пояснительная записка к проекту федерального закона «О внесении изменений в Уголовный кодекс Российской Федерации» // URL: <https://sozd.duma.gov.ru/bill/506240-8> (дата обращения: 03.04.2025).

¹⁰ Постановление Пленума Верховного Суда РФ от 15.12.2022 № 37 «О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть Интернет». П. 22 // Российская газета. 28 декабря 2022 г.

¹¹ Левандовская М. Г. Условия применения единообразного подхода к конструированию квалифицирующего признака публичной демонстрации совершения преступлений против личности // Юридическая наука. 2024. № 10. С. 265.



ная демонстрация преступлений против личности заключается только в их онлайн-трансляции, исходя из того, что стрим (англ. stream — поток, течение, потоковый), в том числе треш-стрим, представляет собой прямой эфир. По своей сути публичная демонстрация — это интерактивные действия, которые происходят в режиме реального времени и доступны для просмотра онлайн (прямые трансляции, стримы, онлайн-презентации и другие формы показа информации, которые происходят «здесь и сейчас»).

Публичное распространение представляет собой размещение информации в сети Интернет, где она становится доступной для неопределенного круга лиц для ознакомления в любое время. Таким образом, публичная демонстрация и публичное распространение различаются по времени передачи медиаконтента, его доступности и продолжительности. Следует иметь в виду, что не любая онлайн-трансляция является стримом, который характеризуется интерактивностью и вовлеченностью участников. Телевизионные передачи в режиме реального времени зачастую не обладают такими признаками, а представляют собой потоковое видео (трансляции спортивных соревнований, мероприятий и т.п.), на которое не влияют зрители.

Учитывая, что появление признака публичной демонстрации в качестве квалифицирующего обусловлено борьбой с треш-стримами, что отражено в пояснительной записке к упомянутому законопроекту, можно уверенно говорить, что средства массовой информации указаны в соответствующих статьях излишне. Кроме того, можно согласиться с тем, что публичная демонстрация преступных посягательств на личность через традиционные средства массовой информации практически невозможна в силу цензурирования подобного контента¹².

Следовательно, рассматривать средства массовой информации отдельно от информационно-телекоммуникационных сетей не требуется, поскольку они соотносятся между собой как общее и частное. Например, интернет-канал известного блогера может быть зарегистрирован как средство массовой информации. Онлайн-показ деструктивного контента на таком канале будет квалифицироваться как преступление, совершенное путем публичной демонстрации в информационно-телекоммуникационной сети, включая сеть Интернет. С учетом изложенного необходимо скорректировать признак публичной демонстрации: «то же деяние, совершенное с публичной демонстрацией в информационно-телекоммуникационных сетях, включая сеть Интернет».

Возвращаясь к делу Шерил Араужо, можно констатировать, что появление интернет-технологий не упразднило, а лишь актуализировало древнюю формулу «хлеба и зрелищ». Современные онлайн-трансляции, подобно делу Шерил Араужо, демонстрируют неизменную природу людей, когда совершение публичных преступных действий вызывает спектр реакций — от пассивного наблюдения до активного участия в них, что свидетельствует о технологической трансформации форм, но сохранении сущностных характеристик коллективного поведения.

В настоящее время все также среди зрителей теперь уже онлайн-трансляций деструктивного контента о посягательствах на личность можно выделить несколько категорий: 1) активные участники, которые осуществляют монетизацию

¹² Левандовская М. Г. Указ. соч. С. 265.

контента, финансируют совершение преступления против личности (аудиторный актив); 2) вовлеченные пользователи, которые поддерживают стримера с помощью механизма обратной связи в виде одобрительных интерактивных реакций (лайков, положительных комментариев), т.е. виртуальная группа поддержки; 3) «теневые» зрители — реальные участники стрима, которые регулярно смотрят онлайн-трансляции полностью, часто заходят на стримы к одному и тому же стримеру или по одной и той же теме контента, но себя не проявляют, хотя охват просмотров повышают; 4) фоновый контингент, к которому относятся боты, заброшенные аккаунты, числящиеся в подписчиках стримера, призрачные зрители, которые подключились к трансляции, но не смотрят ее или смотрят «фоном», не вникая в суть, а также случайно зашедшие и сразу вышедшие, которым не нравятся треш-стримы.

Проводя аналогию с делом Шерил Араужо, к активным участникам публично-го изнасилования можно отнести лиц, которые помогали непосредственному исполнителю держать потерпевшую, раздевали ее, вовлеченными пользователями являлись посетители бара, которые путем улюлюканья, слов, выкриков, свиста поддерживали насильников, «теневые» зрители наблюдали весь процесс совершения преступления, не одобряя исполнителей, но и не мешая им, а «фоновым» контингентом следует признать тех лиц, которые заглядывали в окна бара и, увидев, что происходит, просто уходили, относясь к происходящему безразлично.

Первая категория лиц (донатеры) является либо подстрекателями к совершению преступления, если стример начинает преступные действия (например, убийство) только при условии монетизации контента, либо пособниками, когда стример продолжает начатые действия при перечислении ему донатов. Вторая группа лиц представляет собой пособников, так как они поддерживают решимость виновного к продолжению преступления и доведению его до конца. Третья группа лиц должна нести ответственность за несообщение о преступлении или за оставление в опасности. Четвертую группу лиц нельзя привлечь к уголовной ответственности, так как у них, как правило, отсутствует осознание, что в данный момент совершаются преступные деяния из-за кратковременности увиденного и не возникает желание узнать, что происходит.

В связи с этим с учетом новой формы совершения преступления, когда широкий круг лиц может не просто наблюдать процесс совершения преступления, но и участвовать в нем, когда пассивное присутствие тем не менее приносит дивиденды стримеру в виде увеличения количества просмотров, целесообразно возродить в российском уголовном законодательстве полноценный институт прикосновенности к преступлению по аналогии с советским законодательством, а также придать новое звучание ч. 1 ст. 127 УК РСФСР 1960 г. путем закрепления данной уголовно-правовой нормы в ст. 125 УК РФ: «1. Неоказание лицу, находящемуся в опасном для жизни и здоровья состоянии, необходимой и явно не терпящей отлагательства помощи, если она заведомо могла быть оказана виновным без серьезной опасности для себя или других лиц, либо несообщение надлежащим учреждениям или лицам о необходимости оказания помощи — наказывается...». Действующую редакцию ст. 125 УК РФ предлагается перенести в ч. 2, а в качестве квалифицирующего признака предусмотреть совершение указанных в ч. 1



и 2 деяний с публичной демонстрацией их в информационно-телекоммуникационных сетях, включая сеть Интернет.

Наличие уголовной ответственности за недоносительство (несообщение) о преступлении в уголовном законодательстве разных эпох зависит от общественно-политического устройства и доминирующей правовой доктрины. В советское время донесение о преступлениях, перечисленных в ст. 88.1 и 190 УК РСФСР, рассматривалось как активная сознательная помощь граждан в борьбе с преступностью¹³, а сейчас введение уголовной ответственности за несообщение о преступлении связывается с ущемлением конституционных прав и свобод граждан¹⁴.

Несмотря на различный подход к сущности несообщения о преступлении, такая норма в контексте исследуемой темы может иметь профилактическое значение для пассивных наблюдателей за публичной демонстрацией в цифровом пространстве совершения преступления против личности. В связи с этим следует поддержать предложение о перемещении ст. 205⁶ УК РФ в главу о преступлениях против правосудия и расширения перечня преступлений, несообщение о которых является преступлением.

С точки зрения правоприменения может возникнуть вопрос о разграничении предлагаемых составов оставления в опасности в форме несообщения надлежащим учреждениям или лицам о необходимости оказания помощи и несообщения об известных готовящихся или совершенных преступлениях. Разница между указанными преступлениями заключается в том, что оставление в опасности — это самостоятельное преступление, совершаемое в определенный момент времени, когда человеку грозит немедленная смерть или тяжкий вред здоровью, о чем лицо сообщает компетентным органам, а несообщение осуществляется о готовящемся или уже произошедшем преступлении. Состав несообщения о преступлении должен применяться к лицам, которые ознакомились, в частности, с размещенной в сети Интернет видеозаписью проведенного стрима и не заявили об этом в правоохранительный орган. В целом институт прикосновенности к преступлению должен повысить социальную активность и сознательность граждан, чтобы они не игнорировали факты совершения преступлений.

По итогам проведенного исследования можно сделать ряд выводов и предложений:

1) среди зрителей онлайн-трансляций деструктивного контента о посягательствах на личность можно выделить несколько категорий: а) активные участники, которые осуществляют монетизацию контента; б) пользователи, которые поддерживают стримера с помощью механизма обратной связи в виде одобрительных интерактивных реакций; в) «теневые» зрители — реальные участники стрима, которые регулярно смотрят онлайн-трансляции полностью, но себя никак не проявляют, однако их присутствие повышает количество просмотров контента; г) фоновый контингент — призрачные зрители;

¹³ Носкова Н. А. Недонесение о преступлении по советскому уголовному праву : дис. ... канд. юрид. наук : 12.00.00. М., 1971. С. 3.

¹⁴ Крутикина Ю. А. Уголовная ответственность за несообщение о преступлении : дис. ... канд. юрид. наук : 12.00.08. М., 2020. С. 9.

2) нужно скорректировать признак публичной демонстрации следующим образом: «то же деяние, совершенное с публичной демонстрацией в информационно-телекоммуникационных сетях, включая сеть Интернет»;

3) под публичной демонстрацией следует понимать интерактивные действия, которые происходят в режиме реального времени и доступны только для просмотра онлайн;

4) предлагается расширить состав оставления в опасности путем включения в ст. 125 УК РФ уголовно-правовой нормы следующего содержания: «Неоказание лицу, находящемуся в опасном для жизни и здоровья состоянии, необходимой и явно не терпящей отлагательства помощи, если она заведомо могла быть оказана виновным без серьезной опасности для себя или других лиц, либо несообщение надлежащим учреждениям или лицам о необходимости оказания помощи — ...»;

5) следует переместить ст. 205⁶ УК в главу о преступлениях против правосудия и расширить перечень преступлений, несообщение о которых является преступлением;

6) отличия между оставлением в опасности и несообщением о преступлении заключается в том, что оставление в опасности представляет собой самостоятельное преступление, совершаемое в определенный момент времени, когда человеку грозит немедленная смерть или тяжкий вред здоровью, о чем лицо сообщает компетентным органам, а несообщение **осуществляется о готовящемся или уже произошедшем преступлении.**

БИБЛИОГРАФИЯ

1. Крутикина Ю. А. Уголовная ответственность за несообщение о преступлении : дис. ... канд. юрид. наук : 12.00.08. — М., 2020. — 255 с.
2. Левандовская М. Г. Условия применения единообразного подхода к конструированию квалифицирующего признака публичной демонстрации совершения преступлений против личности // Юридическая наука. — 2024. — № 10.
3. Носкова Н. А. Недонесение о преступлении по советскому уголовному праву : дис. ... канд. юрид. наук : 12.00.00. — М., 1971. — 255 с.
4. Chancer Lynn S. New Bedford, Massachusetts, March 6, 1983 — March 22, 1984: The «Before and after» of a Group Rape // Gender and Society. — 1987. — Vol. 1. — № 3.
5. Massachusetts law about rape and sex crimes // URL: <https://www.mass.gov/info-details/mass-general-laws-c265-ss-22> (дата обращения: 2 апреля 2025 г.).
6. New Bedford Rape Victim Dies // Off Our Backs. — 1987. — Vol. 17. — № 2.
7. New Bedford Rapists Lose Appeal // Off Our Backs. — 1988. — Vol. 18. — № 4.
8. Trial by Media: a troubling Netflix series on press coverage of the courtroom // URL: <https://www.theguardian.com/tv-and-radio/2020/may/11/trial-by-media-troubling-netflix-series-press-coverage-courtroom> (дата обращения: 3 апреля 2025 г.).





**Александрина Сергеевна
РУБЦОВА,**
доцент кафедры
уголовного права
Университета имени
О.Е. Кутафина (МГЮА),
кандидат юридических наук,
доцент
asrubtsova@msal.ru
125993, Россия, г. Москва,
ул. Садовая-Кудринская, д. 9



**Тамара Дмитриевна
УСТИНОВА,**
профессор кафедры
уголовного права
Университета имени
О.Е. Кутафина (МГЮА),
доктор юридических наук,
профессор
tdustinova@msal.ru
125993, Россия, г. Москва,
ул. Садовая-Кудринская, д. 9

Коммерческий секс и виртуальная реальность: уголовно-правовой аспект

Аннотация. В статье рассмотрены актуальные уголовно-правовые вопросы, связанные с распространением половых преступлений с использованием метaprостранства и с вовлечением в занятие проституцией в информационно-телекоммуникационной сети Интернет, а также даны рекомендации по совершенствованию противодействия этим явлениям. Актуальность работы обусловлена тем, что коммерческий секс в цифровую эпоху активно трансформируется благодаря развитию технологий, таких как виртуальная реальность, метавселенные и искусственный интеллект. Эти инновации открывают новые возможности для удовлетворения интимных потребностей, но одновременно создают вызовы для правовой системы и общества. Авторы делают вывод, что правоприменитель может адаптировать существующие практики, чтобы защитить общество от новых угроз, сохраняя баланс между инновациями и безопасностью, в то же время не создавая искусственно новых составов преступления. С данными негативными проявлениями возможно бороться с помощью уже существующих норм, если внести в них дополнения с учетом процессов, появляющихся в метамире.

Ключевые слова: общественная нравственность, изнасилование, половые преступления, вовлечение в занятие проституцией

DOI: 10.17803/2311-5998.2025.129.5.102-111

Aleksandrina S. RUBTSOVA,

Associate Professor of the Department of Criminal Law
of the Kutafin Moscow State Law University (MSAL),
Cand. Sci. (Law), Associate Professor
asrubtsova@msal.ru
9, ul. Sadovaya-Kudrinskaya, Moscow, Russia, 125993

Tamara D. USTINOVA,

Professor of the Department of Criminal Law
of the Kutafin Moscow State Law University (MSAL),
Dr. Sci. (Law), Professor
tdustinova@msal.ru
9, ul. Sadovaya-Kudrinskaya, Moscow, Russia, 125993

Commercial Sex and Virtual Reality: Criminal Law Aspect

Abstract. *The article discusses the actual criminal legal issues related to the spread of sexual crimes using the meta-space and involving prostitution in the information and telecommunication Internet, as well as recommendations for improving counteracting these phenomena. The relevance of the work is due to the fact that commercial sex in the digital era is actively transformed, thanks to the development of technology, such as virtual reality, metaverse and artificial intelligence. These innovations open up new opportunities to satisfy intimate needs, but at the same time create challenges for the legal system and society. The authors conclude that the law enforcer can adapt existing practices in order to protect society from new threats, maintaining a balance between innovation and safety, at the same time, without creating artificially new corpus delicti. With these negative manifestations, it is possible to fight with the help of existing norms if added to them, taking into account the processes that appear in metaverse.*

Keywords: *public morality, rape, sexual crimes, involvement in prostitution*

Коммерческий секс в цифровую эпоху активно трансформируется благодаря развитию технологий, таких как виртуальная реальность (VR), метавселенные и искусственный интеллект (ИИ). Эти инновации открывают новые возможности для удовлетворения интимных потребностей, но одновременно создают вызовы для правовой системы и общества. Уже сейчас стоит задуматься о социальных, психологических и правовых последствиях, технологических рисках, которые станут распространенными в недалеком будущем. В средствах массовой информации появляются материалы о том, что данная сфера весьма востребована¹. Подобная деятельность всегда включала в себя коммерческую

¹ В 2023 г. россияне купили более 50 млн товаров категории «18+» // URL: <https://www.mn.ru/smart/v-2023-godu-rossiyane-kupili-bolee-50-mln-tovarov-v-kategorii-18-gde-v-moskve-iskat-seks-igrushki-i-skol-ko-oni-stoyat>.



деятельность по производству и реализации товаров и услуг сексуального характера. И нет ничего удивительного, что данная индустрия активно развивается и в виртуальном пространстве, в том числе и сфера личных взаимоотношений, связанных с удовлетворением интимных потребностей. Существуют приложения для знакомств, форумы для общения с учетом не самых одобряемых обществом запросов и влечений людей.

Еще на заре Интернета стали появляться чаты, в которых пользователи занимались «виртуальным сексом», на тот момент это был обмен текстовыми сообщениями интимного содержания. В настоящее время возможности виртуальной вселенной существенно расширились, существует отдельная ниша игр, связанных с сексом, сексуальным насилием и более жесткими девиациями. Новым явлением стали секс-игры с использованием искусственного интеллекта. Такие игры задействуют самые сокровенные желания и фантазии пользователей, предлагая им безопасное пространство для исследования без осуждения или последствий. Привлекательность заключается в настройке и контроле — пользователи могут создавать своих идеальных партнеров и сценарии.

Еще одно новое явление — это появление метавселенных, постоянно существующее виртуальное пространство, в котором люди могут взаимодействовать друг с другом и с цифровыми объектами через свои аватары, с помощью технологий виртуальной реальности. Практически это полноценная виртуальная жизнь, где можно построить любые отношения и общаться с другими людьми. Возникает резонный вопрос: если виртуальный мир всегда был привлекателен для любителей острых ощущений именно иллюзией вседозволенности и безопасности, не таят ли данные технологии новые угрозы?

В начале 2025 г. появилась новость, что британская полиция расследует случай с изнасилованием 16-летней девушки в метавселенной. По ее заявлению ее виртуальный аватар в VR-игре подвергся насилию со стороны группы мужчин, «инцидент не привел к физическому ущербу самой девушки, однако нанес психологическую травму, которую переживают жертвы насилия в реальной жизни». Впечатление от нападения «усилило эффект полного погружения» из-за игры в VR-очках, в которых находилась девушка на момент происшествия. Подобный инцидент ранее произошел в 2022 г., по словам потерпевшей «три или четыре аватара мужского пола и с мужскими голосами сначала окружили ее персонаж, начали вербально и сексуально ее добиваться, после чего фактически изнасиловали ее аватар».

В 2022 г. платформа Horizon Worlds ввела функцию «личного пространства», создавая барьер в 4 фута вокруг аватара после жалоб на домогательства. Пострадавшей девушке следовало использовать так называемую «безопасную зону» — одну из стандартных функций безопасности в Horizon Worlds. Данная функция создает защитное пространство вокруг аватара, в итоге никто не может взаимодействовать или разговаривать с ним. Чтобы снова общаться, создателю «безопасной зоны» необходимо ее отключить, подав специальный сигнал. Если задуматься — это перекладывание ответственности на жертв, когда от настроек безопасности зависит возможность общения, похоже на совет «не выходить из дома». Поэтому проблематика «виртуальных изнасилований» в рамках цифрового насилия становится весьма актуальной.

Не надумана ли данная проблема? Возможно ли совершение насильственного преступления против половой свободы в виртуальной реальности? Взрослый человек доцифровой эпохи скажет, что не видит в этом проблемы, так как лицо может просто выключить игру. Существует масса игр, где пользователи убивают друг друга, и это, конечно же, не вызывает необходимости квалификации этих деяний как убийств.

Но мы не должны забывать, что мир меняется, и данный мир тоже становится частью нашей реальности. Когда речь идет о метавселенной, то всегда предполагается виртуальная свобода, к которой и стремятся очень многие разработчики. Но свобода действий в видеоиграх всегда связана с тем, что игроки будут использовать ее в своих целях. И это далеко не всегда зависит от первоначальных мнений разработчиков.

Одной из наиболее известных метавселенных является Roblox, где люди общаются и делятся положительным опытом в иммерсивных пространствах. Именно данная метавселенная весьма популярна у детей. Многие несовершеннолетние в подобных виртуальных пространствах действительно практически живут, скрываясь от реального мира, такие дети очень уязвимы. У Roblox свобода действий колоссальна, потому что там больше пространства для создателей моделей, карт и целых режимов. Цензура в Roblox не пропускает карты, где есть оголенные части тела, а также намеки на секс. Но каждый пользователь может сам создать карту с контентом 18+ и приглашать на нее своих друзей. Карта будет заблокирована, если кто-то пожалуется на нее. Тем не менее не секрет, что даже в данной игре существуют целые сексрежимы².

Существуют и другие метавселенные, где возможно установление и более мягких правил. Появляются новые технологии, которые позволяют данный опыт сделать еще и тактильным. Технологии тактильной обратной связи, такие как костюм Teslasuit и перчатки HaptX, усиливают реализм VR. Костюм Teslasuit, оснащенный 68 датчиками, позволяет ощущать прикосновения и удары, о чем сообщалось в обзоре TechRadar³. Тактильная обратная связь варьируется от легких капель дождя до ударов пуль и взрывной волны в игровых виртуальных баталиях. При минимальном уровне костюм передаст тактильные ощущения от поглаживаний или объятий.

HaptX в 2024 г. представила перчатки, имитирующие текстуру и давление, согласно их официальному сайту⁴. Эти устройства используются в играх для взрослых, таких как VR Kanjo, где игроки могут «прикасаться» к персонажам. Однако в даркнете зафиксированы случаи использования таких технологий для создания платформ с симуляцией насилия.

Не стоит исключать, что метавселенные могут использоваться лицами, совершающими преступления против детей. Думается, в данном случае нам не нужно принимать новые нормы под «виртуальные изнасилования» — если субъект осведомлен о том, что аватар принадлежит пользователю, не достигшему 16 лет,

² Сексуальные игры в Roblox // URL: <https://wol.su/guides/9709-seksualnye-igry-v-roblox-kak-ih-najti-i-vse-chto-vam-nuzhno-znat.html>.

³ URL: <https://www.techradar.com/>.

⁴ URL: haptx.com.



его действия должны квалифицироваться по ст. 135 УК РФ, если же ему известно, что потерпевшему меньше 12 лет, его деяния должны квалифицироваться по п. «б» ч. 4 ст. 132 УК РФ, так как в силу примечания к ст. 131 УК РФ под признаки этого преступления подпадают деяния, предусмотренные ч. 2—4 ст. 135 УК РФ, совершенные в отношении лица, не достигшего 12-летнего возраста, поскольку такое лицо в силу возраста находится в беспомощном состоянии, т.е. не может понимать характер и значение совершаемых с ним действий. Сложность будет создавать только высокая латентность данных деяний.

Широкое распространение получил такой вид общения, как эротические стримы. Данный вид взаимодействия, несмотря на то, что исключает физическое взаимодействие между двумя сторонами, все же позволяет им удовлетворить свои потребности. Эта сфера была сразу же задействована и серым сегментом Интернета — оказание платных сексуальных услуг. Можно говорить о появлении киберпроституции⁵. Демонстрируя себя и осуществляя различные манипуляции со своим телом, «модель» осознает, что эти услуги оказываются за вознаграждение. Признаками проституции являются: систематичность и регулярность половых связей (профессионализм); несвязанность сексуальных контактов с личными отношениями; наличие различных партнеров (клиентов); публичный характер (доступность любому, способному оплатить услугу); получение соответствующего вознаграждения как более или менее регулярного источника дохода. Действующий на практике и распространенный в уголовно-правовой литературе подход к определению границ поведения, относящегося к проституции, предполагающий обязательное физическое сексуальное взаимодействие лица, занимающегося проституцией, с клиентом, представляется необоснованно узким и не соответствующим современным реалиям, в которых, как уже отмечалось, невозможно не заметить стремительно развивающуюся тенденцию к переходу в цифровую среду, в том числе интимного взаимодействия между людьми.

Несмотря на то что транслируемое в эрочатах видеоизображение имеет порнографический характер, сам эрочат не имеет характеристик предмета преступления, предусмотренного ст. 242 УК РФ, поскольку при его использовании не происходит изготовления такого материала. Такой чат представляет собой добровольное онлайн-общение сексуального характера, без права записи самой предоставляемой услуги. Можно попробовать провести аналогию из жизни-офлайн: одно дело, когда человек знакомится с кем-то и вступает в интимные отношения с симпатичными ему людьми, другое — когда человек ищет там тех, кто заплатит ему за это. Совершенно очевидно, что все признаки проституции тут присутствуют.

Онлайн-торговля сексуальными услугами по своей вредоносности для общественной нравственности не уступает традиционной проституции, а использующиеся при этом информационно-телекоммуникационные сети (включая сеть Интернет) значительно расширяют масштаб опасного поведения⁶. Данная форма

⁵ Под проституцией понимается систематическое вступление в сексуальные контакты за вознаграждение.

⁶ Левандовская М. Г. Установление уголовной ответственности за организацию онлайн-проституции // Юридическая наука. 2024. № 2. С. 208—210.

создает иллюзию анонимности и безопасности как для «модели», так и для ее клиента, позволяет лицу, которое в этом участвует, хотя бы на уровне самообмана считать себя моделью, но не проституткой. Эта форма достаточно распространена среди молодых людей, которых нельзя отнести к традиционным группам риска лиц, вовлекаемых в занятие проституцией. Они часто полагают, что их сетевая жизнь и тот образ, который они там создают, и реальная жизнь не пересекаются.

Можно ли привлекать к уголовной ответственности того, кто смог вовлечь в такое занятие другое лицо, сделав это посредством онлайн-общения? Думается да, но для этого надо пересмотреть само понятие проституции. Необходимо расширить понятие проституции, включив в него и нетелесные формы возмездных взаимодействий. Онлайн-проституцию следует признать отдельным сегментом, охватываемым общим понятием «проституция». Например, в Казахстане ввели уголовную ответственность за организацию сексуальных услуг через Интернет. В законе прописали понятие проституции как «возмездного оказания услуги сексуального характера, в том числе посредством использования сетей телекоммуникаций, Интернета в целях удовлетворения половой потребности другого лица путем полового сношения или иных действий сексуального характера»⁷.

На наш взгляд, это явление представляет опасность для нравственного развития несовершеннолетних, нередко их вовлекают в подобные стримы с подменной терминологией, когда лицо уверяет, что это не проституция, а просто продажа эротического контента и что оно само может решать, когда остановиться, просто предоставляя площадку для общения.

Весьма распространенными в сетевом пространстве являются интернет-сайты, содержащие сведения о лицах, оказывающих услуги сексуального характера, перечень оказываемых услуг, прейскурант цен на данные услуги, описывающие привлекательность занятия проституцией или вебкама.

При этом вход на такие сайты свободный, регистрация пользователей для доступа к использованию ресурсов сайта не требуется. Ознакомиться с содержанием сайта может любой интернет-пользователь. Размещенная на страницах сайта информация создает образ проституции как приемлемого общественного явления, способствует формированию мнения у пользователей сайта о ее обыденности и успешности лиц, занимающихся проституцией или пользующихся данными услугами.

Еще одно негативное явление — это «рынок девственности». В данном случае невозможно говорить о торговле людьми, если кто-то помогает продавцу найти нужного покупателя. Несмотря на то, что это, несомненно, проявление сексуальной эксплуатации, нет нарушения непосредственного объекта — физической свободы, так как решение принимается самим потерпевшим, он продолжает контролировать свою свободу в плане перемещения и распоряжения своим телом. Нет признака проституции в силу отсутствия систематичности действий, продавец сам определяет цену и победителя аукциона. Но это является еще одним проявлением коммерциализации секса, сделки заключаются на тематических

⁷ Уголовную ответственность за онлайн-проституцию вводят в Казахстане // URL: <https://orda.kz/ugolovnuju-otvetstvennost-za-onlajn-prostituciju-vvodjat-v-kazahstane-386701/> (дата обращения: 10.09.2024).



сайтах (например, в закрытых Telegram-каналах). Данное явление явно противоречит традиционным семейным ценностям, невинность рассматривается как товар, формирует у несовершеннолетних искаженное представление об институте верности и брака. Приводит к формированию потребительского подхода к своей сексуальности, что негативно влияет на общественную нравственность. В настоящее время подобная информация находится в открытом доступе, блокировка подобных ресурсов не всегда своевременна.

Проблема популяризации коммерческого секса и негласное одобрение услуг, использующих сексуальность человека, косвенно приводит к повышению распространенности ВИЧ и венерических заболеваний, вовлечению в занятие проституцией молодежи, пропаганде паразитического образа жизни; помимо оказания сексуальных услуг за деньги, приводит к виктимизации участников данных отношений. Особенно уязвимы несовершеннолетние, которые не всегда понимают, что участие в подобных деяниях делает их весьма уязвимыми для шантажа.

В настоящее время пропаганда проституции и возмездного оказания услуг сексуального характера — явление распространенное, за это не установлено никакой ответственности. Под пропагандой проституции или оказания возмездных услуг сексуального характера следует понимать деятельность по распространению материалов и (или) информации, направленных на формирование у несовершеннолетнего лица ложного представления о допустимости оказания сексуальных услуг за вознаграждение, в том числе оказания услуг сексуального характера посредством использования информационно-телекоммуникационных сетей, в целях удовлетворения половой потребности другого лица. Распространение подобной информации среди несовершеннолетних должно быть ограничено в целях предотвращения негативного влияния на общественные отношения, обеспечивающие общественную нравственность в рамках существующей в обществе половой культуры и взаимоотношения полов. В сфере сексуальной жизни людей необходимо установить ответственность (административную) за пропаганду проституции и возмездного оказания сексуальных услуг среди несовершеннолетних.

Также подобные деяния содержат риски, связанные с посягательствами на половую свободу и неприкосновенность несовершеннолетних. Как мы уже говорили ранее, лицо может использовать мессенджеры, игры в метавселенных для установления доверительных отношений среди несовершеннолетних, нередко маскируясь под сверстника. Установив доверительные отношения, оно выманивает сначала невинные по содержанию фото- и видеоматериалы, а со временем начинает провоцировать несовершеннолетнего поставлять ему более откровенный контент, вплоть до порнографического. Подростки часто не отдают себе отчет о последствиях, которые могут наступить после того, как они перешлют с использованием мессенджеров либо социальных сетей свои порнографические фото- и видеоматериалы, так как не задумываются о том, кто их «виртуальный друг». Преступники играют на самолюбии или любопытстве несовершеннолетнего, а в последующем посредством шантажа нередко выманивают ребенка на очную встречу для вовлечения в занятия реальной проституцией.

Вот несколько примеров подобных действий, которые, к сожалению, не являются редкостью, а также обладают высокой латентностью, так как стыд и страх не позволяют несовершеннолетним афишировать данные факты.

С 01.03.2022 по 22.05.2022 заключенный по Интернету вел интимную переписку с подростками из Хабаровского края. Мужчина предлагал несовершеннолетним фотографировать и снимать на видео обнаженные части своего тела. Продукцию порнографического характера дети отправляли фигуранту на мобильный телефон. Затем мужчина начал шантажировать подростков пикантными снимками и угрожал, что обнародует их, если несовершеннолетние не продолжат «радовать» его такими материалами. В результате преступных действий Александра П. нарушено нормальное физическое, психологическое и нравственное развитие четырех несовершеннолетних. Несмотря на отрицание самого мужчины, его вину удалось доказать. Приговором Фроловского городского суда Александр П. был признан виновным в совершении преступлений, предусмотренных ч. 5 ст. 135 УК РФ, п. «б, в» ч. 3 ст. 133 УК РФ (2 эпизода), п. «а», «в», «г» ч. 2 ст. 242² УК РФ. На основании ст. 69, 70 УК РФ ему назначено окончательное наказание в виде лишения свободы на срок 16 лет 6 месяцев с отбыванием в исправительной колонии особого режима, с лишением права заниматься деятельностью, связанной с работой с детьми, сроком на 15 лет, с лишением права заниматься деятельностью, связанной с созданием и использованием учетных записей (аккаунтов) в социальных сетях, сроком на 15 лет, с последующим ограничением свободы сроком на 1 год⁸.

17-летняя девушка познакомилась с молодым человеком, который представился Дмитрием на сайте знакомств, между ними завязались переписка и романтические отношения. Спустя некоторое время знакомый попросил ее прислать ему интимные фото и, получив желаемое, начал угрожать несовершеннолетней. Мужчина пообещал, что разошлет компрометирующие девушку снимки всем ее родным и знакомым, если та не начнет заниматься проституцией. Группа, где было выложено фото, закрытая, в ней состоят 3 603 человека. В описании к сообществу отмечается: «Знакомство и общение, а также реклама тех или иных видов услуг. Есть кого слить? Хотите найти шкуру на ночь? Тогда вам к нам. Материал для слива 16+. Предложки кидаем в лс-сообщества». Клиентов запуганной девушке злоумышленник подбирал сам. Часть денег несовершеннолетняя должна была отдать «Дмитрию», но он потребовал больше — около 150 тыс. рублей, в итоге девушка обратилась в полицию⁹.

В Набережных Челнах администратора одной из челнинских групп в «ВКонтакте» и его друга подозревают в понуждении к действиям сексуального характера. Пострадавшей оказалась несовершеннолетняя девушка, в правоохранительные органы с заявлением обратились ее родители. По версии следствия, молодые люди разместили в группе «Слили Набережные Челны 18+» интимные фотографии 17-летней девушки, а потом предложили удалить их, но в обмен за секс-услуги. При этом после того, как мужчины получили то, что требовали, они вымогали у нее 10 тысяч рублей. Администратору группы и его другу вменяется

⁸ URL: <https://bloknot-volgograd.ru/news/pedofil-s-zony-v-volgogradskoy-oblasti-shantazhiro-1761565> (дата обращения: 15.08.2024).

⁹ Виртуальный знакомый угрозами и шантажом заставил девушку заниматься проституцией // URL: <https://www.gazeta.ru/social/news/2023/11/22/21766051.shtml> (дата обращения: 15.08.2024).



преступление, предусмотренное ч. 2 ст. 133 УК РФ «Понуждение к действиям сексуального характера, совершенное в отношении несовершеннолетней»¹⁰.

В силу возраста потерпевшие не всегда осознают, что пересылка интимных фото даже в личных чатах образует признаки такого уголовно наказуемого деяния, как распространение порнографических материалов. В то же время эти же материалы дают основание для их последующего шантажа со стороны заинтересованных лиц, которые под воздействием этого втягивают их в традиционное занятие проституцией, или же принуждают к совершению действий сексуального характера в сети Интернет, или же заставляют совершать их иные преступления.

Виртуальное общение позволяет быстрее найти потенциальную жертву, упрощает возможность установить с ней доверительные отношения, позволяет лицу манипулировать сознанием детей. По нашему мнению, если лицо использует информационно-телекоммуникационные сети, независимо от стадии совершения преступления, создающие условия для вовлечения в занятия проституцией или вовлечения в другие преступления, это существенно увеличивает степень общественной опасности деяния. Поэтому даже начальные этапы, когда речь идет о получении вознаграждения, уже оказывается негативное воздействие на нормальное нравственное развитие несовершеннолетнего, даже если вознаграждение обещано за сексуальные контакты в виртуальном мире, что, на наш взгляд, представляет не меньшую опасность, чем реальное совершение таких действий. В любом случае лицо формирует у несовершеннолетнего установку о допустимости коммерческого секса.

В связи с этим считаем целесообразным дополнить ч. 2 ст. 240 и ч. 2 ст. 241 УК РФ пунктом «г»: «с использованием информационно-телекоммуникационных сетей (включая сеть Интернет)».

Кроме того, целесообразно дополнить ст. 240¹ УК РФ «Получение сексуальных услуг несовершеннолетнего» частью 2 следующего содержания: «То же деяние, совершенное с использованием информационно-телекоммуникационных сетей (включая сеть Интернет)...».

Предлагается дополнить примечание к ст. 240¹ УК РФ и изложить его в следующей редакции: «Примечание. Под сексуальными услугами в настоящей статье понимаются половое сношение, мужеложство, лесбиянство или иные действия сексуального характера, оказание услуги сексуального характера, в том числе посредством использования информационно-телекоммуникационных сетей (включая сеть Интернет), в целях удовлетворения половой потребности другого лица путем полового сношения или иных действий сексуального характера, усвоением совершения которых является денежное или любое другое вознаграждение несовершеннолетнего или третьего лица либо обещание вознаграждения несовершеннолетнему или третьему лицу».

В настоящее время правоприменитель может адаптировать существующие практики, чтобы защитить общество от новых угроз, сохраняя баланс между инновациями и безопасностью и в то же время не создавая искусственно новых составов преступления. Мы видим, что нет необходимости в создании «виртуального

¹⁰ В Челнах будут судить админа группы в «ВК» за склонение к интиму малолетки // URL: <https://chelny-biz.ru/news/243829/> / (дата обращения: 15.08.2024).

уголовного кодекса», с данными негативными проявлениями возможно бороться с помощью уже существующих норм, если внести в них дополнения с учетом процессов, появляющихся в метамире.

БИБЛИОГРАФИЯ

1. В 2023 году россияне купили более 50 млн товаров категории «18+» // URL: <https://www.mn.ru/smart/v-2023-godu-rossiyane-kupili-bolee-50-mln-tovarov-v-kategorii-18-gde-v-moskve-iskat-seks-igrushki-i-skol-ko-oni-stoyat>.
2. В Челнах будут судить админа группы в «ВК» за склонение к интиму малолетки // URL: <https://chelny-biz.ru/news/243829/> (дата обращения: 15.08.2024).
3. Виртуальный знакомый угрозами и шантажом заставил девушку заниматься проституцией // URL: <https://www.gazeta.ru/social/news/2023/11/22/21766051.shtml> (дата обращения: 15.08.2024).
4. *Левандовская М. Г.* Установление уголовной ответственности за организацию онлайн-проституции // Юридическая наука. — 2024. — № 2. — С. 208—210.
5. Сексуальные игры в Roblox // URL: <https://wol.su/guides/9709-seksualnye-igry-v-roblox-kak-ih-najti-i-vse-cto-vam-nuzhno-znat.html>.
6. Уголовную ответственность за онлайн-проституцию вводят в Казахстане // URL: <https://orda.kz/ugolovnuju-otvetstvennost-za-onlajn-prostitutciju-vvodjat-v-kazahstane-386701/> (дата обращения: 10.09.2024).





**Арсений Александрович
БИМБИНОВ,**

доцент кафедры
уголовного права

Университета имени
О.Е. Кутафина (МГЮА),
кандидат юридических
наук, доцент

bimbinov@yandex.ru

125993, Россия, г. Москва,
ул. Садовая-Кудринская, д. 9

Уголовно-правовые риски использования приложений для заказа товаров и коммерческих услуг

Аннотация. Статья является продолжением цикла работ, посвященных описанию уголовно-правовых рисков использования мобильных приложений: рисков претерпевания вреда в результате совершения преступлений и рисков причинения вреда при неочевидности противоправности. Настоящая работа содержит объяснение разницы в деятельности по выявлению рисков между деяниями, совершаемыми с использованием мобильных приложений, и деяниями, в целом совершаемыми с использованием сети Интернет. В ходе исследования установлено, что все анализируемые приложения для заказа товаров или коммерческих услуг объединены возможностью осуществления платежей и поэтому по потенциальным рискам наиболее соответствуют приложениям мобильного банкинга, однако по безопасности им уступают. В приложениях для заказа товаров или коммерческих услуг эксплуатант нередко напрямую взаимодействует с соответствующим поставщиком, определяя существенные условия заключаемых ими сделок. Такая специфика обуславливает самый главный уголовно-правовой риск претерпевания вреда — совершение хищений. К рискам причинения вреда относится приобретение через маркетплейсы ограниченных в обороте предметов. Связано это с тем, что через такие приложения коммуницируют самые разнообразные лица по поводу самых разнообразных товаров, работ и услуг, состав, содержание и исполнение которых могут противоречить законодательству РФ.

Ключевые слова: маркетплейсы, Яндекс, агрегаторы, незаконный оборот, хищения, мошенничество, социология уголовного права, общественная опасность, уголовная ответственность, сервисы

DOI: 10.17803/2311-5998.2025.129.5.112-121

Arseniy A. BIMBINOV,

Associate Professor of the Department of Criminal Law
of the Kutafin Moscow State Law University (MSAL),
Cand. Sci. (Law), Associate Professor
bimbinov@yandex.ru
9, ul. Sadovaya-Kudrinskaya, Moscow, Russia, 125993

Criminal Law Risks of Using Applications to Order Goods and Commercial Services

Abstract. The article is a continuation of a series of works devoted to the description of the criminal law risks of using mobile applications: the risks of suffering harm as a result of committing crimes and the risks of harm if illegality is not obvious. This paper provides an explanation of the difference in risk identification activities between acts committed using mobile applications and acts generally committed using the Internet. The study found that all analyzed applications for ordering goods or commercial services are combined with the ability to make payments and therefore, in terms of potential risks, they are most consistent with mobile banking applications, but they are inferior in terms of security. In applications for ordering goods or commercial services, the operator often interacts directly with the relevant supplier, determining the essential terms of the transactions they conclude. This specificity determines the most important criminal legal risk of suffering harm — the commission of theft. The risks of harm include the purchase of restricted items through marketplaces. This is due to the fact that through such applications, a wide variety of people communicate about a wide variety of goods, works and services, the composition, content and execution of which may contradict the legislation of the Russian Federation.

Keywords: marketplaces, Yandex, aggregators, illicit trafficking, embezzlement, fraud, sociology of criminal law, public danger, criminal liability, services

Как известно, уголовный закон не дифференцирует ответственность в зависимости от того, используются ли при совершении общественно опасных деяний веб-сайты (как правило, через браузеры, например Яндекс Браузер, Google Chrome или Internet Explorer) или мобильные приложения (на смартфонах и планшетах). Для этого нет правовых или социальных оснований, так как по этой причине общественная опасность существенно не меняется (если не брать во внимание случаи с искажением сетевых протоколов и использованием вредоносных программ). Однако для выявления уголовно-правовых рисков, и в первую очередь рисков претерпевания вреда (риска стать потерпевшим от преступления), разница между двумя этими способами использования телекоммуникационных сетей имеется.

Сегодня большинство опытных пользователей удовлетворяют свои производственные и социально-бытовые потребности, используя современные телекоммуникационные возможности через мобильные приложения (звонки и обмен



сообщениями, доставка еды и других товаров, запись к врачу, получение иных услуг, заказ такси, оплата покупок, перевод денег, поиск новостей, общение по интересам и т.д.). Объясняется это удобством мобильных приложений при их использовании в вышеуказанных целях.

Изначально движущей силой развития индустрии мобильных приложений были технологические особенности и маркетинг (приложения использовались как основная рекламная тактика поставщиков популярных товаров и услуг)¹. В настоящее время люди делают выбор в пользу мобильного приложения из-за его функциональных характеристик. Наличие привычного и удобного интерфейса управления², независимость функционала от времени и местоположения³, ориентация на индивидуальные потребности и личные предпочтения пользователя⁴, стратегическая координация между производителями и потребителями (например, UGC, когда накопленные отзывы потребителей расширяют спрос на определенные товары и услуги, а также позволяют их корректировать и улучшать)⁵, большая автономность (возможность выполнять свои функции без подключения к сети Интернет) и специализированность⁶ преобразовали коммуникационный потенциал приложений в интерактивный клиентский опыт, определяющий модели поведения человека⁷.

Если до пандемии COVID-19 лишь бренды и крупные поставщики товаров и услуг влияли на модели поведения через свои приложения⁸, то теперь чуть ли

¹ Stocchi L., Pourazad N., Michaelidou N., Tanusondjaja A., Harrigan P. Marketing research on Mobile apps: past, present and future // J Acad Mark Sci. 2022. Vol. 50 (2). P. 195—225. doi: 10.1007/s11747-021-00815-w.

² Kim E., Lin J., Sung Y. To app or not to app: Engaging consumers via branded mobile apps // Journal of Interactive Advertising. 2013. Vol. 13. P. 53—65.

³ Alnawas I., Aburub F. The effect of benefits generated from interacting with branded mobile apps on consumer satisfaction and purchase intentions // Journal of Retailing and Consumer Services. 2016. Vol. 31. P. 313—322.

⁴ Kopalle P. K., Kumar V., Subramaniam M. How legacy firms can embrace the digital ecosystem via digital customer orientation // Journal of the Academy of Marketing Science. 2020. Vol. 48. P. 114—131.

⁵ Kumar D. S., Purani K., Viswanathan S. A. Influences of «appscape» on mobile app adoption and m-loyalty // Journal of Retailing and Consumer Services. 2018. Vol. 45. P. 132—141 ; Lee S. A. M-servicescape: Effects of the hotel mobile app servicescape preferences on customer response // Journal of Hospitality and Tourism Technology. 2018. Vol. 9. P. 172—187.

⁶ Piccoli G., Brohman M. K., Watson R. T., Parasuraman A. Process completeness: Strategies for aligning service systems with customers' service needs // Business Horizons. 2009. Vol. 52. P. 367—376.

⁷ Kim J., Yu E. A. The holistic brand experience of branded mobile applications affects brand loyalty // Social Behavior and Personality. 2016. Vol. 44. P. 77—88.

⁸ Fang Y. An app a day keeps a customer connected: Explicating loyalty to brands and branded applications through the lens of affordance and service-dominant logic // Information & Management. 2019. Vol. 56. P. 377—391 ; Tseng T. H., Lee C. T. Facilitation of consumer loyalty toward branded applications: The dual-route perspective // Telematics and Informatics. 2018. Vol. 35. P. 1297—1309.

не каждый участник соответствующего рынка предлагает свою продукцию через социальные сети или специальное программное обеспечение и может оказывать определенное влияние.

Цифровизация в целом направлена на создание более комфортной среды, в которой человек может без дополнительных усилий решать стоящие перед ним задачи и удовлетворять потребности. В наибольшей степени такая возможность сегодня реализована функционалом смартфона. Эта вещь, без преувеличения, всегда находящаяся при пользователе, является основным проводником того самого клиентского опыта, определяющего модели поведения. Предустановленные или скачанные на смартфон мобильные приложения зачастую сами обуславливают привязанность и частоту их использования⁹, которые прямо пропорциональны уровню доверия к ним, но не определяют, по крайней мере напрямую, безопасность соответствующего ИТ-ресурса.

Так, приверженец мобильного шопинга всегда имеет приложение какого-нибудь маркетплейса, а путешественник — приложение агрегатора туров, билетов или отелей. Частота использования подобных программ (нередко обусловленная персонализированным контентом и push-уведомлениями) и опыт удачных приобретений изменяют восприятие риска, полезности и личной заинтересованности в использовании соответствующего приложения¹⁰. Например, тот же активный пользователь приложения для онлайн-шопинга часто по инерции запускает соответствующую программу, подбирает товары по цене и делает быстрые покупки, рассчитывая на гарантированное соблюдение прав потребителя. Нередко это заканчивается получением товара ненадлежащего качества и невозможностью предъявления требований (из-за «исчезновения» продавца). Признаваемые усилия разработчиков рассматриваемых ИТ-ресурсов, а также лиц, осуществляющих их модерацию и противодействие противоправному поведению, тем не менее не способны полностью исключить небезопасный контент в силу масштаба участников и частоты использования таких программ.

Поисковое поведение через мобильные устройства (как правило, через мобильные приложения) серьезным образом отличается от компьютерного поведения частотой и целеполаганием. Виктимные и другие неодобряемые в обществе действия чаще совершаются с использованием мобильных ИТ-программ, что объясняется индивидуальной принадлежностью смартфонов, персонализированными настройками отображения и поиска контента, удобством и доступностью соответствующих приложений.

Изложенное послужило поводом для проведения специального исследования, посвященного уголовно-правовым рискам мобильных приложений. На основе результатов опроса более 1 100 пользователей мобильных приложений, анкетирования 52 экспертов (ученых-юристов, ученых-медиков и психологов), наблюдения с ведением автором и двумя соисполнителями дневника использования

⁹ Wu L. Factors of continually using branded mobile apps: The central role of app engagement // International Journal of Internet Marketing and Advertising. 2015. Vol. 9. P. 303—320.

¹⁰ Kübler R., Pauwels K., Yildirim G., Fandrich T. App popularity: Where in the world are consumers most sensitive to price and user ratings? // Journal of Marketing. 2018. Vol. 82. P. 20—44.



мобильных приложений и эксперимента, заключающегося в ситуативном, необдуманном, порой провокационном использовании популярных мобильных программ¹¹, были сделаны выводы о наиболее распространенных моделях поведения человека при использовании приложений, сопряженных с риском причинения или претерпевания вреда. Возможность уголовного преследования при этом устанавливалась на основе анализа действующего законодательства и материалов судебно-следственной практики. Таким образом были описаны уголовно-правовые риски использования приложений для знакомств¹², приложений мобильного банкинга¹³, социальных сетей и мессенджеров¹⁴. В настоящей работе будет предпринята попытка описать уголовно-правовые риски четвертой, наиболее распространенной группы мобильных приложений — сервисов для заказа товаров и коммерческих услуг.

Приложения для заказа товаров (мобильный шопинг через так называемые маркетплейсы) являются одними из самых популярных ИТ-продуктов. С популярностью социальных сетей и мессенджеров им, конечно, не сравниться, так как, в отличие от маркетплейсов, указанные сервисы используются для межличностного общения по любому поводу, в том числе на отдыхе и при проведении досуга, тогда как приложения, связанные с электронной коммерцией (мобильные банки и приложения для заказа товаров и услуг), обычно используются по необходимости и в соответствии с потребностями. Вместе с тем, по данным портала Statista, маркетплейс Wildberries по итогам 2024 г. занял третье место по количеству скачиваний из App Store и Google Play, уступив самому популярному приложению в России Telegram на почти 10 млн загрузок (27,8 млн против 38 млн загрузок)¹⁵. В 2023 г., по данным отечественной системы RuStore, одним из самых скачиваемых приложений (для платформы Android) был сервис Ozon¹⁶.

Кроме названных ИТ-продуктов, к рассматриваемой группе следует отнести приложения для заказа готовой еды или продуктов (например, «Купер», «Пятерочка», «Яндекс Еда»), а также приложения для путешествий (например, «Яндекс Go», «Авиасейлс», «Островок»). Все эти сервисы объединены возможностью осуществления платежей и поэтому по потенциальным рискам наиболее соответствуют приложениям мобильного банкинга, однако по безопасности им уступают. В мобильном банкинге пользователь, управляя счетами, взаимодействует с окружающим миром через кредитную организацию, использующую всевозможные

¹¹ Результаты опросов см.: URL: <https://disk.yandex.ru/i/B9fGGinkKPfGvg> (дата обращения: 28.03.2025).

¹² См. об этом: Бимбинов А. А. Уголовно-правовые риски использования мобильных приложений для знакомств // Всероссийский криминологический журнал. 2024. Т. 18. № 2. С. 181—190.

¹³ См. об этом: Бимбинов А. А. Преступления с использованием мобильного банкинга // Уголовный процесс. 2024. № 10 (238). С. 70—75.

¹⁴ См. об этом: Bimbimov A. A. Criminal Prohibitions when Using Mobile Applications // Kutafin Law Review. 2024. Vol. 11. No. 3. P. 514—533.

¹⁵ URL: <https://www.statista.com/statistics/1175491/most-downloaded-free-mobile-apps-russia/> (дата обращения: 28.03.2025).

¹⁶ URL: <https://habr.com/ru/news/789264/> (дата обращения: 28.03.2025).

протоколы безопасности. В приложениях для заказа товаров или коммерческих услуг эксплуатант нередко напрямую взаимодействует с соответствующим поставщиком, определяя существенные условия заключаемых ими сделок.

Вышеуказанная специфика обуславливает самый главный уголовно-правовой риск рассматриваемых приложений — совершение хищений. Тайные хищения и хищения путем обмана или злоупотребления доверием совершают любые участники процесса по реализации товаров и услуг через анализируемые ИТ-сервисы: покупатели (как правило, при завладении товаром без оплаты), продавцы (как правило, при поставке ненадлежащей продукции вместо заявленной), посредники, в том числе работники службы доставки и пунктов выдачи, а также иные лица, обеспечивающие функционирование соответствующей торговой площадки.

Так, приговором Долгопрудненского городского суда Московской области Н. признан виновным в совершении преступления, предусмотренного ч. 3 ст. 159 УК РФ. По делу установлено, что Н. в период времени до ДД.ММ.ГГГГ, находясь в неустановленном в ходе следствия месте, путем обмана, используя возможность и доступ как лицо, занимающееся продвижением сервиса «Яндекс.Маркет», к статусам поступивших заказов, заведомо зная, что при продаже товара посредством маркетплейса покупателю от ООО «Яндекс» начисляются бонусные баллы, эквивалентные одному рублю за каждый бонусный балл, умышленно принял решение осуществить фиктивные заказы с созданного им на маркетплейсе «Яндекс.Маркет» аккаунта и намеренно указать сведения об оплате наличными денежными средствами. Реализуя задуманное, Н. на маркетплейсе создавал заказы, в системе делал пометку «доставлено», в результате чего автоматически получал кешбэк в виде бонусных баллов, которыми впоследствии оплачивал товары, принадлежащие ООО «Яндекс»¹⁷.

Наиболее распространенной схемой совершения мошенничеств на маркетплейсах является подмена товара. Так, Тимирязевский районный суд города Москвы квалифицировал деяние К. по ч. 2 ст. 159 УК РФ. По делу установлено, что К. совместно с Ц. разработали и реализовали план, согласно которому они через установленное в мобильном телефоне приложение Ozon заказывают одежду и обувь марок Adidas и Nike, приискивают внешне похожие товары для подмены и при получении заказа в пункте выдачи Ozon заменяют оригинальный товар контрафактным¹⁸.

Следует отметить, что подмена оригинального товара, стоимость которого не превышает 2 500 рублей, не образует состава преступления и квалифицируется как мелкое хищение, ответственность за которое предусмотрена ст. 7.27 КоАП РФ. Продавцы-мошенники на маркетплейсах используют этот криминообразующий стоимостной порог, реализуя через временные аккаунты контрафактные товары под видом оригинальных, стоимость которых не превышает 2 500 рублей.

При этом совершение краж с банковских счетов (путем списания денежных средств через аккаунты покупателей за незаказанные товары) является

¹⁷ Приговор Долгопрудненского городского суда Московской области от 23.09.2022 по делу № 1-138/2022 // СПС «КонсультантПлюс».

¹⁸ Постановление Тимирязевского районного суда города Москвы от 08.11.2023 по делу № 1-650/2023 // СПС «КонсультантПлюс».



преступлением независимо от суммы причиненного ущерба, поскольку такое хищение образует квалифицированный состав. Так, приговором Московского районного суда города Санкт-Петербурга П. признан виновным в совершении преступления, предусмотренного п. «г» ч. 3 ст. 158 УК РФ. По делу установлено, что П., имея умысел на тайное хищение денежных средств с банковского счета и реализуя его, действуя умышленно, из корыстных побуждений, используя имеющийся у него мобильный телефон марки Xiaomi, совершил перевод, повлекший списание денежных средств с банковского счета потерпевшего на сумму 2 000 рублей с комиссией в 39 рублей¹⁹.

Учитывая изощренность и масштабность деятельности мошенников на маркетплейсах, представляется возможным создание квалифицированного состава мошенничества, специальным признаком которого будет списание денежных средств через систему приема платежей маркетплейсов и других агрегаторов либо с использованием модификации компьютерной информации, искажение которой нарушает права потребителей.

Помимо подмены товара, пользователи могут столкнуться с подменой платежной информации или самого ИТ-ресурса. В отношении популярных мобильных приложений это маловероятно, но при использовании веб-версий соответствующих сервисов вполне возможно. Так, приговором Октябрьского районного суда города Самары ФИО1 признана виновной в том числе в совершении мошенничества через поддельный сайт по бронированию номеров в отеле²⁰.

Злоумышленники совершают преступления, пользуясь несовершенством программного обеспечения и технологического процесса. Так, С. признана виновной в совершении преступлений, предусмотренных ч. 4 ст. 159 УК РФ и ч. 3 ст. 30, ч. 3 ст. 159 УК РФ. По делу установлено, что С. в период с 12.07.2023 по 16.08.2023, находясь по месту своего проживания, обнаружив, что в платежной системе Wildberries произошел сбой и заказанные по условиям постоплаты товары отражаются как оплаченные, осознавая, что заказанные ею товары фактически не оплачены, из корыстных побуждений действуя с умыслом, направленным на хищение чужого имущества путем обмана, неоднократно получала товары (в том числе противень с антипригарным покрытием, стульчик-трансформер Biscuit, швабру с распылителем SprayPro, пакеты для грудного молока, шезлонг для новорожденных и т.д.) в пункте выдачи заказов Wildberries, сообщая работнику указанного пункта выдачи заказов ложную информацию о том, что вышеуказанные товары ею оплачены²¹.

С использованием приложений для заказа товаров или коммерческих услуг совершаются и иные преступления, однако все они, как правило, либо направлены на последующее совершение хищения, либо являются производными от них. Так, Г. признан виновным в совершении 50 краж, двух мошенничеств, неправомерного доступа к компьютерной информации и легализации (отмывания)

¹⁹ Приговор Московского районного суда города Санкт-Петербурга от 21.09.2022 по делу № 1-879/2022 // СПС «КонсультантПлюс».

²⁰ Приговор Октябрьского районного суда города Самары от 21.11.2023 № 1-396/2023 // СПС «КонсультантПлюс».

²¹ Приговор Левобережного районного суда города Липецка от 13.12.2024 по делу № 1-250/2024 // СПС «КонсультантПлюс».

денежных средств или иного имущества, приобретенных лицом в результате совершения им преступления. Как установлено судом, Г., в том числе используя устройства связи, осуществил регистрацию неустановленного аккаунта в мессенджере Telegram, указывая на его принадлежность к официальной поддержке маркетплейса Wildberries, затем приискал в группах в мессенджере Telegram с тематикой Wildberries сообщение от потерпевшего № 47 с вопросом о проблемах функционирования платформы Wildberries и обратился к нему под видом сотрудника технической поддержки. Под предлогом оказания помощи Г. завладел кодом доступа к личному аккаунту потерпевшего на Wildberries, поступившим ему посредством смс-сообщения, и осуществил неправомерный доступ к компьютерной информации, повлекший ее блокирование (доступ потерпевшего к личному кабинету был заблокирован)²².

К деяниям, сопряженным с риском причинения вреда при неочевидности противоправности, надлежит относить приобретение через маркетплейсы технических средств, предназначенных для негласного получения информации. Так, приговором Нижегородского районного суда г. Нижнего Новгорода В. признан виновным в совершении преступления, предусмотренного ст. 138¹ УК РФ. По делу установлено, что В., не являясь уполномоченным лицом в соответствии с постановлением Правительства РФ «Об утверждении Положения о ввозе в Российскую Федерацию и вывозе из Российской Федерации специальных технических средств, предназначенных для негласного получения информации, и списка видов специальных технических средств, предназначенных для негласного получения информации, ввоз и вывоз которых подлежат лицензированию», находясь в неустановленном месте, через маркетплейс Wildberries, не имея лицензии на деятельность по приобретению специальных технических средств, предназначенных для негласного получения информации, приобрел у неустановленного лица GPS трекер Mini A8, который согласно заключению эксперта относится к категории специальных технических средств, предназначенных для негласного получения информации, по функциональной возможности и конструктивной приспособленности для негласного получения информации²³.

Таким образом, можно сделать следующие выводы. Использование приложений для заказа товаров или коммерческих услуг сопряжено с риском претерпевания вреда в результате хищений. Все рекомендации пользователям банковских приложений актуальны и для пользователей приложений для заказа товаров и услуг, так как они используют систему обработки платежей, связанную с банковскими счетами.

Рассматриваемые приложения несут большие риски как в части претерпевания вреда, так и относительно возможности причинения вреда, в том числе при неочевидности противоправности деяния. Связано это в первую очередь с тем, что через такие приложения коммуницируют самые разнообразные лица по поводу самых разнообразных товаров, работ и услуг, состав, содержание и исполнение которых могут противоречить законодательству РФ.

²² Апелляционное определение Волгоградского областного суда от 17.07.2024 по делу № 22-2795/2024 // СПС «КонсультантПлюс».

²³ Приговор Нижегородского районного суда города Нижнего Новгорода от 30.08.2022 № 1-345/2022 // СПС «КонсультантПлюс».



Кроме того, популярные маркетплейсы выступают лишь посредниками между продавцом товара и его приобретателем, не всегда имея возможность удостовериться в качестве реализуемой продукции, а также благонадежность сторон, самостоятельно порождая претерпевая вред от участников торговых отношений.

БИБЛИОГРАФИЯ

1. Бимбинов А. А. Преступления с использованием мобильного банкинга // Уголовный процесс. — 2024. — № 10 (238). — С. 70—75.
2. Бимбинов А. А. Уголовно-правовые риски использования мобильных приложений для знакомств // Всероссийский криминологический журнал. — 2024. — Т. 18. — № 2. — С. 181—190.
3. Alnawas I., Aburub F. The effect of benefits generated from interacting with branded mobile apps on consumer satisfaction and purchase intentions // Journal of Retailing and Consumer Services. — 2016. — Vol. 31. — P. 313—322.
4. Bimbinov A. A. Criminal Prohibitions when Using Mobile Applications // Kutafin Law Review. — 2024. — Vol. 11. — No. 3. — P. 514—533. — DOI: 10.17803/2713-0533.2024.3.29.514-533.
5. Fang Y. An app a day keeps a customer connected: Explicating loyalty to brands and branded applications through the lens of affordance and service-dominant logic // Information & Management. — 2019. — Vol. 56. — P. 377—391.
6. Kim E., Lin J., Sung Y. To app or not to app: Engaging consumers via branded mobile apps // Journal of Interactive Advertising. — 2013. — Vol. 13. — P. 53—65.
7. Kim J., Yu E. A. The holistic brand experience of branded mobile applications affects brand loyalty // Social Behavior and Personality. — 2016. — Vol. 44. — P. 77—88.
8. Kopalle P. K., Kumar V., Subramaniam M. How legacy firms can embrace the digital ecosystem via digital customer orientation // Journal of the Academy of Marketing Science. — 2020. — Vol. 48. — P. 114—131.
9. Kübler R., Pauwels K., Yildirim G., Fandrich T. App popularity: Where in the world are consumers most sensitive to price and user ratings? // Journal of Marketing. — 2018. — Vol. 82. — P. 20—44.
10. Kumar D. S., Purani K., Viswanathan S. A. Influences of “appscape” on mobile app adoption and m-loyalty // Journal of Retailing and Consumer Services. — 2018. — Vol. 45. — P. 132—141.
11. Lee S. A. M-servicescape: Effects of the hotel mobile app servicescape preferences on customer response // Journal of Hospitality and Tourism Technology. — 2018. — Vol. 9. — P. 172—187.
12. Piccoli G., Brohman M. K., Watson R. T., Parasuraman A. Process completeness: Strategies for aligning service systems with customers’ service needs // Business Horizons. — 2009. — Vol. 52. — P. 367—376.
13. Stocchi L., Pourazad N., Michaelidou N., Tanusondjaja A., Harrigan P. Marketing research on Mobile apps: past, present and future // J Acad Mark Sci. — 2022. — Vol. 50 (2). — P. 195—225. — DOI: 10.1007/s11747-021-00815-w.

14. *Tseng T. H., Lee C. T.* Facilitation of consumer loyalty toward branded applications: The dual-route perspective // *Telematics and Informatics*. — 2018. — Vol. 35. — P. 1297—1309.
15. *Wu L.* Factors of continually using branded mobile apps: The central role of app engagement // *International Journal of Internet Marketing and Advertising*. — 2015. — Vol. 9. — P. 303—320.





Уголовно-правовая характеристика торговли алкогольной продукцией с использованием информационно-телекоммуникационных сетей, включая сеть Интернет

**Тимофей Викторович
АЛТУНИН,**
ведущий юрисконсульт
ООО «ПИ «Арена»»,
кандидат юридических наук
masher92@mail.ru
129090, Россия, г. Москва,
ул. Гиляровского, д. 5, стр. 1

Аннотация. В статье рассматриваются существующие уголовно-правовые запреты в сфере оборота алкогольной продукции в Российской Федерации. Проведен анализ такого признака, как «использование информационно-телекоммуникационных сетей, включая сеть Интернет» при квалификации преступлений, связанных с оборотом алкогольной продукции. Наиболее опасными деяниями в сфере оборота алкогольной продукции является сбыт некачественной алкогольной продукции и сбыт алкогольной продукции несовершеннолетним. Именно эти деяния посягают на общественные отношения, подлежащие уголовно-правовой охране. Реализация алкогольной продукции с использованием ИТКС обладает повышенной общественной опасностью, однако в настоящее время размещение информации о продаже алкоголя с использованием ИТКС не запрещено уголовным законом. На основании данного вывода автором обосновывается предложение изменить диспозицию исследуемой уголовно-правовой нормы, а также добавить в соответствующую часть квалифицирующий признак «с использованием средств массовой информации либо электронных или информационно-телекоммуникационных сетей (включая сеть Интернет)».

Ключевые слова: незаконный оборот алкогольной продукции, незаконный оборот метанола, использование информационно-телекоммуникационных сетей, Интернет, алкоголь

DOI: 10.17803/2311-5998.2025.129.5.122-127

Timofey V. ALTUNIN,
Leading Legal Counsel, LLC "PI Arena",
Cand. Sci. (Law)
masher92@mail.ru
5/1, ul. Gilyarovskogo, Moscow, Russia, 129090

Criminal and Legal Characteristics of Alcohol Product Trade Using Information and Telecommunication Networks, Including the Internet

Abstract. The article discusses existing criminal prohibitions in the field of alcoholic turnover in the Russian Federation. An analysis was carried out such as "the use of information and telecommunication networks, including the Internet"

in the qualification of crimes related to alcohol turnover. The most dangerous acts in the field of alcoholic turnover are the sale of poor-quality alcoholic beverages and the sale of alcohol products to minors. It is these acts that encroach on public relations subject to criminal law protection. The sale of alcoholic beverages using ITKS has an increased public danger, but at the present placement of information about the sale of alcohol using ITKS is not prohibited by criminal law. On the basis of this conclusion, the author justifies the proposal to change the disposition of the undergoing criminal legal norm, as well as add to the corresponding part of the qualifying sign "using the media or electronic or information and telecommunication networks (including the Internet)".

Keywords: illegal alcohol trafficking, methanol trafficking, use of information and telecommunication networks, Internet, alcohol

Пристрастие человека к алкоголю зачастую провоцирует его на необдуманные поступки. Люди стремятся удовлетворить свою потребность, минуя все государственные ограничения и запреты, и находят на рынке предложения со стороны предприимчивых продавцов. Товар у таких продавцов далеко не всегда отвечает требованиям качества, и его употребление может повлечь серьезный вред здоровью.

Среди указанных запретов в настоящее время действуют: запрет на продажу алкоголя несовершеннолетним, запрет на продажу алкоголя в определенное время суток (временной промежуток устанавливается каждым субъектом Федерации по своему усмотрению), запрет на продажу алкоголя без лицензии (с определенными исключениями), запрет на продажу немаркированной алкогольной продукции (с определенными исключениями). В уголовном законе данные запреты нашли отражение в следующих статьях: ст. 151¹, ч. 5 ст. 171¹, ст. 171³, ст. 171⁴ УК РФ.

Одним из способов обхода запретов является продажа алкоголя с использованием информационно-телекоммуникационных сетей (ИТКС), в том числе сети Интернет. Таким образом нарушителям проще всего избежать внимания правоохранительных органов и органов, осуществляющих контроль за оборотом алкогольной продукции в России. Важно отметить, что дистанционная продажа алкоголя также запрещена согласно п. 14, ч. 2, ст. 16 Федерального закона о государственном регулировании производства и оборота этилового спирта¹, ст. 171⁴ УК РФ.

Основными источниками предложений по дистанционной продаже алкоголя являются всем привычные мессенджеры Telegram, WhatsApp, Viber и т.д., а также интернет-сайты. Сайты и каналы регулярно блокируются, но при этом число их зеркал увеличивается. Кроме того, активно развиваются другие каналы продаж с использованием чат-ботов и приложений для смартфонов².

¹ Федеральный закон от 22.11.1995 № 171-ФЗ «О государственном регулировании производства и оборота этилового спирта, алкогольной и спиртосодержащей продукции и об ограничении потребления (распития) алкогольной продукции» // Российская газета. 19.01.1999. № 9.

² Попов А. А., Догданов Д. В., Шорин С. А., Айрапетьянц К. А. Оценка нелегального рынка алкогольной продукции в Интернете // Актуальные вопросы современной экономики. 2023. № 9. С. 377—389.



К признакам, характеризующим интернет-ресурс (с информацией о торговле алкогольной продукцией) как подлежащий включению в реестр запрещенных, суды относят следующие: заказ оформляется через корзину, по указанному телефонному номеру или через электронную почту, содержащаяся в ресурсе информация направлена на реализацию алкогольной продукции неизвестным лицам, возрастной ценз пользователей не установлен, ограничения на передачу, копирование, распространение информации отсутствуют, осуществляется розничная дистанционная торговля продукцией неограниченному кругу лиц³.

При рассмотрении уголовных дел о незаконной торговле алкоголем суды не акцентируют внимание на повышенной опасности его реализации с использованием ИТКС⁴. Факт размещения информации в Интернете является лишь доказательством того, что лицо имело умысел на продажу алкоголя дистанционным способом. Причина кроется в том, что размещение информации о розничной продаже дистанционным способом алкогольной продукции в сети Интернет запрещена ч. 8 ст. 13.15 КоАП РФ. Из этого следует вывод, что размещение информации с использованием ИТКС о такой продаже не запрещено уголовным законом.

На взгляд автора, принимая во внимание законодательную инициативу Минфина РФ по легализации дистанционной продажи алкоголя в России⁵, учитывая зарубежный опыт⁶, продажа качественного алкоголя через Интернет совершенным гражданам не создает угрозы общественным отношениям, которые следовало бы охранять уголовным законом.

В то же время продажа некачественной алкогольной продукции через Интернет обладает повышенной общественной опасностью по сравнению с торговлей «офлайн». Причина заключается в том, что продажа через Интернет позволяет охватить большую аудиторию и увеличить рынок сбыта, продавец имеет высокую степень анонимности, сложно отследить местонахождение склада и др.

Для целей настоящего исследования под некачественной алкогольной продукцией предлагается понимать алкогольную продукцию, содержащую такие токсичные примеси, как метанол, метанолсодержащие жидкости, метилацетат,

³ См., например: решение Ленинского районного суда г. Саранска Республики Мордовия от 19.10.2023 по делу № 2а-2397/2023 ; решение Ногинского городского суда (Московская область) от 21.08.2023 по делу № а-4900/2023 // URL: sudact.ru.

⁴ См., например: апелляционное постановление Московского городского суда от 22.06.2023 по делу № 10-12841/2023 ; кассационное определение Четвертого кассационного суда общей юрисдикции от 19.01.2023 № 77-328/2023 ; постановление Второго кассационного суда общей юрисдикции от 21.06.2022 по делу № 7У-4543/2022, 77-2014/2022 // СПС «КонсультантПлюс».

⁵ Проект федерального закона «О внесении изменений в Федеральный закон “О государственном регулировании производства и оборота этилового спирта, алкогольной и спиртосодержащей продукции и об ограничении потребления (распития) алкогольной продукции”» (подготовлен Минфином России, ID проекта 02/04/05-17/00066760) // СПС «КонсультантПлюс».

⁶ Как мир осваивает интернет-торговлю алкоголем // URL: https://rg.ru/2023/09/22/ot-zapreta-k-regulirovaniu.html?ysclid=m98cuex8pj577034733&utm_referrer=https%3A%2F%2Fya.ru%2F (дата обращения: 01.04.2025).

ацетальдегид, изоамилол, бутанон, гексанол и другие, во вредной для здоровья концентрации.

Реализация некачественной алкогольной продукции подпадает под запреты ст. 234², 238 УК РФ. Употребление некачественной алкогольной продукции может повлечь причинение вреда здоровью различной степени тяжести, а также наступление смерти. Так, смертельная доза метанола крайне мала и составляет около 30 грамм, а его употребление в меньшем количестве может повлечь слепоту и иные необратимые негативные последствия для организма⁷. Случаи отравления населения суррогатом регулярно появляются в новостных сводках. Таким образом, вред от употребления некачественной алкогольной продукции сопоставим с вредом от употребления наркотических средств и психотропных веществ. Употребление как алкоголя, так и наркотиков вызывает зависимость, и лицо со временем начинает все меньше уделять внимание качеству потребляемых веществ. В связи с этим представляется целесообразным обратиться к опыту уголовно-правового противодействия наркотизму.

Размещение информации о сбыте наркотических средств и психотропных веществ в Интернете входит в объективную сторону состава преступления, предусмотренного пп. «б», ч. 2 ст. 228¹ УК РФ. И такая логика представляется разумной ввиду повышенной общественной опасности использования ИТКС при совершении преступления. Важно отметить, что квалифицирующим признаком обладают только те преступления, при совершении которых ИТКС использовались в целях выполнения именно объективной стороны состава преступления, т.е. сбыта⁸, а не в целях переговоров соучастников между собой, осуществления ими поиска в Интернете и др. Данный подход получил поддержку и в научном сообществе⁹.

Ранее выдвигалась позиция, согласно которой при сбыте суррогатного алкоголя ст. 234² УК РФ выступает специальной по отношению к ст. 238 УК РФ при

⁷ Метанол // URL: <https://niik.ru/activity/methanol/> (дата обращения: 01.04.2025).

⁸ См., например: приговор Димитровского районного суда г. Костромы по делу №1-94/2021 от 16.07.2021 // URL: <https://sudact.ru/regular/doc/yxar6xxuifzk/>; определение судебной коллегии по уголовным делам Московского областного суда по делу № 22-5358/2023 от 29.08.2023 // URL: <https://sudrf.cntd.ru/document/1302961034>.

⁹ См., например: *Куричков Д. О.* Бесконтактный способ сбыта наркотиков: к вопросу о квалификации сбыта наркотических средств, психотропных веществ или их аналогов, совершенного с использованием средств массовой информации либо электронных или информационно-телекоммуникационных сетей (включая сеть Интернет) // *Борьба с преступностью: теория и практика : тезисы докладов X Международной научно-практической конференции, Могилев, 22 апреля 2022 г.* Могилев : Могилевский институт Министерства внутренних дел Республики Беларусь, 2022. С. 82—86; *Топильская Е. В.* Проблемы квалификации сбыта наркотиков с использованием средств массовой информации либо электронных или информационно-телекоммуникационных сетей // *Актуальные проблемы борьбы с преступностью: вопросы теории и практики : материалы XXV международной научно-практической конференции : в 2 ч.* Красноярск, 7—8 апреля 2022 г. Красноярск : Сибирский юридический институт Министерства внутренних дел РФ, 2022. Ч. 2. С. 165—168.



наличии в его составе, помимо метанола, иных примесей¹⁰. Предмет преступления ст. 234² УК РФ не является предметом настоящего исследования. Однако автором планируется раскрыть данную тему в дальнейшем и отнести к предмету преступления, предусмотренного ст. 234² УК РФ, не только метанол и метанолсодержащие жидкости, но и любые опасные для здоровья человека примеси, наделяющие напиток вредными свойствами. Концентрация этих примесей должна быть такой, при которой вредные свойства проявятся при употреблении напитка внутрь. Представляется, что такие изменения сократят избыточность уголовно-правовых запретов на распространение алкогольной продукции, установленных ч. 5 ст. 171¹, ст. 171³, 171⁴ УК РФ.

На основании изложенного предлагается:

— диспозицию ч. 1 ст. 234² УК РФ принять в следующей редакции:

«Незаконное производство, приобретение, хранение, перевозка или пересылка в целях сбыта, а равно сбыт метилового спирта (метанола), метанолсодержащих жидкостей, иных опасных для здоровья человека примесей под видом алкогольной продукции...»;

— дополнить ч. 2 ст. 234² УК РФ пунктом «в» в следующей редакции:

«с использованием средств массовой информации либо электронных или информационно-телекоммуникационных сетей (включая сеть Интернет)».

В части продажи алкоголя через Интернет несовершеннолетним, коллегами неоднократно предлагалось дополнить ст. 151¹ УК РФ квалифицирующим признаком «использование средств массовой информации, информационно-телекоммуникационных сетей, включая сеть Интернет»¹¹. Автором выражается полная поддержка такой инициативы в целях борьбы с алкогольной зависимостью среди несовершеннолетних.

Таким образом, наиболее опасными деяниями в сфере оборота алкогольной продукции, на авторский взгляд, являются сбыт некачественной алкогольной продукции и сбыт алкогольной продукции несовершеннолетним. Именно эти деяния посягают на общественные отношения, подлежащие уголовно-правовой

¹⁰ См., например: *Шевелева С. В., Сорокина О. С.* Уголовная ответственность за незаконный оборот метанола под видом алкогольной продукции // *Юридический вестник Кубанского государственного университета*. 2023. № 15 (4). С. 137 ; *Алтунин Т. В.* О некоторых вопросах объекта и предмета преступления, предусмотренного ст. 234² УК РФ // *Вестник Университета имени О.Е. Кутафина (МГЮА)*. 2024. № 4 (116). С. 160—164.

¹¹ См., например: *Готин А. А., Кузьмина Н. В.* К вопросу о продаже алкоголесодержащей продукции несовершеннолетним дистанционным способом // *Проблемы правоохранительной деятельности на современном этапе : сборник трудов Всероссийской (с международным участием) научно-практической конференции*. Кострома, 22—23 апреля 2022 г. Кострома : Костромской государственный университет, 2022. С. 316—320 ; *Александрова О. П., Осолков А. В.* Некоторые вопросы привлечения к уголовной ответственности за розничную продажу алкогольной продукции несовершеннолетним // *Вопросы российского и международного права*. 2023. Т. 13. № 8—1. С. 403—409 ; *Купирова Ч. Ш.* Розничная продажа несовершеннолетним алкогольной продукции: закон и проблемы его применения // *Юридическая наука и правоохранительная практика*. 2014. № 2 (28). С. 117—123.

охране. Реализация алкогольной продукции с использованием ИТКС обладает повышенной общественной опасностью, однако в настоящее время размещение информации о продаже алкоголя с использованием ИТКС не запрещено уголовным законом. По этой причине в уголовный закон необходимо внести ряд изменений, указанных в данной статье.

БИБЛИОГРАФИЯ

1. *Александрова О. П., Осколков А. В.* Некоторые вопросы привлечения к уголовной ответственности за розничную продажу алкогольной продукции несовершеннолетним // Вопросы российского и международного права. — 2023. — Т. 13. — № 8–1. — С. 403–409.
2. *Алтунин Т. В.* О некоторых вопросах объекта и предмета преступления, предусмотренного ст. 234² УК РФ // Вестник Университета имени О.Е. Кутафина (МГЮА). — 2024. — № 4 (116). — С. 160–164.
3. *Готин А. А., Кузьмина Н. В.* К вопросу о продаже алкоголесодержащей продукции несовершеннолетним дистанционным способом // Проблемы правоохранительной деятельности на современном этапе : сборник трудов Всероссийской (с международным участием) научно-практической конференции. Кострома, 22–23 апреля 2022 г. — Кострома : Костромской государственный университет, 2022. — С. 316–320.
4. *Купирова Ч. Ш.* Розничная продажа несовершеннолетним алкогольной продукции: закон и проблемы его применения // Юридическая наука и правоохранительная практика. — 2014. — № 2 (28). — С. 117–123.
5. *Куричков Д. О.* Бесконтактный способ сбыта наркотиков: к вопросу о квалификации сбыта наркотических средств, психотропных веществ или их аналогов, совершенного с использованием средств массовой информации либо электронных или информационно-телекоммуникационных сетей (включая сеть Интернет) // Борьба с преступностью: теория и практика : тезисы докладов X Международной научно-практической конференции. Могилев, 22 апреля 2022 г. — Могилев : Могилевский институт Министерства внутренних дел Республики Беларусь, 2022. — С. 82–86.
6. *Попов А. А., Догданов Д. В., Шорин С. А., Айрапетьянц К. А.* Оценка нелегального рынка алкогольной продукции в Интернете // Актуальные вопросы современной экономики. — 2023. — № 9. — С. 377–389.
7. *Топильская Е. В.* Проблемы квалификации сбыта наркотиков с использованием средств массовой информации либо электронных или информационно-телекоммуникационных сетей // Актуальные проблемы борьбы с преступностью: вопросы теории и практики : материалы XXV международной научно-практической конференции : в 2 ч. Красноярск, 7–8 апреля 2022 г. — Красноярск : Сибирский юридический институт Министерства внутренних дел РФ, 2022. — Ч. 2. — С. 165–168.
8. *Шевелева С. В., Сорокина О. С.* Уголовная ответственность за незаконный оборот метанола под видом алкогольной продукции // Юридический вестник Кубанского государственного университета. — 2023. — № 15 (4).





**Владислав Владимирович
РАДОВ,**

руководитель
уголовной практики
Key Consulting Group,
кандидат юридических наук
v.radov@kcgggroup.ru
123290, Россия, г. Москва,
Филипповский пер., д. 8,
стр. 1

Наказуемость преступлений в сфере информационных технологий

Аннотация. Статья посвящена проблеме справедливого, адекватного правоограничения лиц, совершивших уголовно-запрещенные деяния с использованием информационных технологий. Автор рассматривает криминологическую картину места и объема таких преступлений в структуре преступности, динамику и наиболее ярко выраженные случаи их совершения, каковыми признаются компьютерные и компьютеризированные преступления в классификации Е. А. Русскевича. Основываясь на обобщении массива судебной практики, автор показывает, что последняя группа преступлений фактически сводится к краже, мошенничеству и наркосбыту, на что государство реагирует нетаргетированными правоограничениями, в том числе условным лишением свободы, ограничением свободы и штрафом. Указывая на выстраивание тонкой настройки уголовно-правовой реакции, автор показывает возможные пути обеспечения связи между характером информационного преступления и соразмерной карой за его совершение. Результаты работы могут быть использованы для дальнейшего переосмысления уголовных наказаний лицам, совершившим преступления в сфере информационных технологий.

Ключевые слова: наказание, правоограничение, наказуемость, компьютерные преступления, уголовное право, эффективность наказания, ограничение свободы, меры пресечения, лишение права заниматься определенной деятельностью

DOI: 10.17803/2311-5998.2025.129.5.128-136

Vladislav V. RADOV,

Head of Criminal Practice at Key Consulting Group,
Cand. Sci. (Law)

v.radov@kcgggroup.ru

8/1, per. Filippovsky, Moscow, Russia, 123290

Punishability of Crimes in the Field of Information Technology

Abstract. The article is devoted to the problem of fair, adequate legal restrictions for persons who have committed criminally prohibited acts using information technology. The author examines the criminological picture of the place and volume of such crimes in the structure of crime, the dynamics and the most pronounced cases of their commission, which are recognized as computer and computerized crimes in the classification of E.A. Russkevich. Based on the generalization of an array of judicial practice, the author shows

that the latter group of crimes actually comes down to theft, fraud and drug trafficking, to which the state responds with non-targeted legal restrictions, including conditional imprisonment, restriction of freedom and a fine. Pointing to the development of a fine-tuning of the criminal-legal response, the author shows possible ways to ensure the connection between the nature of an information crime and a proportionate punishment for its commission. The results of the work can be used to further rethink criminal penalties for persons who have committed crimes in the field of information technology.

Keywords: *punishment, restriction of rights, punishability, computer crimes, criminal law, effectiveness of punishment, restriction of freedom, preventive measures, deprivation of the right to engage in certain activities*

Вопросы наказуемости незаслуженно остаются в тени, хотя именно их решение позволяет выкристаллизовать социальное значение уголовного права, а также обеспечить права человека в контексте назначения уголовного судопроизводства. Видится любопытным поставить проблематику следующим образом: должна ли быть связь между особенностями преступления в сфере информационных технологий и наказанием, назначаемым лицу, его совершившему. К названным деяниям логично относить, с одной стороны, преступления в сфере компьютерной информации, с другой стороны, всяческие деяния, совершенные с использованием электронных или информационно-телекоммуникационных сетей, включая сеть Интернет¹.

Обратимся к картине преступности. Ежегодно регистрируется все больше преступлений с использованием информационно-телекоммуникационных технологий. Их динамика по годам ретроспективно следующая: в 2024 г. — рост на 13,1 %, в 2023 г. — на 29,7 %, в 2022 г. — на 0,8 %, в 2021 г. — на 1,4 %, в 2020 г. — на 73,4 %, в 2019 г. — на 68,5 %. В реальном выражении это выглядит так: в 2019 г. зарегистрировано 294 409 таких деяний, а в 2024 г. — 765 365². Рассматриваемые деяния составляют 40 % от всего массива преступности, и это без учета латентности.

Важно подчеркнуть, что в общей структуре преступности на первый план выходят две формы хищения — кража (26,1 %) и мошенничество (23,3 %), тогда как в сфере информационных технологий за 2024 г. кража составила 14 %, а мошенничество — 50 % от всех преступлений. Значительную долю составляют деяния, запрещенные ст. 228¹ УК РФ (12 %), компьютерные преступления — по гл. 28 (14 %). Иными словами, 90 % всех преступлений, осложненных

¹ Постановление Пленума Верховного Суда РФ от 15.12.2022 № 37 «О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть Интернет» // Бюллетень Верховного Суда РФ. 2023. № 3.

² Состояние преступности // URL: <https://xn--b1aew.xn--p1ai/reports> (дата обращения: 02.04.2025).



информационными технологиями, представлены четырьмя деяниями, в том числе по ст. 158, 159, 228¹, 272 УК РФ.

Наказуемость компьютерных преступлений. В 2023 г. по преступлениям, предусмотренным гл. 28 УК РФ, осуждено 333 лица, из которых 13 приговорены к лишению свободы, 123 — к условному лишению свободы, 75 — к ограничению свободы, 97 — к штрафу, 12 — к исправительным работам. В качестве дополнительного наказания 67 лицам назначено лишение права занимать должности или заниматься определенной деятельностью.

Обобщение правоприменительной практики показывает, что дополнительное наказание в виде лишения права занимать определенную деятельность назначается за компьютерные преступления именно в тех случаях, когда осуждение осуществляется по ч. 3 ст. 272 УК РФ, т.е. по признаку «с использованием служебного положения». Вариации запрета того или иного вида деятельности могут быть следующими (по мере распространенности в судебных текстах):

- лишение права заниматься деятельностью, связанной с доступом к охраняемой законом компьютерной информации³;
- лишение права заниматься деятельностью, связанной с обработкой, хранением и распоряжением охраняемой законом информацией⁴;
- лишение права заниматься деятельностью, связанной с доступом к информации об абонентах, о соединениях между абонентами и абонентскими устройствами⁵;

³ Приговор Дорогомиловского районного суда г. Москвы от 10.10.2024 по делу № 01-0562/2024 ; приговор Бутырского районного суда г. Москвы от 20.09.2024 по делу № 01-0813/2024 ; приговор Ленинского районного суда г. Орска (Оренбургская область) от 13.01.2025 по делу № 1-27/2025 ; приговор Октябрьского районного суда г. Пензы (Пензенская область) от 07.02.2025 по делу № 1-71/2025 ; приговор Советского районного суда г. Брянска (Брянская область) от 21.11.2024 по делу № 1-506/2024 ; приговор Ленинского районного суда г. Астрахани (Астраханская область) от 31.01.2025 по делу № 1-143/2025 ; приговор Бийского городского суда (Алтайский край) от 26.08.2024 ; приговор Полярнозоринского районного суда (Мурманская область) от 30.01.2025 по делу № 1-3/2025 ; приговор Свердловского районного суда г. Перми (Пермский край) от 23.01.2025 по делу № 1-33/2025.

⁴ Приговор Туймазинского районного суда (Республика Башкортостан) от 21.01.2025 по делу № 1-14/2025 ; приговор Жигулевского городского суда (Самарская область) от 15.10.2024 по делу № 1-111/2024 ; приговор Магаданского городского суда (Магаданская область) от 24.09.2024 по делу № 1-430/2024 ; приговор Новотроицкого городского суда (Оренбургская область) от 29.08.2024 по делу № 1-290/2024 ; приговор Промышленного районного суда г. Курска (Курская область) от 20.12.2024 по делу № 1-354/2024 ; приговор Сургутского городского суда (Ханты-Мансийский автономный округ — Югра) от 13.12.2024 по делу № 1-1315/2024 ; приговор Ленинского районного суда г. Владивостока (Приморский край) от 05.08.2024 по делу № 1-591/2024.

⁵ Приговор Центрального районного суда г. Комсомольска-на-Амуре (Хабаровский край) от 03.10.2024 по делу № 1-781/2024.

- лишение права заниматься деятельностью в сфере компьютерной информации, связанной с доступом к персональным данным граждан РФ⁶;
- лишение права заниматься деятельностью, связанной с обслуживанием абонентов операторов сотовой связи⁷;
- лишение права заниматься деятельностью, связанной с допуском к охраняемой законом государственной, служебной, коммерческой или иной тайной, а также с обработкой персональных данных⁸.

В отдельных случаях судьи подчеркивают, что обращаются к дополнительному наказанию именно в связи с тем, что преступление совершено с использованием служебного положения, уточняя, что «избранное наказание будет в большей мере способствовать исправлению»⁹, в других случаях — отталкиваются от наличия корыстного мотива¹⁰, в прочих — акцентируют внимание на способе совершения преступления¹¹. Между тем в большинстве случаев назначение дополнительного наказания (как и весь процесс назначения наказания) остается скрытым от глаз исследователя, что объясняется отсутствием правовой культуры вербального объяснения выбора основного и дополнительного наказания, их размера (срока).

Итак, в абсолютном большинстве случаев (89 %) лица, совершившие компьютерное преступление, наказываются ограничением права на передвижение посредством условного лишения свободы и ограничения свободы (60 % от всех осужденных по гл. 28 УК РФ) или штрафом (29 %). В то же время лишение права заниматься деятельностью, связанной с доступом (обработкой, хранением, передачей) компьютерной информации, применяется к 20 % от общего числа осужденных по гл. 28 УК РФ. То есть непосредственная уголовно-правовая реакция на виртуальную преступность остается «аналоговой», что в отдельных случаях обоснованно.

Таким образом, прослеживается связь между тем, что лицо совершает компьютерное преступление, и той карательной составляющей правовых последствий, наступающих для него: совершение преступления в отношении компьютерной информации наказывается лишением права заниматься деятельностью, связанной с доступом к ней или оперированием таковой.

⁶ Приговор Троицкого городского суда (Челябинская область) от 12.09.2024 по делу № 1-402/2024 // СПС «КонсультантПлюс».

⁷ Приговор Ленинского районного суда г. Чебоксары (Чувашская Республика — Чувашия) от 29.08.2024 по делу № 1-419/2024 // СПС «КонсультантПлюс».

⁸ Приговор Городецкого городского суда (Нижегородская область) от 26.08.2024 по делу № 1-185/2024 // СПС «КонсультантПлюс».

⁹ См., например: приговор Автозаводского районного суда г. Тольятти (Самарская область) от 26.12.2024 по делу № 1-1047/2024 // СПС «КонсультантПлюс».

¹⁰ Приговор Советского районного суда г. Брянска (Брянская область) от 21.11.2024 по делу № 1-506/2024 // СПС «КонсультантПлюс».

¹¹ Приговор Свердловского районного суда г. Перми (Пермский край) от 23.01.2025 по делу № 1-33/2025 [1-697/2024] // СПС «КонсультантПлюс».



Наказуемость компьютеризированных преступлений (в терминологии, введенной в научный оборот профессором Е. А. Русскевичем¹²). Нельзя не согласиться с тезисом о том, что «появление нового (информационного) способа совершения преступлений не свидетельствует априорно о том, что он является более опасным, чем традиционный, а во многом указывает на проблему отставания социального контроля от развития общества и изменения преступности»¹³. Представляется, что складывающаяся судебная практика назначения наказания на сегодняшний день являет собой самопроверяемость («критерий истины»), подтверждающую высказанную мысль. В данном случае речь идет о преступлениях, находящихся за пределами гл. 28 УК РФ, но совершаемых с использованием Интернета. К таковым, как видно из анализа судебной практики, относятся деяния, запрещенные ст. 158, 159 и 228¹ УК РФ. Уголовно-правовая реакция на лиц, их совершивших, концентрируется на следующих видах уголовного наказания: за мошенничество и кражи при отягчающих обстоятельствах — изоляция от общества (реальное лишение свободы), ограничение права на передвижение (условное лишение свободы) и имущественное взыскание (штраф). Дополнительное наказание в виде запрета заниматься определенной деятельностью не находит должного применения¹⁴.

Совершение указанных деяний, как показывает правоприменительная практика, не влечет ограничений, связанных с доступом лица к виртуальному пространству. В этой связи любопытно предложение Е. А. Русскевича о введении нового уголовного наказания в виде ограничения права на цифровое присутствие¹⁵. Вместе с тем представляется, что есть перспективы и расширения сферы действия имеющихся уголовных наказаний, в том числе ограничения свободы или лишения права заниматься определенной деятельностью. Говоря об этом, заметим, что сходным инструментом государственной реакции является известная, хотя и сравнительно новая, мера пресечения в виде запрета определенных действий по ст. 105.1 УПК РФ. Ее содержание включает в себя меры, которые объединяют правоограничения, предусмотренные указанными уголовными наказаниями: с одной стороны, запрет на передвижение (выходить за пределы жилого помещения; находиться в определенных местах, а также ближе установленного расстояния до определенных объектов, посещать определенные мероприятия и участвовать в них) как процессуальный аналог ограничения свободы, с другой стороны, запрет на управление автомобилем или иным транспортным средством как процессуальный аналог лишения права заниматься деятельностью в этой сфере.

¹² Русскевич Е. А. Дифференциация ответственности за преступления, совершаемые с использованием информационно-коммуникационных технологий, и проблемы их квалификации : автореф. дис. ... д-ра юрид. наук. М., 2020. С. 11.

¹³ Русскевич Е. А. Дифференциация ответственности за преступления, совершаемые с использованием информационно-коммуникационных технологий... С. 13.

¹⁴ Данные судебной статистики Судебного департамента при Верховном Суде РФ (URL: [s://cdcp.ru/?id=79](https://cdcp.ru/?id=79) (дата обращения: 02.04.2025)).

¹⁵ Русскевич Е. А. Дифференциация ответственности за преступления, совершаемые с использованием информационно-коммуникационных технологий... С. 14.

В редких случаях суды формулируют в пределах своей дискреции подобные правоограничения именно посредством наиболее гибкого (в то же время имеющего недооцененный объем репрессивного воздействия¹⁶) наказания — лишения права заниматься определенной деятельностью. Так, лицо, осужденное за совершение деяния по ч. 3 ст. 30, ч. 5 ст. 228¹ УК РФ, приговорено к дополнительному наказанию в виде лишения права заниматься деятельностью, связанной с администрированием сайтов и каналов с использованием электронных и информационно-телекоммуникационных сетей, в том числе сети Интернет¹⁷.

Особенно ценным в рамках настоящего исследования является наличие в процессуальном законе таких особых ограничений, не коррелирующих с видами уголовных наказаний, как запрет общаться с определенными лицами; запрет отправлять и получать почтово-телеграфные отправления; запрет использовать средства связи и информационно-телекоммуникационную сеть Интернет. Приведенные запреты едва ли могут быть сформулированы в рамках лишения права заниматься определенной деятельностью, поскольку являются именно действиями, но не деятельностью. Представляется, что карательный и таргетированный потенциал таких правоограничений может найти воплощение посредством переосмысления содержательного характера наказания в виде ограничения свободы.

Заметим, что правовая реальность уже движется в этом направлении. Обратимся к постановлению Конституционного Суда РФ от 31.01.2024 № 4-П. Так, генеральным доводом потерпевшей по уголовному делу (ст. 119 УК РФ), обратившейся в орган конституционной юстиции, было указание на неправовое отличие запрета определенных действий (как меры пресечения) и ограничения свободы (как наказания) в той части, в которой суд не имеет оснований возложить на осужденного запрет по нахождению в определенных местах, например, ближе установленного расстояния до конкретных объектов (места жительства, работы, учебы потерпевшего), по общению с определенными лицами, по приближению к потерпевшему. В ответ на это Конституционный Суд РФ рассуждает в мотивировочной части от противного так: если исходить из того, что если в рамках ограничения свободы нельзя устанавливать такие запреты, значит, этот вид наказания не позволяет достичь (пресловутых и обоснованно раскритикованных¹⁸) целей наказания (в частности, предупреждения новых преступлений), а значит, следует избирать более строгое наказание (ст. 43, 60 УК РФ). Признавая несправедливость такой посылки, Конституционный Суд РФ приходит к выводу о том, что корректировка карательного потенциала имеющегося наказания (ограничения свободы) служит наилучшим интересам как обвиняемого (имея в виду гуманизацию уголовного наказания, не сводимого к изоляции от общества), так и потерпевшего¹⁹.

¹⁶ Лопашенко Н. А. Об уголовном наказании в России: заметки на полях Уголовного кодекса (от настоящего к будущему) // Закон. 2021. № 12. С. 33—48.

¹⁷ Приговор Майкопского гарнизонного военного суда (Республика Адыгея (Адыгея)) от 18.10.2024 по делу № 1-116/2024 // СПС «КонсультантПлюс».

¹⁸ Бабаев М. М., Пудовочкин Ю. Е. О целях наказания // Российский следователь. 2022. № 5. С. 46—50.

¹⁹ Постановление Конституционного Суда РФ от 31.01.2024 № 4-П по делу о проверке конституционности части первой статьи 53 Уголовного кодекса Российской Федерации



Аналогично можно рассуждать и в случае индивидуализации наказания лицам, совершившим компьютеризированные преступления, исходя из того, что лишение их свободы позволит предупредить новые деяния. Между тем пресечение доступа в Интернет для совершения кражи, мошенничества или наркосбыта *de facto* не обеспечивает ни одно из применяемых сегодня уголовных наказаний²⁰, в связи с чем возложение более релевантных правоограничений позволило бы обеспечить справедливую кару, предупреждающую продолжение или возобновление преступной деятельности.

Примечательно, что в указанном решении высший орган конституционной юстиции не обсуждает случаи, когда осужденный может буквально «терроризировать» потерпевшего дистанционно, т.е. не говорит о возможностях ограничения свободы для предупреждения совершения преступлений, связанных с навязчивым преследованием, в том числе запрещенных ст. 119, 133, 135, 137, 138 УК РФ, хотя смоделировать их нетрудно. В целом же Конституционный Суд РФ поддерживает широту судебного усмотрения в формулировании и содержательном уточнении конкретных запретов при ограничении свободы (п. 7 мотивировочной части постановления Конституционного Суда РФ от 31.01.2024 № 4-П).

Развивая логику указанного акта правосудия, заметим, что особое внимание уделяется тому, что соответствующие правоограничения имеют место в качестве мер пресечения, что, по мнению высшей инстанции, доказывает их эффективность, а потому обоснованность принципиального отвержения. Ограниченный подход преодолевает постклассическая теория уголовного права, в которой исследуется фактическая наказуемость, только частично пересекающаяся с официальным дискурсом, поскольку она представляет собой практическое измерение уголовного права, т.е. «приземляет» высокие абстракции к земным вопросам, что методологически объясняет И. Л. Честнов²¹.

Так, например, в материально-правовых нормах не предусмотрены такие процессуально-правовые запреты, как общение с определенными лицами, запрет отправлять и получать почтово-телеграфные отправления, запрет использовать средства связи и информационно-телекоммуникационную сеть Интернет, хотя именно их применение позволило бы развить нормативно-функциональное единство уголовного процесса и права, пресечения и осуждения, что, например, имеет место в случае содержания под стражей как меры пресечения и лишения свободы как уголовного наказания. Это открывает вполне справедливые перспективы совершенствования карательной деятельности государства.

С одной стороны, трудно отрицать, что на изучение приведенных мер (в том числе запрета определенных действий) постулируется исключительность

в связи с жалобами граждан О. А. Балуковой и Ю. М. Чернигиной // СЗ РФ. 2024. № 7. Ст. 1032.

²⁰ Русскевич Е. А. Об уголовном наказании и цифровизации // Уголовно-исполнительное право. 2024. № 3. С. 464.

²¹ Честнов И. Л. Переосмысление юридической практики с позиций постклассической методологии права // Теоретическая и прикладная юриспруденция. 2024. № 1 (19). С. 16 ; Его же. Юридическая наука в ожидании перемен // Известия высших учебных заведений. Правоведение. 2017. № 5 (334). С. 14.

уголовно-процессуальной научной и нормативной «юрисдикции». С другой стороны, такие правоограничения, основанные на принуждении и представляющие собой реакцию на нарушение уголовно-правового запрета, на наш взгляд, незаслуженно обделены уголовно-правовым вниманием. Известно, что предварительным наказанием являются как меры процессуального принуждения, так и сам факт уголовного преследования в отношении лица, т.е. приписывание (аскрипция по Г. Л. А. Харту) ему статуса подозреваемого или обвиняемого. Эти меры государственного принуждения сопровождаются значительным наказывающим эффектом. Любопытно, что еще французский мыслитель Ж. Делез при анализе «Алисы в стране чудес» писал о парадоксах перевернутого мира, одним из которых является «взаимообратимость причины и эффекта: *отбывать наказание до совершения преступления* (курсив наш. — В. Р.), плакать до того, как уколешься, исполнять работу до получения задания»²².

В нашем случае имеет место непоследовательность уголовно-правовой политики в отношении лиц, совершающих преступления в сфере информационных технологий, в связи с чем нельзя не процитировать суждение профессора М. М. Бабаева и профессора Ю. Е. Пудовочкина, справедливо констатирующих понимание системы наказаний так: «Впрочем, изначальная заданность не означает незыблемости, неспособности уголовно-правовых институтов меняться. Но, чтобы перемены эти приносили результат, в котором заинтересованы общество и граждане, они должны быть своевременны, научно обоснованы и мотивированы объективными новационными потребностями социума»²³.

БИБЛИОГРАФИЯ

1. Бабаев М. М., Пудовочкин Ю. Е. О целях наказания // Российский следователь. — 2022. — № 5. — С. 46—50.
2. Бабаев М. М., Пудовочкин Ю. Е. Уголовное наказание и преступность // Научный вестник Омской академии МВД России. — 2023. — № 3 (90). — С. 181—188.
3. Лопашенко Н. А. Об уголовном наказании в России: заметки на полях Уголовного кодекса (от настоящего к будущему) // Закон. — 2021. — № 12. — С. 33—48.
4. Русскевич Е. А. Дифференциация ответственности за преступления, совершаемые с использованием информационно-коммуникационных технологий, и проблемы их квалификации : автореф. дис. ... д-ра юрид. наук. — М., 2020. — 52 с.
5. Русскевич Е. А. Об уголовном наказании и цифровизации // Уголовно-исполнительное право. — 2024. — № 3. — С. 457—468.

²² Логика смысла / пер. с фр. Я. И. Свирского. М. : Академический проект, 2011. С. 10.

²³ Бабаев М. М., Пудовочкин Ю. Е. Уголовное наказание и преступность // Научный вестник Омской академии МВД России. 2023. № 3 (90). С. 181—188.



6. *Честнов И. Л.* Переосмысление юридической практики с позиций постклассической методологии права // Теоретическая и прикладная юриспруденция. — 2024. — № 1 (19). — С. 13—16.
7. *Честнов И. Л.* Юридическая деятельность в постклассической перспективе // Журнал российского права. — 2022. — Т. 26. — № 8. — С. 5—21.

Зарубежный опыт

Использование искусственного интеллекта при назначении наказания в зарубежных странах и принцип справедливости

Аннотация. В статье рассматриваются проблемы использования технологий искусственного интеллекта при назначении наказания в зарубежных правовых системах через призму уголовно-правового принципа справедливости. Актуальность темы обусловлена масштабной цифровизацией правосудия и нарастающим внедрением алгоритмических систем в сферу уголовного судопроизводства. В работе применены методы сравнительно-правового анализа, а также критико-аналитический подход к оценке зарубежной практики (США, Китай, Япония) и доктринальных подходов. Особое внимание уделено таким феноменам, как алгоритмическая дискриминация, проблема непрозрачности ИИ-моделей, датификация судебной практики, ограничение судебского усмотрения. В контексте зарубежных примеров анализируются риски снижения индивидуализации наказания, подмены принципа справедливости статистической нормой и утраты доверия к правосудию. Сделан вывод о необходимости критической переоценки роли ИИ при избрании меры наказания, выработке комплексных правовых и этических механизмов, гарантирующих защиту фундаментальных принципов уголовного закона. Работа актуализирует дискуссию о пределах цифровой трансформации в сфере уголовного права.

Ключевые слова: искусственный интеллект, правосудие, мера наказания, справедливость наказания, индивидуализация наказания



**Вячеслав Николаевич
ВОРОНИН,**

доцент кафедры
уголовного права
Университета имени
О.Е. Кутафина (МГЮА),
кандидат юридических
наук, доцент
vnvoronin@msal.ru
125993, Россия, г. Москва,
ул. Садовая-Кудринская,
д. 9

DOI: 10.17803/2311-5998.2025.129.5.137-147

Vyacheslav N. VORONIN,

Associate Professor of the Department of Criminal Law
of the Kutafin Moscow State Law University (MSAL),
Cand. Sci. (Law), Associate Professor
vnvoronin@msal.ru
9, ul. Sadovaya-Kudrinskaya, Moscow, Russia, 125993

Abstract. The article explores the challenges of applying artificial intelligence (AI) technologies to sentencing practices in foreign jurisdictions, through the lens of the criminal law principle of justice. The relevance of the topic stems from the ongoing digitalization of justice and the increasing use of algorithmic systems in criminal proceedings. The methodology includes comparative legal analysis and a critical evaluation of foreign practices (United States, China, Japan) and theoretical approaches. Special attention is given to such phenomena as algorithmic discrimination, opacity of AI models, the

© Воронин В. Н., 2025

datafication of judicial practice, and restrictions on judicial discretion. Based on international examples, the study analyzes the risks of reducing sentencing individualization, replacing justice with statistical norms, and eroding public trust in the judiciary. The author concludes that a critical reassessment of AI's role in criminal justice is needed, along with the development of comprehensive legal and ethical safeguards to uphold fundamental principles of criminal law. The study engages with a vital debate on the permissible boundaries of digital transformation in criminal law.

Keywords: artificial intelligence, justice, sentencing, fairness of punishment, individualization of punishment

Введение

Проблема справедливости при назначении наказания исторически является одной из центральных в уголовном праве. В условиях современной цифровой трансформации общественной жизни в целом особую актуальность приобретает вопрос использования технологий искусственного интеллекта (ИИ) для решения задач, в том числе стоящих перед уголовным правом¹, включая и назначение справедливого наказания. Внедрение таких технологий вызвано стремлением к повышению эффективности правосудия по уголовным делам, однако при этом порождает серьезные этические, правовые и социальные вызовы².

Отмечают, что искусственный интеллект в общем понимании — это способность нематериальных сущностей мыслить и принимать решения подобно человеку. ИИ-системы демонстрируют разумное поведение посредством анализа своего окружения и принятия действий с определенной степенью автономии для достижения конкретных целей. Системы, основанные на ИИ, могут быть как программными, функционирующими в виртуальной среде (например, голосовые помощники, программы анализа изображений, поисковые системы, системы распознавания речи и лиц), так и встроенными в аппаратные устройства (например, передовые роботы, автономные транспортные средства, дроны и др.).

Обратим внимание на следующие отличительные свойства ИИ, которые подчеркнуты в определении: а) способность к восприятию и интерпретации параметров внешней среды; б) способность принимать решения для выполнения базовых задач устройства, обычно заранее заданных человеком-разработчиком. Ключевое значение также имеет свойство «с определенной степенью автономии»: несмотря на участие человека, технологии ИИ способны функционировать автономно, например, выбирая наиболее подходящий сценарий действий из нескольких альтернативных вариантов. Автономия здесь также подразумевает способность некоторых технологий искусственного интеллекта, аналогично человеку, к обучению. Системы ИИ способны совершенствовать свои «навыки» и

¹ Bangura G. The European Union Artificial Intelligence Act: Mitigating Discrimination in Artificial Intelligence Systems : Master Thesis. University of Applied Arts Vienna, 2024.

² Transforming Justice: Implications of Artificial Intelligence in Legal Systems / A. R. Vargas-Murillo [et al.] // Academic Journal of Interdisciplinary Studies. 2024. Vol. 13. No. 2. P. 433—450. DOI: 10.36941/ajis-2024-0059.

изменять свои «действия» по мере накопления новой информации. Поэтому термином «машинное обучение» обозначаются те ИИ-системы, которые выявляют закономерности в имеющихся данных и затем применяют полученные знания к новой информации³.

Интерес представляет зарубежный опыт тех стран, где технологии ИИ уже используются при избрании меры наказания на достаточно системной основе. Например, широко известны такие алгоритмы, как COMPAS (Correctional Offender Management Profiling for Alternative Sanctions)⁴ и LSI-R (Level of Service Inventory — Revised)⁵, используемые в США, а также активно развиваемая концепция «умных судов»⁶ в Китайской Народной Республике. При этом, несмотря на особую привлекательность подобных решений для оптимизации юридической деятельности, данные технологии неоднократно подвергались критике в связи с недостаточной прозрачностью, принятием дискриминационных решений и нарушением фундаментальных уголовно-правовых и процессуальных принципов.

Цель обзора, приведенного в работе, заключается в представлении и интерпретации данных о зарубежном опыте использования технологий ИИ при назначении наказания, а также в сопоставлении их с представлениями уголовно-правовой доктрины о справедливости наказания⁷. Основная задача — выявить преимущества и риски, сопряженные с использованием искусственного интеллекта в этой чувствительной области.

1. Справедливость и алгоритмические модели назначения наказаний: обзор теоретических концепций

Вопрос о том, может ли искусственный интеллект обеспечить справедливость при назначении наказания, активно поднимается в зарубежной юридической науке⁸ и философии уголовного права. Понимание справедливости наказания традиционно основывается на двух основных подходах — ретрибутивном⁹ и

³ *Agarwal Srishti*. Use of Artificial Intelligence in Criminal Cases (October 21, 2023) // International Review of Law and Technology. Vol. 2. Is. 2. Forthcoming. SSRN: <https://ssrn.com/abstract=4609135>. URL: <http://dx.doi.org/10.2139/ssrn.4609135>.

⁴ *Zhang Y., Li J.* COMPAS Risk Score and Prediction of Recidivism // International Journal of Environmental Research and Public Health. 2022. Vol. 19. No. 10594.

⁵ *Lai J., Lin H., Zhang L., Wu C.* A Comparative Study of Risk Assessment Tools in Criminal Justice: COMPAS, LSI-R, and Others // Journal of Forensic Psychology Research and Practice. 2023. Vol. 23. No. 1. P. 45—67.

⁶ *Papagiannas S.* Automating Intervention in Chinese Justice: Smart Courts and Supervision Reform // Asian Journal of Law and Society. 2023. Vol. 10. No. 1. P. 123—145. DOI: 10.1017/als.2023.5.

⁷ *Bell F., Legg M.* Judicial Impartiality: AI in Courts // Cambridge Handbook of AI in Courts. Cambridge University Press, 2025.

⁸ *Simmons R.* Big Data and Procedural Justice: Legitimizing Algorithms in the Criminal Justice System // Ohio State Journal of Criminal Law. 2018. Vol. 15. No. 2. P. 573—615.

⁹ *Воронин В. Н.* Ретрибутивизм, справедливость наказания и учет общественного мнения в современном уголовном праве // Социально-экономическое развитие и качество правовой среды : сборник докладов VIII Московского юридического форума (XIX Меж-



утилитарном¹⁰. Если ретрибутивная модель справедливости предполагает необходимость соотносить меру наказания с общественной опасностью деяния и характеристикой личности виновного, то утилитарная концепция оценивает наказание прежде всего с позиции достижения целей наказания.

Й. Рибберг считает, что алгоритмические модели назначения наказания должны учитывать обе эти концепции и быть способными удовлетворять их базовые требования, что является сложной задачей в связи с техническими и этическими ограничениями искусственного интеллекта¹¹. Также Й. Рибберг спорит с позицией сторонников полного отказа от алгоритмических решений в уголовном праве, утверждая, что карательная сущность наказания может быть сохранена даже в условиях широкого использования алгоритмов, если алгоритмы будут служить вспомогательным, а не определяющим инструментом в руках судей. При этом Рибберг подчеркивает необходимость сохранения прозрачности и возможности использования судейского усмотрения судьей-человеком, который должен оставаться ответственным за решение, принятое и при участии алгоритма¹².

Проблемы возникают также в связи с тем, что алгоритмические решения по своей природе основываются на анализе больших данных (big data), которые содержат в себе информацию о предыдущем поведении лиц, совершивших преступления, и о практике вынесения судебных решений по сходным категориям дел. В результате алгоритмы нередко «наследуют» те предубеждения и искажения, которые исторически существовали в правоприменительной практике, что приводит к дискриминации определенных социальных групп и фактическому нарушению принципов равенства и справедливости. Данный феномен обозначают как «проблема входных данных» (input problem)¹³, подчеркивая зависимость качества алгоритмических решений от исходных данных и неспособность алгоритмов самостоятельно выявлять и корректировать скрытые предвзятости¹⁴.

Кроме сказанного выше, существует комплекс этических проблем, связанных с использованием ИИ при избрании меры наказания. Один из важнейших вопросов — это проблема законности судебных постановлений, которые вынесены с использованием генеративного ИИ. Генеративные модели, создающие тексты судебных постановлений, обоснования и рекомендации по назначению наказаний, ставят под сомнение в целом легитимность судебной власти, поскольку публично

дународная научно-практическая конференция), г. Москва, 8—10 апреля 2021 г. : в 5 ч. М. : Университет имени О.Е. Кутафина (МГЮА), 2021. Ч. 4. С. 16—19.

¹⁰ Hirsch Andrew Von. Past or future crimes: Deservedness and dangerousness in the sentencing of criminals. New Brunswick : Rutgers University Press, 1985.

¹¹ Ryberg J. Justice by Algorithm? The Limits of AI in Criminal Sentencing // Criminal Law and Philosophy. 2024. Vol. 18. P. 1—18.

¹² Ryberg J. Sentencing, Artificial Intelligence, and Condemnation: A Reply to Taylor // Philosophy & Technology. 2024. Vol. 37. № 2.

¹³ Brożek B., Furman M., Jakubiec M., Kucharzyk B. The Black Box Problem Revisited: Real and Imaginary Challenges for Automated Legal Decision Making // Artificial Intelligence and Law. 2024. Vol. 32. P. 427—440. DOI: 10.1007/s10506-023-09356-9.

¹⁴ Ryberg J. Criminal Sentencing and Artificial Intelligence: What is the Input Problem? // Criminal Law, Philosophy (2024). URL: <https://doi.org/10.1007/s11572-024-09739-2>.

не раскрываются основания и принципы, лежащие в основе их работы. Это вызывает значительные опасения в отношении возможности обеспечить достаточную прозрачность и объяснимость принимаемых решений, а также общественный контроль, что предопределяет важность обязанности суда мотивировать выводы, сделанные в судебном постановлении, особенно при использовании алгоритмических решений, поскольку это влияет на общественное восприятие справедливости наказания и уровень доверия к судебной власти¹⁵.

Следовательно, при всей перспективности использования ИИ в механизме назначения наказания, уже на теоретическом уровне возникают фундаментальные проблемы и ограничения¹⁶, которые требуют адекватного разрешения до внедрения таких технологий в осуществление правосудия.

2. Практика применения систем искусственного интеллекта при назначении наказаний: исследования зарубежного опыта

2.1. США. Наиболее известным зарубежным примером использования искусственного интеллекта в практике назначения уголовных наказаний является алгоритм COMPAS, разработанный компанией Northpointe и используемый в судах многих штатов США для оценки рисков рецидива и вынесения рекомендаций судье в части наказания. Эмпирическим анализом применения COMPAS занимаются многие исследователи, и полученные ими выводы во многом сходны, а также вызывают интерес¹⁷. В частности, это касается вывода о том, что данный алгоритм демонстрирует статистически значимую расовую предвзятость: лица афроамериканского происхождения чаще относились алгоритмом к лицам, имеющим высокий риск рецидива по сравнению с лицами белой расы даже в таких случаях, когда афроамериканцы фактически совершали преступление впервые¹⁸.

Такая проблема именуется в литературе «алгоритмической дискриминацией», которая относится к систематическим различиям в результатах, генерируемых алгоритмическими системами, которые оказывают неблагоприятное воздействие на определенные социальные группы. Эти различия могут быть результатом предвзятости, встроенной в данные или алгоритмы, или же порождаться структурными факторами, приводящими к неравенству. В отличие от традиционных форм дискриминации, алгоритмическая дискриминация часто не является следствием умышленного намерения, а возникает в силу технических,

¹⁵ *Hendrickx V.* The Judicial Duty to State Reasons in the Age of Automation? The Impact of Generative AI Systems on the Legitimacy of Judicial Decision-Making // *European Law Review*. 2024. № 1.

¹⁶ *Rudin C.* Stop Explaining Black Box Machine Learning Models for High Stakes Decisions and Use Interpretable Models Instead // *Nature Machine Intelligence*. 2019. Vol. 1. No. 5. P. 206—215.

¹⁷ *Wadsworth Ch., Vera F., Piech Ch.* Achieving Fairness through Adversarial Learning: an Application to Recidivism Prediction // *Proceedings of the FAT/ML Workshop*. Stockholm, 2018.

¹⁸ *Engel Ch., Linhardt L., Schubert M.* Code is Law: How COMPAS Affects the Way the Judiciary Handles the Risk of Recidivism // *Artificial Intelligence and Law*. 2024. DOI: 10.1007/s10506-024-09389-8.



институциональных или социальных процессов, формирующих разработку и функционирование алгоритмов¹⁹.

Алгоритмическая дискриминация может проявляться в различных формах. Она может быть явной, когда алгоритм прямо использует чувствительные признаки, такие как раса, национальность, пол, а может быть и скрытой, когда негативные последствия вытекают из косвенных взаимосвязей различных факторов. Например, исторические данные, в которых отражается неравенство, могут привести к тому, что алгоритм будет учиться на прошлом опыте с уже учтенной дискриминацией, не распознавая его как негативный и неправильный.

Так, например, упомянутый алгоритмы COMPAS не использует напрямую данные о расе лица. Однако в системе учитываются такие факторы, как: уровень образования; трудоустройство; социальная среда; место жительства; возраст, в котором лицо впервые совершило преступление (или правонарушение). В литературе они получили наименование «прокси-переменные (proximity variables)»²⁰: совокупность этих переменных может опосредованно предопределять расовую принадлежность. Таким образом, предвзятость возникает не из-за намеренного включения дискриминационных признаков, а из-за того, что алгоритм обучается на системно искаженных исторических данных, которые отражают структурную несправедливость в прошлом²¹.

2.2. Китай. Особое внимание в контексте прозрачности и объяснимости алгоритмических решений заслуживает опыт Китая. Правительство Китая с середины 2010-х гг. активно развивает систему так называемых «умных судов»²² (Smart Courts), использующих технологии искусственного интеллекта и большие данные для оптимизации и автоматизации принятия судебных решений, в том числе и по уголовным делам. «Платформа 206» была разработана Китайским центром информационных технологий в сотрудничестве с Министерством общественной безопасности КНР. Она функционирует как единая цифровая среда для уголовного дела, охватывая стадии: предварительного расследования; возбуждения уголовного дела; предъявления обвинения; судебного разбирательства; вынесения приговора²³. Судьи используют эту систему как вспомогательный инструмент при вынесении приговора. Основная цель — обеспечить единообразие судебной практики, одновременно снижая вероятность судебных ошибок.

Так, в литературе представлено детальное описание китайской модели интеграции искусственного интеллекта в судебную систему. В рамках этого подхода

¹⁹ Dou L. & Dou X. (2025). Towards Just AI: Challenges and Solution Framework for Algorithmic Discrimination in Judicial System // International Journal of Digital Law and Governance. URL: <https://doi.org/10.1515/ijdlg-2024-0020>.

²⁰ Zhang J. & Han Yu. (2022). Algorithms Have Built Racial Bias in Legal System-Accept or Not? 10.2991/assehr.k.220105.224.

²¹ COMPAS and Proxies: Algorithmic Discrimination in Practice / J. Zhang [et al.] // Unpublished manuscript, 2021.

²² Papagianneas S. Smart Courts and Governance in the PRC. Preprint // SSRN, 2023. URL: <https://ssrn.com/abstract=3777378>.

²³ Nyu Wang, Michael Yuan Tian. Intelligent Justice: AI Implementations in China's Legal System // Chapter in Edited Volume, 2022.

алгоритмы активно используются не только для оценки рисков рецидива, как в США, но и для автоматического принятия решений о мере наказания на основе «стандартов наказаний», что в значительной степени позволяет добиться большей унификации и предсказуемости судебных постановлений²⁴.

Алгоритмы осуществляют квалификацию преступления, а также формируют проект судебного постановления, в котором судье предлагается: автоматическая квалификация содеянного; типовая мера наказания; статистическая сопоставимость с аналогичными делами (модель «одинаковое дело — одинаковый приговор»). При этом отклонение от алгоритма требует особой мотивировки и увеличивает риск отмены судебного постановления. Следовательно, происходит формализация судебского усмотрения: судья не лишается права принимать решение, но вынужден действовать в границах «алгоритмической нормативности».

Также подобный подход может оказывать влияние на процессуальную независимость судьи: если любое отклонение от этой нормативности вызывает проверку, повышается уровень самоцензуры. При этом сторона защиты и сам подсудимый не имеют доступа к данному алгоритму расчета меры наказания, что нарушает принципы состязательности и прозрачности. Критика китайской модели состоит в том, что, по мнению исследователей, «технологическая централизация может трансформировать судебную функцию из осуществления правосудия в администрируемую функцию, где законность вынесенного решения зависит не от усмотрения суда, а от соответствия требуемому шаблону»²⁵.

Также китайская судебная система зачастую не предоставляет подробных объяснений логики, лежащей в основе решений ИИ, ссылаясь на техническую сложность и государственную тайну в вопросах работы алгоритмов. Такая практика значительно затрудняет возможность судебного и общественного контроля, что порождает риски снижения доверия к судебной системе. Алгоритмы при таком подходе способны учесть объективные факторы, необходимые для назначения наказания, однако учесть такие признаки, как степень вины, влияние наказания на исправление и условия жизни семьи осужденного, для ИИ гораздо сложнее, поэтому алгоритмическая стандартизация может вести к нарушениям принципов индивидуализации и справедливости наказания.

2.3. Япония. Особый интерес представляют результаты исследований эмпирических данных, проведенных как в тех странах, где внедрены различные компоненты ИИ в деятельность судов, так и в странах, где ведется дискуссия по этому вопросу. К последним относится, например, Япония. Одно из наиболее значимых эмпирических исследований, проведенных недавно в Японии, посвящено сравнению восприятия судебных постановлений, вынесенных людьми и алгоритмами. Исследование было проведено в форме опроса с использованием интернет-анкетирования, целью которого стало выявление отношения граждан

²⁴ Wang N., Tian M. Y. «Intelligent Justice»: human-centered considerations in China's legal AI transformation // *AI Ethics* 3, 349—354 (2023). URL: <https://doi.org/10.1007/s43681-022-00202-3>.

²⁵ Bell F. and Legg M. Judicial Impartiality: AI in Courts (February 11, 2025) // *UNSW Law Research* No. 25—4. SSRN: <https://ssrn.com/abstract=5161571>. URL: <http://dx.doi.org/10.2139/ssrn.5161571>.



к использованию искусственного интеллекта при назначении наказания судом, а также факторов, влияющих на формирование этого отношения.

Опрос проводился в октябре 2021 г. С целью моделирования восприятия ИИ в судебной системе респондентам был представлен следующий гипотетический сценарий: «В будущем в судах начнут использоваться системы искусственного интеллекта. Предположим, что в судебном процессе по уголовному делу, помимо участия человека-судьи, используется ИИ, обученный на большом массиве данных аналогичных дел, который предоставляет информацию о рекомендуемом наказании. Судья, выслушав мнения сторон и изучив обстоятельства дела, принимает окончательное решение, учитывая в том числе и рекомендации ИИ». После прочтения этой ситуации участникам было предложено оценить, насколько они поддерживают использование ИИ в описанных условиях, а также ответить на ряд вопросов, касающихся их представлений, опасений и степени доверия к ИИ и его использования судами. Целью исследования было эмпирически проанализировать, в какой степени общество поддерживает использование ИИ в судопроизводстве, а также какие факторы определяют уровень этой поддержки.

В качестве выводов авторы исследования отмечают, что общий уровень поддержки использования ИИ в судебной системе (при условии, что окончательное решение остается за судьей) является умеренно положительным. Отношение респондентов к ИИ при избрании меры наказания определяется не столько знанием права или опытом взаимодействия с системой правосудия, сколько символическим и эмоциональным отношением к технологиям как таковым. Иными словами, граждане не оценивают ИИ как правовой механизм, а, скорее, как объект, отношение к которому сформировалось через повседневный технологический опыт.

Следовательно, поддержка ИИ в судебной системе может существовать даже при отсутствии правовых знаний, если у граждан сформированы устойчиво позитивные представления об ИИ в целом²⁶.

Выводы и дальнейшие направления исследований

Чтобы соотнести возможности ИИ при избрании меры наказания в направлении реализации принципа справедливости, в работе приведены примеры, как ИИ в большей степени представляет угрозу тому, чтобы наказание становилось справедливым. И проблема рассогласованности справедливости наказания и «цифровой» справедливости выходит за пределы использования элементов ИИ в этом процессе. Угрозой реализации справедливости служат в целом современные процессы датификации судебной практики.

Под датификацией понимают процесс перевода сложных, динамичных, контекстуальных форм человеческого поведения (например, постановлений суда) в фиксированные категории, пригодные для сетевой обработки, сопоставления и нормирования²⁷. Как результат, цифровая трансформация судебной системы

²⁶ *Watanabe Eiichiro, Liu Yichen, Ioku Tomohiro. Judges versus Artificial Intelligence in Juror Decision-Making in Criminal Trials: Evidence from Two Pre-Registered Experiments // PLOS ONE. 2025. Vol. 20. № 1.*

²⁷ См.: *Gil Rothschild-Elyassi. The Datafication of Law: How Technology Encodes Carceral Power and Affects Judicial Practice in the United States (2022).*

и внедрение различных ИИ-систем прогнозирования, визуализации и формализации меры наказания в приговоре, вопреки декларируемым целям повышения прозрачности и стремления к единообразию, в действительности приводит к подрыву фундаментального принципа справедливости.

Упрощенно механизм деградации справедливости в судебных системах, основанных на ИИ, выглядит следующим образом: каждый новый приговор вносится в централизованную базу данных, где приговоры систематизируются и обрабатываются при помощи цифровых средств обработки данных. На основе этой информации формируются некие нормативные ориентиры — усредненные значения размеров наказаний, которые затем визуализируются в виде графиков, диаграмм или таблиц. Эти визуализированные данные доступны для судьи, и он может перед вынесением приговора обратиться к ним и получить в итоге некий ориентир в следующем виде: «наказание по такой категории дел обычно составляет N лет».

Судья начинает соотносить меру наказания с этой усредненной практикой. Даже если конкретное дело требует более глубокой индивидуализации наказания и учета множества обстоятельств дела и характеристик личности виновного, судья может опасаться, что наказание, назначенное им, будет существенно выпадать из статистического диапазона, и назначит это усредненное наказание, чтобы не увеличивать риск отмены или изменения судебного постановления в рамках процедур судебного контроля. Каждый такой приговор снова попадает в информационную систему, увеличивая количество приговоров, в которых размер наказания будет соответствовать усредненному нормативу. В итоге такая нормализация подменяет принципы индивидуализации и справедливости наказания.

Таким образом, средняя статистика превращается в нормативное давление, фактически ограничивая свободу судебного усмотрения и вытесняя содержательные, основанные на праве суждения.

Следовательно, риск реализации принципа справедливости несет не только «цифровой судья», который назначает наказание вместо судьи-человека, но и одобряемое в науке использование ИИ в форме поддержки судейского усмотрения. То есть судья может принять информацию, предоставленную алгоритмами ИИ, во внимание, но мера наказания определяется самим судьей.

Возможность подобной практики требует критического переосмысления роли цифровых технологий в правосудии и разработки комплексных механизмов правовой и этической оценки алгоритмов, используемых в сфере назначения наказания.

БИБЛИОГРАФИЯ

1. Воронин В. Н. Ретрибутивизм, справедливость наказания и учет общественного мнения в современном уголовном праве // Социально-экономическое развитие и качество правовой среды : сборник докладов VIII Московского юридического форума (XIX Международная научно-практическая конференция), г. Москва, 8—10 апреля 2021 г. : в 5 ч. — М. : Университет имени О.Е. Кутафина (МГЮА), 2021. — Ч. 4. — С. 16—19.



2. *Agarwal Srishti*. Use of Artificial Intelligence in Criminal Cases (October 21, 2023) // International Review of Law and Technology. — Vol. 2. — Is. 2. — Forthcoming. — SSRN: <https://ssrn.com/abstract=4609135>. — URL: <http://dx.doi.org/10.2139/ssrn.4609135>.
3. *Bangura G*. The European Union Artificial Intelligence Act: Mitigating Discrimination in Artificial Intelligence Systems : Master Thesis. — University of Applied Arts Vienna, 2024.
4. *Bell F., Legg M*. Judicial Impartiality: AI in Courts // Cambridge Handbook of AI in Courts. — Cambridge University Press, 2025.
5. *Bell F. and Legg M*. Judicial Impartiality: AI in Courts (February 11, 2025) // UNSW Law Research. — No. 25-4. — SSRN: <https://ssrn.com/abstract=5161571>. — URL: <http://dx.doi.org/10.2139/ssrn.5161571>.
6. *Brożek B., Furman M., Jakubiec M., Kucharzyk B*. The Black Box Problem Revisited: Real and Imaginary Challenges for Automated Legal Decision Making // Artificial Intelligence and Law. — 2024. — Vol. 32. — P. 427—440. — DOI: 10.1007/s10506-023-09356-9.
7. *Dou L. & Dou X*. (2025). Towards Just AI: Challenges and Solution Framework for Algorithmic Discrimination in Judicial System // International Journal of Digital Law and Governance. — URL: <https://doi.org/10.1515/ijdlg-2024-0020>.
8. *Engel Ch., Linhardt L., Schubert M*. Code is Law: How COMPAS Affects the Way the Judiciary Handles the Risk of Recidivism // Artificial Intelligence and Law. — 2024. — DOI: 10.1007/s10506-024-09389-8.
9. *Gil Rothschild-Elyassi*. The Datafication of Law: How Technology Encodes Carceral Power and Affects Judicial Practice in the United States (2022).
10. *Hendrickx V*. The Judicial Duty to State Reasons in the Age of Automation? The Impact of Generative AI Systems on the Legitimacy of Judicial Decision-Making // European Law Review. — 2024. — № 1.
11. *Hirsch Andrew Von*. Past or future crimes: Deservedness and dangerousness in the sentencing of criminals. — New Brunswick : Rutgers University Press, 1985. — 220 p.
12. COMPAS and Proxies: Algorithmic Discrimination in Practice / J. Zhang [et al.] // Unpublished manuscript, 2021.
13. *Lai J., Lin H., Zhang L., Wu C*. A Comparative Study of Risk Assessment Tools in Criminal Justice: COMPAS, LSI-R, and Others // Journal of Forensic Psychology Research and Practice. — 2023. — Vol. 23. — No. 1. — P. 45—67.
14. *Papagiannas S*. Automating Intervention in Chinese Justice: Smart Courts and Supervision Reform // Asian Journal of Law and Society. — 2023. — Vol. 10. — No. 1. — P. 123—145. — DOI: 10.1017/als.2023.5.
15. *Papagiannas S*. Smart Courts and Governance in the PRC. Preprint // SSRN, 2023. — URL: <https://ssrn.com/abstract=3777378>.
16. *Rudin C*. Stop Explaining Black Box Machine Learning Models for High Stakes Decisions and Use Interpretable Models Instead // Nature Machine Intelligence. — 2019. — Vol. 1. — No. 5. — P. 206—215.
17. *Ryberg J*. Criminal Sentencing and Artificial Intelligence: What is the Input Problem? // Criminal Law, Philosophy (2024). — URL: <https://doi.org/10.1007/s11572-024-09739-2>.

18. *Ryberg J.* Justice by Algorithm? The Limits of AI in Criminal Sentencing // *Criminal Law and Philosophy*. — 2024. — Vol. 18. — P. 1—18.
19. *Ryberg J.* Sentencing, Artificial Intelligence, and Condemnation: A Reply to Taylor // *Philosophy & Technology*. — 2024. — Vol. 37. — № 2.
20. *Simmons R.* Big Data and Procedural Justice: Legitimizing Algorithms in the Criminal Justice System // *Ohio State Journal of Criminal Law*. — 2018. — Vol. 15. — No. 2. — P. 573—615.
21. *Vargas-Murillo A. R.* et al. Transforming Justice: Implications of Artificial Intelligence in Legal Systems // *Academic Journal of Interdisciplinary Studies*. — 2024. — Vol. 13. — No. 2. — P. 433—450. — DOI: 10.36941/ajis-2024-0059.
22. *Wadsworth Ch., Vera F., Piech Ch.* Achieving Fairness through Adversarial Learning: an Application to Recidivism Prediction // *Proceedings of the FAT/ML Workshop*. — Stockholm, 2018.
23. *Wang N., Tian M. Y.* Intelligent Justice: AI Implementations in China's Legal System // Chapter in Edited Volume, 2022.
24. *Wang N., Tian M. Y.* Intelligent Justice: human-centered considerations in China's legal AI transformation // *AI Ethics* 3, 349—354 (2023). — URL: <https://doi.org/10.1007/s43681-022-00202-3>.
25. *Watamura Eiichiro, Liu Yichen, Ioku Tomohiro.* Judges versus Artificial Intelligence in Juror Decision-Making in Criminal Trials: Evidence from Two Pre-Registered Experiments // *PLOS ONE*. — 2025. — Vol. 20. — № 1.
26. *Zhang Y., Li J.* COMPAS Risk Score and Prediction of Recidivism // *International Journal of Environmental Research and Public Health*. — 2022. — Vol. 19. — No. 10594.
27. *Zhang J. & Han Yu.* (2022). Algorithms Have Built Racial Bias in Legal System-Accept or Not? — 10.2991/assehr.k.220105.224.





**Елена Александровна
АНТОНЯН,**

заведующий кафедрой
криминологии
и уголовно-
исполнительного права
Университета имени
О.Е. Кутафина (МГЮА),
доктор юридических наук,
профессор
eaantonyan@msal.ru
125993, Россия, г. Москва,
ул. Садовая-Кудринская, д. 9

Китайский опыт борьбы с преступлениями в сфере информационных технологий

Аннотация. Статья посвящена комплексному анализу системы противодействия киберпреступности в Китайской Народной Республике в условиях активного развития цифровых технологий и роста преступлений в информационном пространстве. Представлено развитие законодательства КНР в сфере кибербезопасности, включая основные нормативные акты — Закон о кибербезопасности (2017 г.), Закон о безопасности данных (2021 г.) и Закон о защите личной информации (2021 г.), а также Закон против телекоммуникационного и интернет-мошенничества (2022 г.). Рассматриваются меры усиления уголовной ответственности за IT-преступления, формирование новых составов преступлений и практика их применения. Особое внимание уделено институциональной структуре — роли правоохранительных органов и сотрудничеству с крупными технологическими компаниями. Проанализированы результаты реализации целевых кампаний, направленных на выявление и пресечение преступных схем, в том числе с использованием искусственного интеллекта, систем мониторинга интернет-трафика, технологий блокчейна и алгоритмов анализа больших данных. Подчеркивается международное изменение политики КНР в области кибербезопасности — участие в операциях Интерпола, двустороннее и многостороннее сотрудничество, продвижение концепции цифрового суверенитета. Делается вывод о высокой степени интеграции технологических, правовых и организационных механизмов в борьбе с киберпреступностью в Китае, что позволяет эффективно реагировать на современные угрозы в глобальном цифровом пространстве.

Ключевые слова: цифровизация, противодействие киберпреступности, Китай, мошенничество, искусственный интеллект, превентивные меры, правоохранительные органы, финансовые схемы

DOI: 10.17803/2311-5998.2025.129.5.148-158

Elena A. ANTONYAN,

*Head of the Department of Criminology
and Criminal-Executive Law*

of the Kutafin Moscow State Law University (MSAL),

Dr. Sci. (Law), Professor

eaantonyan@msal.ru

9, ul. Sadovaya-Kudrinskaya, Moscow, Russia, 125993

China's Experience in Combating IT Crimes

Abstract. *The article is devoted to a comprehensive analysis of the system of counteracting cybercrime in the People's Republic of China (hereinafter referred to as the PRC) in the context of the active development of digital technologies and the growth of crimes in the information space. The development of the PRC legislation in the field of cybersecurity is presented, including the main regulations — the Cybersecurity Law (2017), the Data Security Law (2021) and the Personal Information Protection Law (2021), as well as the Telecommunication and Internet Fraud Prevention Law (2022). Measures to strengthen criminal liability for IT crimes, the formation of new crimes and the practice of their application are considered. Particular attention is paid to the institutional structure — the role of law enforcement agencies and cooperation with large technology companies. The results of the implementation of targeted campaigns aimed at identifying and suppressing criminal schemes, including the use of artificial intelligence, Internet traffic monitoring systems, blockchain technologies and big data analysis algorithms are analyzed. The international change of China's cybersecurity policy is emphasized — participation in Interpol operations, bilateral and multilateral cooperation, promotion of the concept of digital sovereignty. A conclusion is made about the high degree of integration of technological, legal and organizational mechanisms in the fight against cybercrime in China, which allows for an effective response to modern threats in the global digital space.*

Keywords: *digitalization, counteraction to cybercrime, China, fraud, artificial intelligence, preventive measures, law enforcement agencies, financial schemes*

В условиях стремительной цифровизации Китая, его экономика и общество, столкнулись с ростом преступлений в сфере информационных технологий. За последние пять лет в Китае последовательно наблюдается тенденция усиления мер противодействия киберпреступности: сформирована всеобъемлющая нормативно-правовая база; модернизирована работа правоохранительных органов; используются новейшие технологии — от искусственного интеллекта до сетевого мониторинга. Такие меры принесли конкретные результаты. Например,



только в 2021 г. правоохранительные органы Китая раскрыли около 400 тыс. преступлений в телекоммуникационной сфере и интернет-мошенничеств¹.

Основным законом в Китае стал Закон КНР о кибербезопасности 2017 г., установивший требования по защите сетей, хранению данных внутри страны и ответственности провайдеров. В 2021 г. были приняты сразу два важных акта: Закон о безопасности данных и Закон о защите личной информации, которые усилили ответственность компаний за утечки данных и обработку персональных сведений². Эти законы обязали организации классифицировать данные по уровню важности для национальной безопасности и внедрять меры по их защите, а также ввели правила обработки персональных данных граждан, во многом аналогичные международным (с учетом практики ЕС и АСЕАН)³.

Одновременно обновлялось китайское уголовное законодательство в части ужесточения наказания за киберпреступления. Появились специальные составы, такие как «за злоупотребление личной информацией» (незаконный сбор и сбыт персональных данных) и за «помощь в преступной деятельности в информационных сетях» (охватывает создание и распространение вредоносных программ, хакерских инструментов и пособничество онлайн-мошенникам). По данным Верховной народной прокуратуры КНР, именно преступления, связанные с использованием информационных сетей, в 2021 г. вышли на третье место по числу преступлений в стране.

Рост киберпреступности обусловил принятие новых законов, специально направленных на борьбу с наиболее распространенными ее видами. Так, нововведением стал Закон КНР против телекоммуникационного и интернет-мошенничества, принятый Постоянным комитетом Всекитайского собрания народных представителей 02.09.2022. По сути, этот Закон дополнил уголовные нормы административными санкциями за мелкие мошенничества в онлайн и детализировал меры превентивного характера. Он возложил на телекоммуникационные и финансовые структуры строгие обязанности по предотвращению мошенничества.

В частности, операторы связи и интернет-провайдеры обязаны обеспечить идентификацию пользователей (настоящее имя) при предоставлении услуг (включая мобильную связь, хостинг, обмен сообщениями, онлайн-платежи, игры и т.д.). Провайдеры должны отслеживать подозрительную активность, выявлять сомнительные аккаунты и трафик, связанный с мошенничествами, и при обнаружении требовать повторной верификации личности пользователя либо блокировать услуги. Банки и платежные системы должны мониторить необычные счета и транзакции, собирать данные об устройствах и местоположении при возникновении подозрений, а также мгновенно передавать информацию правоохранительным органам.

Тем самым устанавливается режим «должной осмотрительности» для компаний в предотвращении мошеннических действий в онлайн. В 2021 г. в стране

¹ URL: <https://ипи.рф/news/razvitie-zakonodatelstva-knr-v-oblasti-tsifrovoy-ekonomiki/?ysclid=lu61e572xo553621939> (дата обращения: 30.03.2025).

² URL: <https://www.recordedfuture.com/research/restrictive-laws-push-chinese-cybercrime-toward-novel-monetization-techniques> (дата обращения: 30.03.2025).

³ URL: <https://ипи.рф/news/razvitie-zakonodatelstva-knr-v-oblasti-tsifrovoy-ekonomiki/?ysclid=lu61e572xo553621939> (дата обращения: 30.03.2025).

были запрещены операции с криптовалютой (торговля, майнинг, реклама) и ужесточено регулирование в сфере отмыwania средств. Все эти меры связаны с тем, что злоумышленники активно использовали криптовалюты для перевода полученных незаконным путем доходов за рубеж. Правительство КНР считает, что такие меры должны рассматриваться не как ограничение свободы, а только как необходимый шаг для защиты граждан и экономики страны от растущих киберугроз⁴.

В Китае за борьбу с киберпреступностью отвечает много органов, координируемых Министерством общественной безопасности (МОВ). В его структуре создано специализированное Бюро сетевой безопасности, на которое возложена задача защиты информационных сетей и расследования преступлений в ней⁵. Аналогичные подразделения действуют в управлениях общественной безопасности провинций и городов. Кроме того, регулирование Интернета осуществляет Администрация киберпространства Китая (САС) — орган, ответственный за цензуру и надзор за онлайн-контентом, тесно взаимодействующий с правоохранительными структурами. На каждом официально зарегистрированном веб-сайте в Китае указывается номер местного управления интернет-безопасности полиции (Public Security Bureau), ответственного за его мониторинг.

Таким образом, выстроена многоуровневая система «киберпатруля»: от центрального бюро МОВ до специальных отделов в районах, которая непрерывно отслеживает и пресекает противоправную активность в сети.

В своей деятельности китайские правоохранительные органы применяют проактивный подход, заключающийся в сочетании кибераналитики с масштабными полицейскими операциями. Ежегодно проводятся целевые кампании против наиболее острых угроз. Например, с 2020 г. в стране реализуется операция «Прерывание SIM-карт», в рамках которой полиция совместно с регуляторами связи и Народным банком Китая осуществляют контроль сети, незаконно скупаемые SIM-карты и банковские счета для использования в мошеннических целях. Только в 2021 г. в ходе такого контроля было изъято огромное количество «серых» SIM-карт и устранено свыше 30 тыс. подставных банковских счетов.

Параллельно МОВ совместно с органами, отвечающими за контроль мигрантов в стране, преследует формирования (банды), вывозящие граждан Китая за рубеж для работы в мошеннических колл-центрах. И это не случайно, поскольку многие организаторы телеком-фрода переместились в страны Юго-Восточной Азии с целью скрыться от китайской юрисдикции.

В целях повышения раскрываемости киберпреступлений внедряются новые технологии и специализированные аналитические подразделения. Примером может служить создание в г. Куньшань инновационной команды «Искусственный интеллект (AI) полиции», состоящей из 35 офицеров, использующих более 220 интеллектуальных моделей на базе больших данных, которые помогают оперативно выявлять мошеннические схемы и отслеживать перемещение денежных потоков. В результате эффективность расследований резко возросла (в 2023 г.

⁴ URL: <https://legascom.ru/> (дата обращения: 30.03.2025).

⁵ URL: <https://www.uschina.org/wp-content/uploads/2016/07/Ministry-of-Public-Security-MPS.pdf> (дата обращения: 30.03.2025).



было возвращено жертвам мошенников в сети более 32 млн юаней, при этом доля возмещения по сравнению с предыдущим годом выросла на 62 %).

Известно, как в 2024 г., благодаря автоматизированному анализу, правоохранительные органы Китая за 10 минут отследили перевод 980 тыс. юаней, заблокировав половину суммы, а в течение 8 часов выявили 87 связанных подозрительных счетов, что привело к задержанию 9 преступников в течение трех дней и возврату 200 тыс. юаней пострадавшему⁶. Ранее потребовалось бы несколько недель работы группы следователей, теперь внедряемый в деятельность правоохранительных органов Китая искусственный интеллект позволяет даже малоопытным сотрудникам действовать как профессионалам высокого уровня, значительно сокращая время и повышая результативность расследований.

Изменения в законодательстве позволили существенно улучшить показатели борьбы с киберпреступностью в Китае, ежегодно раскрываются сотни тысяч таких преступлений. Так, в 2023 г. Прокуратура КНР привлекла к уголовной ответственности около 300 000 человек за различные преступления в киберпространстве (на треть больше, чем за аналогичный период 2022 г.). Наибольшую долю случаев составляют⁷ интернет-мошенничества (свыше 42 000 обвиняемых в 2022 г.). Значительное число уголовных дел связано с нелегальным оборотом персональных данных (более 7 000 обвиняемых в злоупотреблениях личной информацией: торговле утечками, мошенничестве с данными). Более 1 000 человек были обвинены за преступления, угрожающие сетевой безопасности (хакерские взломы, распространение вирусов), и около 1 400 человек — за нарушения авторских прав в Интернете. Эти данные демонстрируют многопрофильный характер киберпреступности и масштаб ресурсов, которые задействует Китай для противодействия ей.

В Китае применяются масштабные превентивные меры в борьбе с киберпреступностью. Так, с 2016 по 2019 г. органы МОВ закрыли более 5 000 фальшивых веб-сайтов и 20 000 аккаунтов, выдававших себя за государственные структуры и выманивавших деньги у граждан. Причем такие сайты маскировались под официальные (содержали слова China, National и т.п. в названии), распространяя дезинформацию, мошеннические схемы «вложения в государственные фонды», даже занимались вымогательством⁸. Их ликвидация прошла в рамках целевой кампании против незаконного использования названий государственных органов. Еще одним направлением стало пресечение игровой деятельности онлайн. Дело в том, что в период пандемии COVID-19 наблюдался всплеск нелегальных азартных игр в Интернете, и к концу 2020 г. правоохранительные органы Китая начали расследование около 9 000 уголовных дел, арестовав около 50 000 подозреваемых.

Одной из характерных черт китайского подхода в борьбе с киберпреступностью является активное применение передовых технологий для выявления и

⁶ URL: <https://www.chinadaily.com.cn/a/202410/23/ws6718580ca310f1265a1c9146.html> (дата обращения: 30.03.2025).

⁷ URL: <https://ru.apa.az/asia/kitai-nakazal-za-kiberprestupleniya-280-tys-celovek-za-11-mesyacev-559481> (дата обращения: 30.03.2025).

⁸ URL: https://english.www.gov.cn/statecouncil/ministries/201911/15/content_ws5dcdfd1ac6d0bcf8c4c17220.html (дата обращения: 30.03.2025).

расследования таких преступлений. Это масштабные инструменты мониторинга интернет-трафика, системы цензурной фильтрации, в последние два года — решения на базе искусственного интеллекта.

Китайские правоохранители одними из первых начали внедрять ИИ для анализа киберпреступлений. Алгоритмы машинного обучения используются для обнаружения подозрений в сетевом трафике, распознавания мошеннических звонков и сообщений, сопоставления больших массивов данных о транзакциях. Специальные AI-команды позволяют быстро проследивать сложные финансовые схемы, связанные с мошенничеством. Помимо этого, ИИ применяется для защиты объектов интеллектуальной собственности — автоматизированные системы отслеживают появление в сети контрафактной продукции и фишинговых сайтов, имитирующих бренды. Тестовые внедрения ИИ в ряде китайских городов позволили повысить эффективность расследования без увеличения штата сотрудников. Также ведется работа над прогнозированием киберугроз. Так, анализируя данные (например, всплески определенных схем обмана), алгоритмы могут предупредить о надвигающейся волне кибератак и вовремя применить профилактические меры.

Китай известен самой масштабной системой цензурирования Интернета, часто упоминается как проект «Золотой щит». С технической точки зрения это совокупность средств глубокого анализа пакетов (DPI), фильтрации по ключевым словам и блокировки доменов (адресов), интегрированных в узлы национальных сетей передачи данных. Первые версии системы появились еще в начале 2000-х гг., но за последние годы она значительно усложнилась. Сейчас китайские фильтры способны выявлять запрещенный контент даже при попытках обхода через VPN или прокси-серверы, мгновенно разрывая соединения. «Золотой щит» позиционируют как «общенациональный барьер, фильтрующий и контролирующий информационные потоки», призванный проверять достоверность информации и не допускать запрещенный контент⁹. Под запрещенным контентом здесь понимается не только экстремистский или порнографический материал, но и все, что противоречит законам КНР (например, сайты азартных игр, мошеннические ресурсы, хакерские форумы).

Таким образом, цензура в Китае выполняет одновременно политическую и правоохранительную функцию, делая затруднительной деятельность киберпреступников внутри страны, отсекая их коммуникационные каналы. В дополнение к техническим блокировкам китайское законодательство запретило использование несанкционированных VPN, что затрудняет злоумышленникам связь с зарубежными «теневыми» платформами: провайдеры обязаны пресекать попытки обхода цензуры.

В ответ на использование преступниками новых технологий Китай адаптирует свои подходы. Так, Народный банк Китая, в целях недопущения отмывания преступных доходов переходом на криптовалюты, внедрил системы мониторинга цепочек блокчейн-транзакций, чтобы отслеживать движения незаконных средств. В 2022 г. был принят целый комплекс мер против отмывания денег, обязывающий

⁹ URL: <https://legascom.ru/notes/7480-proekt-zolotoj-shchit-kak-mera-protivodejstviya-kiberprestupleniyam-v-kitajskoj-narodnoj-respublike> (дата обращения: 30.03.2025).



обменники криптовалют и финтех-компании тщательнее проверять операции. В результате большинство криптобирж закрылись или ушли из Китая, а злоумышленники лишились удобного способа сокрытия прибыли.

Но есть и другой пример, когда Китай использует позитивный потенциал блокчейна: например, для хранения цифровых доказательств. С 2018 г. Верховный народный суд КНР допускает доказательства, сохраненные в блокчейне, к рассмотрению в судах, при условии обеспечения их подлинности. Правоохранительные органы экспериментируют с блокчейн-платформами для фиксации цепочки хранения улик, с целью исключения фальсификации цифровых доказательств при расследовании.

Технологические платформы Китая также вовлечены в борьбу с киберугрозами. Крупнейшие интернет-компании (Tencent, Alibaba и др.) сотрудничают с органами МОВ, предоставляя доступ к необходимым данным при расследовании. На основании совместных приказов правоохранительных органов и регуляторов связи созданы системы раннего предупреждения: при обнаружении попытки мошеннического звонка или подозрительного сообщения возможной жертве автоматически отправляется предупреждение. Скоординированная между банками, операторами и полицией система уведомления способна определять, что звонок может исходить от мошенника, и выдать на экране телефона пользователя примерно такую надпись: «Осторожно». Кроме того, при зафиксированных случаях мошенничества полиция обязана выяснять, какие персональные данные использованы злоумышленниками, и устранять утечку в источнике. Такой подход позволяет более комплексно перекрывать возможность для повторных атак.

Важно отметить, что, усиливая технократический контроль над Интернетом, власти Китая стараются сохранять баланс между безопасностью и развитием цифровой экономики. Так называемая цифровая цензура нацелена прежде всего на криминальный и вредоносный контент. В последние годы даже наблюдается смягчение давления на IT-сектор с учетом необходимости инноваций. Например, в 2023 г. были даны сигналы о поддержке развития технологических компаний при одновременном соблюдении требований к безопасности данных. Но, несмотря на это, Интернет в Китае остается самым контролируемым в мире, что, с одной стороны, создает для киберпреступников среду, доставляющую затруднения, а с другой — заставляет их искать новые ухищрения и иногда перемещаться за пределы страны.

Понимая трансграничный характер киберугроз, Китай активно поддерживает международные усилия по их нейтрализации. КНР является членом Интерпола и регулярно пользуется его механизмами для розыска киберпреступников, скрывающихся за рубежом. Национальное центральное бюро (НЦБ) Интерпола в Пекине входит в состав Бюро международного сотрудничества МОВ. Через эту структуру китайские правоохранительные органы обмениваются разведывательной информацией о киберпреступниках с коллегами по всему миру и инициируют издание так называемых красных уведомлений на розыск преступников. Китайское НЦБ принимает активное участие в глобальных операциях Интерпола, направленных против киберпреступности и других преступлений, связанных с ней.

В частности, представители Китая регулярно задействованы в совместных рейдах, координируемых Интерполом, по пресечению сетей финансового

мошенничества, торговли данными и др. В 2021—2022 гг. проходила серия международных операций (First Light, Killer Bee и др.), направленных против телефонных мошенников, в реализацию которых китайская полиция внесла значительный вклад, особенно по линии обмена информацией о схемах и счетах, используемых преступниками. Деятельность через Интерпол помогает Китаю обнаружить преступников, скрывающихся вне его юрисдикции, и добиваться их привлечения к ответственности.

Тенденцией последних лет стала миграция части китайского криминального киберрынка за рубеж. Под давлением усиленного внутреннего контроля значительная часть криминальной активности переместилась на иностранные площадки. Опытные китайские хакеры и продавцы краденых данных все чаще действуют на англоязычных и русскоязычных теневых форумах (RaidForums, Exploit, XSS и др.), на которых они предлагают к продаже украденные банковские карты, базы данных и доступы. При этом внутри страны такие действия стали почти невозможными, поскольку постоянные операции правоохранительных и других контролирующих органов приводят к закрытию локальных нелегальных маркетплейсов и групп в мессенджерах. Преступники вынуждены шифроваться и переходить в защищенные каналы, как правило, в мессенджер Telegram, поскольку китайские форумы мониторят власти.

В последние годы Китай выстраивает тесное взаимодействие со странами Юго-Восточной Азии по вопросам борьбы с трансграничными киберпреступлениями, и прежде всего с телеком-фродом и онлайн-азартными играми. Эти виды преступлений часто организуются в соседних государствах, но нацелены на граждан КНР (их называют «заморские мошеннические фабрики»). В 2023 г. китайские власти инициировали совместные операции с Таиландом, Мьянмой, Лаосом, Камбоджей и Филиппинами, чтобы ликвидировать преступные хабы. Так, Китай вместе с партнерами провел зачистки ряда скам-комплексов в приграничных районах Мьянмы и Камбоджи, где удерживались обманом тысячи людей, которых заставляли заниматься телефонными и интернет-мошенничествами.

Китайские правоохранительные органы поделились с коллегами списками разыскиваемых лиц и методической информацией, разъясняющей: какими способами вербуются жертвы, как маскируют интернет-трафик, как переводят деньги через криптовалюты. Это позволило скоординировать рейды: например, в Таиланде при содействии Китая были отключены энергосбережение и связь у ряда подозрительных объектов вдоль границы с Мьянмой, чтобы парализовать работу мошенников. В результате только за 2023 г. Таиланд и Филиппины закрыли несколько крупных центров онлайн-казино и мошеннических колл-центров, депортировав в Китай около 1 000 китайских граждан — предполагаемых организаторов и участников этих схем. Также были освобождены сотни вовлеченных в эту деятельность обманом работников, пострадавших от траффикинга. Такой опыт признан удачным примером сотрудничества в сфере безопасности, когда страны с разными политическими системами объединяются против общей криминальной угрозы, невзирая на все разногласия.

Китай укрепляет кибербезопасное партнерство и с другими государствами. С Российской Федерацией еще в 2015 г. было подписано межправительственное Соглашение о сотрудничестве в обеспечении международной информационной



безопасности, заложившее основы обмена информацией о киберугрозах и координации действий. В тот же 2015 г., в рамках Шанхайской организации сотрудничества (ШОС), в г. Сямэнь прошли первые совместные учения Xiamen-2015 по борьбе с кибертерроризмом в сети, в которых Китай и Россия участвовали вместе с другими членами ШОС. Эти учения отработали методики совместного выявления и пресечения террористической пропаганды и координации преступников через Интернет.

С тех пор Китай регулярно выступает за усиление роли ШОС и БРИКС в вопросах обеспечения кибербезопасности. На саммитах обсуждаются идеи о создании кодекса поведения в киберпространстве и рабочих групп по противодействию киберпреступности. В 2021 г. Китай и Россия опубликовали совместное заявление о сотрудничестве в сфере международной информационной безопасности, подтвердив тем самым намерение противостоять попыткам использования ИКТ в преступных и военных целях. Помимо этого, китайские компании, обеспечивающие кибербезопасность, сотрудничают с зарубежными структурами: например, российская «Лаборатория Касперского» и китайская GETS Cyber Security заключили соглашение об обмене опытом и технологиями для борьбы с киберугрозами.

Взаимодействие с западными странами осложнено геополитическими разногласиями, Китай избирательно участвует в диалоге по вопросам борьбы с киберпреступностью. В частности, КНР поддерживает инициативы ООН: активно участвует в проекте Конвенции ООН против киберпреступности (запущен в 2019 г. при ведущей роли России) и выступает за суверенное право государств регулировать Интернет внутри своих границ.

Также Китай присоединился к ряду двухсторонних соглашений об обмене данными по киберугрозам. Например, до 2020 г. действовал механизм китайско-американских консультаций по кибербезопасности (создан в 2015 г.), позволивший на время снизить активность хакерских атак на коммерческие компании. Кроме того, китайская полиция сотрудничает с крупными транснациональными IT-корпорациями в расследовании конкретных дел. Так, в 2020 г. при поддержке Microsoft и международных экспертов китайские правоохранительные органы раскрыли одну из ботнет-сетей, использовавших сервера в разных странах для атак на китайские учреждения.

Таким образом, Китай постепенно интегрируется в глобальную систему противодействия киберпреступности, продвигая при этом собственное видение «цифрового суверенитета».

За пятилетний период 2018—2023 гг. Китай достиг значительных результатов в пресечении киберпреступлений. Если в 2018—2019 гг. основной упор делался на борьбу с утечками данных и взломами (после ряда скандальных инцидентов с продажей баз персональных данных), то к 2020—2021 гг. приоритет сместился к массовым мошенничествам. В последние годы в Китае явно прослеживается консолидация криминальной активности в онлайн-среде. Многие традиционные преступления уходят в киберпространство. Такие преступные деяния, как азартные игры, мошенничество, финансовые пирамиды, все чаще осуществляются через интернет-технологии.

Одновременно появляются и совершенно новые киберпреступления, связанные с инновационными технологиями. В 2023 г. китайские правоохранители

зафиксировали первые случаи мошенничества, использующего элементы метавселенной и блокчейн-платформ: злоумышленники продавали несуществующие «виртуальные земли» и NFT-активы, оформляя их как инвестиционные проекты. Отмечается рост преступлений с применением технологии Deepfake и искусственного интеллекта. Известны многочисленные попытки выдавать себя за знакомых через сгенерированные видео или голос с целью выманивания денег. В Китае на эти вызовы реагируют прежде всего экспертные подразделения, которые, например, разработали в 2023 г. стандарты для обнаружения поддельных цифровых лиц и представили первый в стране стандарт Deepfake в финансовой сфере.

Одним из самых резонансных киберпреступлений последних лет в Китае явилась утечка в 2022 г. данных полиции Шанхая, когда хакер под псевдонимом ChinaDan выставил на продажу базу данных объемом 23 терабайта, содержащую персональные данные 1 млрд граждан Китая, включая имена, адреса, телефоны, биометрические данные. Такая утечка ведомственной базы является одним из крупнейших в мире взломов IT-системы. Этот факт ускорил принятие дополнительных мер по защите государственных информационных систем и, скорее всего, стал одной из причин огромного штрафа компании Didi, которую обвинили в недостаточной защите данных.

Другим примером, способствовавшим усилению мер безопасности в Китае, явилась многолетняя борьба с хакерской группировкой Dark Hotel, которая занималась кибершпионажем против китайских высокопоставленных лиц через заражение Wi-Fi в отелях. В 2019—2020 гг. китайские спецслужбы выявили и нейтрализовали деятельность данной группы на своей территории, что было весьма необычно, так как ранее операции Dark Hotel фиксировались в основном за рубежом. Стоит также отметить серию уголовных дел против хакеров внутри страны. Так, в 2018 г. правоохранительные органы Китая арестовали группу программистов, развивавших ботнет WireLoader, с помощью которого похищались учетные записи и деньги у китайских пользователей. В 2020 г. в г. Сиань были задержаны несколько человек, продававших в даркнете данные клиентов крупных отелей с информацией о 130 млн гостей.

Китай действительно преследует киберпреступников и привлекает их к ответственности по всей строгости уголовного закона, особенно если их действия направлены против внутренних интересов государства.

В области международных угроз Китай все чаще выступает не только как обвиняемый (страны Западной Европы часто заявляют о китайских арт-группах), но и как жертва кибератак. Китайские инфраструктуры регулярно подвергаются атакам извне: атакуются правительственные сайты, базы данных компаний, организаций и учреждений (в 2013 г. произошла DDoS-атака на сайт газеты «Жэньминь жибао», а ранее, в 2010 г., в результате хакерской операции была нарушена работа китайской поисковой системы Baidu на несколько часов). Китай реагирует на такие эпизоды, во-первых, усилением международного сотрудничества, требуя уважать цифровой суверенитет, во-вторых, повышением собственной киберустойчивости (создаются резервные инфраструктуры, совершенствуются национальные шифровальные стандарты).

Опыт Китая в противодействии IT-преступлениям за последние годы демонстрирует целостный и проактивный подход государства к обеспечению



кибербезопасности. За короткий срок была создана законодательная база — от Закона о кибербезопасности до специальных нормативных актов против онлайн-мошенничества, что обеспечило прозрачность в цифровой среде и дало правоохранительным структурам обоснованные дополнительные полномочия. Правоохранительные органы, опираясь на новые законы, развернули беспрецедентные по масштабу кампании по выявлению и пресечению киберпреступлений, используя как традиционные методы работы, так и современные технологии (ИИ, большие данные, автоматический мониторинг). При этом важной составляющей стало привлечение частного сектора (компании связи, интернет-платформы и банков), которые юридически обязаны помогать в предотвращении и расследовании преступлений, связанных с их сервисами.

Именно эффективные системные меры, сочетающие превентивное регулирование, четкое правоприменение и международное сотрудничество, позволяют достичь эффективности в борьбе с киберпреступностью в Китае.

Безусловно, китайский подход имеет свою специфику — значительная роль отводится контролю над информационным пространством и государственному надзору, что может быть неприменимо в странах с другими ценностными моделями. В то же время ряд элементов опыта Китая представляет интерес и для других стран: в частности, законодательное закрепление обязанностей интернет-сервисов по противодействию преступлениям; создание межведомственных систем раннего предупреждения граждан о киберугрозах; интеграция технологий ИИ в работу правоохранительных органов.

БИБЛИОГРАФИЯ

1. Ван Г. Уголовно-правовое регулирование противодействия киберпреступности в Китае: состояние, тенденции, недостатки // Вестник Санкт-Петербургского университета. — Право. — 2022. — Т. 13. — № 3. — С. 661—677.
2. Се Ч. Противодействие цифровой преступности в сфере торговли людьми в государстве АСЕАН: опыт Китая // Вестник Поволжского института права и управления. — 2025. — Т. 25. — № 1. — С. 5—13.
3. Сюй Кай. Законодательство о борьбе с организованной преступностью в КНР: недостатки и совершенствование // Право и государство: теория и практика. — 2010. — № 1 (61). — С. 138—142.

Современное состояние и тенденции киберпреступности в Монголии

Аннотация. Статья посвящена криминологической характеристике и особенностям киберпреступности в Монголии, основные черты которой во многом свойственны подавляющему большинству государств в мире, в том числе и соседней Российской Федерации. При этом в ходе анализа количественных и качественных показателей данного негативного явления выявляются ряд особенностей, свойственных для развивающихся стран. Предметом исследования явились современное состояние, динамика и тенденции киберпреступности государства, расположенного на азиатском континенте между одними из основателей БРИКС, Российской Федерацией и Китаем. Киберпреступность как явление, не имеющее государственных границ, отчетливо проявляет транснациональные и мультинациональные черты и характер. В ходе изучения и анализа указанного феномена были использованы следующие методы исследования: формально-логический, сравнительно-правовой, статистический, социологический и др. Новизна материала заключается в использовании самых новейших статистических данных по сути проблематики исследования, оценке и рассмотрении разных мнений и суждений по существу вопроса. Цель исследования заключается в подчеркивании утверждения, что современная киберпреступность — это явление, свойственное всем государствам, с разной структурой внутреннего устройства, независимо от политических, экономических, идеологических и других аспектов, проявляющее повсеместно стойкую тенденцию к росту и увеличению своих масштабов, в то время как повсюду наблюдаются снижение и стабилизация числа зарегистрированных преступлений в целом.

Ключевые слова: состояние, тенденция, динамика, киберпреступность, Монголия, транснациональный, мошенничество, уголовная ответственность



Юрий Владимирович ХАРМАЕВ,
доцент кафедры
криминологии
и уголовно-
исполнительного
права имени
В. Е. Эминова
Университета имени
О.Е. Кутафина (МГЮА),
кандидат юридических
наук, доцент
yuvharmaev@msal.ru
125993, Россия, г. Москва,
ул. Садовая-Кудринская,
д. 9

DOI: 10.17803/2311-5998.2025.129.5.159-168

Yuri V. KHARMAEV,

Associate Professor of the Department of Criminology
and Criminal-Executive Law named after V. E. Eminov
of the Kutafin Moscow State Law University (MSAL),
Cand. Sci. (Law), Associate Professor
yuvharmaev@msal.ru

9, ul. Sadovaya-Kudrinskaya, Moscow, Russia, 125993

Cybercrime in Mongolia. Up-to-date state and trends

Abstract. *The article is devoted to criminological characteristics and peculiarities of a cybercrime in Mongolia, the main features of which is mainly typical for most states in the world, including its neighbor the Russian Federation. At the same time during the analysis of quantity and quality indicators of such a negative phenomenon, there are some peculiarities, typical for developing countries. The subject of the study is up-to-date state, dynamics and trends of cybercrime of the state, which is located at the Asian continent between one of the BRICS founder, the Russian Federation and China. Cybercrime as a phenomenon without any state borders is vividly shows transnational and multinational traits and character. During the study and analysis of the said phenomenon the following study methods were used: formal-logical, comparative, statistical, sociological and others. The novelty of the content is in usage of the newest statistical data on the essence of the research problem, assessment and consideration of different opinions and judgements on the subject matter. The aim of the study is to highlight the statement, that the modern cybercrime is a phenomenon, typical for all states, with different internal structure, regardless political, economic, ideological and other aspects, which widely shows persistent growth trend and expanding its scale at a time when there is a decrease and stabilization of the number of reported crimes in general.*

Keywords: *state, trend, dynamics, cybercrime, Mongolia, transnational, fraud, criminal liability*

Объективные современные реалии убедительно показывают, что трансформация современного общества приносит не только преимущества и блага при использовании новейших технологий в целях улучшения качества жизни (коммуникации, получение информации и др.), но и привносит целый комплекс новых видов и форм преступных проявлений.

В юридической литературе отсутствует законодательное закрепление данного деликта, однако в соответствии с доктринальными подходами можно согласиться с пониманием киберпреступности (от англ. cybercrime — киберпреступность, киберпреступление) как преступности, связанной с использованием

информационных технологий, социальных сетей и Интернета¹. Следует согласиться с мнением ряда исследователей, констатирующих, что определение «киберпреступность» шире, чем понятие «компьютерная преступность», и более точно отражает природу такого явления, как преступность в информационном пространстве.

Современные новейшие IT-технологии, интернет-услуги явились лакомым куском для противоправных посягательств, вызовов и угроз со стороны злоумышленников, следовательно, противодействие киберпреступности становится одним из приоритетных направлений в деятельности правоохранительных структур любого государства².

В данном исследовании предпринимается попытка проанализировать современное состояние, динамику и тенденции киберпреступности в Монголии — государстве, некогда особо не отличавшемся от России (СССР) в политической, экономической, социальной сферах жизни, ранее в целом представителе социалистической правовой семьи. Современная Монголия, расположенная на азиатском континенте между одними из основателей БРИКС³, Российской Федерацией и Китаем, по-прежнему представляет повышенный интерес со стороны не только соседей, но и других государств.

Монгольское государство традиционно представляет исторический, культурный, политический, а в последнее время и законодательный интерес, и стоит отметить, что граница между Россией и Монголией составляет более 3 500 км. Сегодня экономика Монголии развивается наиболее динамично из всех стран азиатского континента⁴. Республика представляется едва ли не самым перспективным рынком сбыта не только в Северо-Восточной Азии, но и во всем Азиатско-Тихоокеанском регионе. По прогнозам специалистов Всемирного банка, в ближайшие десять лет экономика Монголии будет расти в среднем на 15 % в год. С момента установления суверенной Народной республики в 1924 г., не без помощи и поддержки молодого Советского государства, социально-экономическая, политическая, идеологическая и правовая жизнь протекала в тесном взаимодействии и при взаимовлиянии⁵. Не случайно во времена СССР Монгольскую

¹ Кувшинова В. С. Криминологическая характеристика киберпреступности // Международный журнал гуманитарных и естественных наук. 2020. № 5–4. С. 53—57 ; Агаркова А. А., Синицына В. А. Киберпреступность в современной России // Международный журнал гуманитарных и естественных наук. 2021. № 5–3. С. 13—16.

² Дерюгин Р. А. Киберпреступность в России: современное состояние и актуальные проблемы // Вестник Уральского юридического института МВД России. 2019. № 2. С. 46—49.

³ БРИКС (англ. BRICS — сокращение от Brazil, Russia, India, China, South Africa) — объединение десяти государств: Бразилии, России, Индии, КНР, ЮАР, ОАЭ, Ирана, Египта, Эфиопии и Индонезии, основанное в июне 2009 г. как БРИК (BRIC) в рамках Петербургского экономического форума с участием министров экономики Бразилии, России, Индии, Китая.

⁴ Монгол улсын статистикийн эмхтгэл. Mongolian Statistical Yearbook. 2012. Улаанбаатар, 2023.

⁵ Жанцан С. Монгол Улсын Эрүүгийн эрх зүйн онол. Улаанбаатар, 2009.



Народную Республику называли 16-й республикой, настолько близкими и дружественными были связи между двумя государствами.

Конституция Монголии в ч. 1 ст. 19 четко определяет приоритет защиты прав, свобод человека и обязанность государства по обеспечению экономических, социальных и правовых гарантий, а также ведению борьбы с нарушением прав, свобод и законных интересов человека и гражданина, государство должно следить за своевременным восстановлением незаконно нарушенных и ограниченных прав граждан⁶.

Монголия в свое время поддержала резолюцию, выдвинутую Российской Федерацией на Генеральной Ассамблее ООН в 2021 г., на злободневную и актуальную тему «Противодействие использованию информационно-коммуникационных технологий в преступных целях» и активно занялась реализацией Конвенции по противодействию киберпреступности у себя в стране.

Проблемы с криминализацией и преступной активностью в информационно-телекоммуникационном пространстве имеют стойкую тенденцию роста (причем многократно) во многих странах мира⁷. Не обошли такие особенности и развивающиеся страны (страны Глобального Юга), в том числе и Монголию⁸.

Согласно официальным статистическим данным МВД России, динамика снижения уровня преступности в целом наблюдается на протяжении уже ряда лет, в то же время показатели киберпреступности стремительно увеличиваются из года в год (рис. 1)⁹.

Если в 2020 г. общее количество зарегистрированных преступлений составляло 2 044,2 тыс., то число киберпреступлений составило 511 050, т.е. порядка 25 % от всей преступности; в 2021 г. общее количество зарегистрированных преступлений снизилось до 2 004,4 тыс., а число киберпреступлений увеличилось до 517 135 (25,8 %). Похожая картина наблюдалась и в 2022 г. — общая преступность составила 1 966,8 тыс. делитов, а киберпреступления возросли до 521 202 преступления (их доля составила 26,5 %); в 2023 г. общее количество преступлений



Рис. 1. Динамика и доля киберпреступлений в Российской Федерации за 2020—2024 гг.

⁶ Гантулга Н., Хармаев Ю. В. Некоторые вопросы ресоциализации осужденных в Монголии // Криминологический журнал Байкальского государственного университета экономики и права. 2015. Т. 9. № 2. С. 379.

⁷ Ищук Я. Г., Пинкевич Т. В., Смолянинов Е. С. Цифровая криминология : учебное пособие. М., 2021.

⁸ Какие страны относятся к Глобальному Югу // URL: <https://dzen.ru/a/zuvi4sj3hqkv2riz> (дата обращения: 12.03.2023).

⁹ Краткая характеристика состояния преступности в Российской Федерации за январь — декабрь 2024 года // URL: <https://xn--b1aew.xn--p1ai/reports/item/60248328/> (дата обращения: 11.03.2025).

снизилось до 1 947,2 тыс., из них число киберпреступлений составило 677 626 (34,8 %), наконец, в 2024 г. количество преступлений составило 1 911,3 тыс., а число киберпреступлений увеличились до 764 520, что составило 40 % от всей зарегистрированной преступности.

В Монголии за этот период также можем наблюдать увеличение доли киберпреступлений, хотя и не такое резкое, как в Российской Федерации, но преступность в целом у юго-восточного соседа ежегодно увеличивалась (рис. 2).

Как следует из рис. 2, в Монголии в 2020 г. общее количество зарегистрированных преступлений составило 23 064, из них киберпреступлений — 1 179, т.е. 7,8 % от всей преступности; в 2021 г. общее количество зарегистрированных преступлений увеличилось до 25 429, соответственно, число киберпреступлений также увеличилось до 4 825 (доля — 19,0 %); в 2022 г. общее количество преступлений увеличилось до 35 340 делитов, а число киберпреступлений — до 8 563 (24,2 %); в 2023 г. общее количество преступлений возросло до 35 574, из них число киберпреступлений увеличилось до 9 270 (23,3 %), наконец, в 2024 г. количество преступлений составило 44 673, число киберпреступлений также увеличилось до 13 061, что составило 32,2 % от всей зарегистрированной преступности (табл. 1).

В официальной статистике Аналитического центра Главного управления полиции (ГУП) Монголии регистрируются по 33 статьям Уголовного кодекса Монголии деяния, связанные с использованием IT-технологий, среди них особо выделяются следующие составы преступлений: мошенничество (ст. 17.3); незаконный доступ к электронной информации (ст. 26.1); распространение ложной информации (ст. 13.14); кража (ст. 17.1) и хищение (ст. 17.4)¹⁰ (табл. 2).

Как видно из представленной табл. 2, наибольшую долю среди киберпреступлений составляет мошенничество (ст. 17.3 УК Монголии). По сравнению с 2020 г. в 2021 г. рост числа преступлений по статье о мошенничестве в абсолютных показателях составил 2 577, в то время как доля в целом киберпреступности — 79,9 %. В 2022 г. прирост числа преступлений по данной статье достиг уже 3 850, т.е. 90,0 % от всей киберпреступности. В 2023 г. также наблюдается неуклонный рост данных преступлений до 7 906 преступлений мошеннического характера (85,2 %). В 2024 г. также фиксируется резкий скачок данных преступлений: рост



Рис. 2. Динамика и доля киберпреступлений в Монголии за 2020—2024 гг.

¹⁰ В УК Монголии ст. 17.1 предусматривает ответственность за кражу личного имущества граждан, ст. 17.4 включает ответственность за посягательство на иные формы собственности (включая государственную).



на 3 805 преступлений, их доля составила 89,6 % от общего количества киберпреступлений. Указанная тенденция хорошо про-
демонстрирована на рис. 3 и 4.

Таблица 1

Динамика киберпреступности в Монголии за 2021—2024 гг.

Показатель	2021	Динамика		2023	Динамика		2024	Динамика	
		Рост числа	%		Рост числа	%		Рост числа	%
Общее количество преступлений	25 429	35 340	39,0	35 574	234	0,7	44 673	9 099	25,6
Киберпреступления	4 825	8 563	77,5	9 270	707	8,3	13 061	3 791	40,9
Доля от общего чис- ла преступлений, %	19,0	24,2	5,3	26,1	1,8		29,2	3,2	

Таблица 2

Наиболее часто совершаемые преступления с использованием компьютерных технологий в Монголии

Статьи УК	2015	2016	2017	2018	2019	2020	2021	2022	2023	2024	Общее количество
Ст. 17.3	17	69	136	590	641	1 281	3 858	7 708	7 906	11 711	33 917
Ст. 26.1	—	—	39	43	53	145	150	256	383	400	1 469
Ст. 13.14	—	—	—	—	—	173	126	124	208	327	958
Ст. 17.1	—	—	—	—	—	67	92	126	129	140	554
Ст. 17.4	—	—	—	—	—	13	12	29	25	73	152

Следует также отметить, что в Монголии наблюдается значительный рост данной формы хищений (мошенничества) и среди несовершеннолетних. По оценкам практических работников правоохранительных органов Монголии, это связано в первую очередь с использованием подростками возможностей социальных сетей для посягательств на чужое имущество¹¹, что особенно проявилось во времена ковидных ограничений.

Исходя из представленных статистических данных о состоянии и динамике киберпреступности в Монголии, можно выделить некоторые тенденции:

- в начале 20-х гг. XXI столетия начинается рост киберпреступлений в Монголии;
- во времена ковидных ограничений (2019 и 2020 гг.) наблюдаются следующие особенности: если в 2019 г. абсолютные показатели киберпреступности особо не заметны, то в 2020 г. произошел резкий рост киберпреступлений: в абсолютных показателях почти вдвое, в процентном соотношении на 87,1 %;
- среди всех киберпреступлений преобладает мошенничество, которое на протяжении ряда последних лет составляет от 79,9 % до 90,0 % от всех остальных киберпреступлений;
- как отмечают эксперты¹² и представители правоохранительных структур Монголии, представленные статистические показатели не всегда объективны в силу высокого уровня латентности других составов преступлений (помимо мошенничества) в силу различных обстоятельств, среди которых отмечают следующие:
- неосведомленность граждан Монголии о факте противоправного воздействия в отношении их законных интересов;
- межтерриториальность киберпреступлений — злоумышленники и потерпевшие зачастую могут быть расположены на территориях разных государств;



Рис. 3. Мошенничество с использованием IT (ст. 17.3 УК Монголии)



Рис. 4. Иные преступления, совершенные с помощью IT-технологий в Монголии

¹¹ Хармаев Ю. В. К вопросу об особенностях преступности несовершеннолетних в Монголии на современном этапе // Конституционные основы противодействия преступности в России: к 30-летию Конституции Российской Федерации : сборник статей по материалам Всероссийской (национальной) научно-практической конференции. Ставрополь, 2024. С. 139—144.

¹² Одонгэрэл Д. Цахим гэмт хэрэг нь Монгол Улсын эдийн засгийн аюулгүй байдалд заналхийлж байна. Улаанбаатар, 2023.



- сложность и трудности предупреждения, профилактики и пресечения киберпреступлений ранее известными и распространенными методами и средствами;
- специфика современной характеристики личности преступника (интеллектуальная подготовленность преступников, экспертная деятельность в IT-технологиях);
- специалистам отдела по борьбе с киберпреступностью Департамента отдела экономических преступлений Монголии требуется повышение уровня подготовки и специального образования в соответствии с современными угрозами киберпреступности.

Как совершенно верно подчеркивают профессор Д. А. Степаненко и доцент А. А. Митрофанова, современная ситуация с киберпреступностью в России отличается ростом «негативной (криминальной) информационной грамотности одной части населения страны и информационной безграмотности другой его части... определенной неспособностью правоохранительной системы контролировать такую преступность, принимать адекватные меры, направленные на борьбу с IT-преступлениями, с учетом новых способов и методов их совершения»¹³.

Учитывая научные предположения о будущем развитии киберпреступности во всем мире, в национальных законодательствах России и Монголии должны быть учтены практика и опыт зарубежных стран, осуществлены иные способы модернизации функций правоохранительных структур, направленные на борьбу с киберпреступностью. Например, в отличие от УК РФ, в китайском законодательстве предусмотрена уголовная ответственность юридических лиц, что позволило китайским правоохранителям, как отмечают исследователи, повысить эффективность противодействия киберпреступности¹⁴.

В Объединенных Арабских Эмиратах, как наиболее интернет-активном государстве в мире, кибербезопасность определена как один из главных приоритетов национальной безопасности. По данным UN Broadband Commission report 2014 г., около 85 % людей, проживающих в ОАЭ, пользуются Интернетом. ОАЭ на Ближнем Востоке занимают 3-е место по использованию Интернета, а в мировом масштабе — 17-е место, в связи с этим социальные сети и цифровое пространство Арабских Эмиратов активно подвергаются нападениям хакеров¹⁵. Огромный ущерб наносится потерпевшим от мошеннических действий в США, например, в 2021 г. более 95 000 человек подверглись интернет-атакам, в результате чего убыток составил 770 млн долларов, что в 18 раз больше, чем в 2017 г.¹⁶

¹³ Степаненко Д. А., Митрофанова А. А. Противодействие киберпреступности как современный вызов традиционной криминалистике // Союз криминалистов и криминологов. 2022. № 3. С. 91—97.

¹⁴ Дегтярев А. А. Противодействие киберпреступности: необходимость учета зарубежного опыта // Союз криминалистов и криминологов. 2023. № 1. С. 50—55.

¹⁵ О мерах по обеспечению кибербезопасности в ОАЭ // URL: <http://www.iimes.ru/?p=47341> (дата обращения: 12.03.2023).

¹⁶ Флетчер Э. (25.01.2022). Социальные сети — золотая жила для мошенников в 2021 году / Федеральная торговая комиссия // URL: <https://www.ftc.gov/news-events/data-visualizations/data-spotlight/2022/01/social-media-gold-mine-scammers-2021>.

В Монголии, несмотря на расширение полномочий правоохранительных структур, вопрос электронного сбора данных и вторжения в личную жизнь тщательно рассматривается в Законе о связи (2019 г.) и Законе об оперативно-розыскной деятельности (1997 г.), также в Законе «О защите персональных данных» (с изменениями) (2022 г.)¹⁷. Стали более четко и подробно регламентироваться вопросы, связанные с защитой неприкосновенности частной жизни при сборе, обработке и использовании информации в интернет-среде (например, в социальных сетях)¹⁸.

Резюмируя вышесказанное, следует подчеркнуть, что современные направления киберпреступности постоянно трансформируются, видоизменяются и обладают специфическими криминологическими характеристиками, свойственными конкретным государствам, в зависимости от их социально-экономического развития, политической обстановки, состояния законодательства, идеологической составляющей и эффективности и потенциала правоохранительных структур, а также правовой грамотности (культуры) населения.

БИБЛИОГРАФИЯ

1. *Азаркова А. А., Сеницына В. А.* Киберпреступность в современной России // Международный журнал гуманитарных и естественных наук. — 2021. — № 5–3. — С. 13–16. — DOI: 10.24412/2500-1000-2021-5-3-13-16.
2. *Гантулга Н., Хармаев Ю. В.* Некоторые вопросы ресоциализации осужденных в Монголии // Криминологический журнал Байкальского государственного университета экономики и права. — 2015. — Т. 9. — № 2. — С. 378–384.
3. *Дегтярев А. А.* Противодействие киберпреступности: необходимость учета зарубежного опыта // Союз криминалистов и кримиологов. — 2023. — № 1. — С. 50–55.
4. *Дерюгин Р. А.* Киберпреступность в России: современное состояние и актуальные проблемы // Вестник Уральского юридического института МВД России. — 2019. — № 2. — С. 46–49.
5. *Жанцан С.* Монгол Улсын Эрүүгийн эрх зүйн онол. — Улаанбаатар, 2009.
6. *Зүмбэрэллхам Д.* Криминологийн онол. — Улаанбаатар, 2023.
7. *Ищук Я. Г., Пинкевич Т. В., Смольянинов Е. С.* Цифровая криминология : учебное пособие. — М., 2021.
8. Какие страны относятся к Глобальному Югу // URL: <https://dzen.ru/a/zuvi4sj3hqkv2riz> (дата обращения: 12.03.2023).
9. Краткая характеристика состояния преступности в Российской Федерации за январь — декабрь 2024 года // URL: <https://xn--b1aew.xn--p1ai/reports/item/60248328/> (дата обращения: 11.03.2025).
10. *Кувшинова В. С.* Криминологическая характеристика киберпреступности // Международный журнал гуманитарных и естественных наук. — 2020. — № 5–4. — С. 53–57.
11. Монгол улсын статистикийн эмхтгэл Mongolian Statistical Yearbook. 2012. — Улаанбаатар, 2023.

¹⁷ Сборник законодательных актов Монголии // URL: <http://www.legal.info.mn>.

¹⁸ *Зүмбэрэллхам Д.* Криминологийн онол. Улаанбаатар, 2023.



12. *Одонгэрэл Д.* Цахим гэмт хэрэг нь Монгол Улсын эдийн засгийн аюулгүй байдалд заналхийлж байна. — Улаанбаатар, 2023.
13. О мерах по обеспечению кибербезопасности в ОАЭ // URL: <http://www.iimes.ru/?p=47341> (дата обращения: 12.03.2025).
14. *Степаненко Д. А., Митрофанова А. А.* Противодействие киберпреступности как современный вызов традиционной криминалистике // Союз криминалистов и криминологов. — 2022. — № 3. — С. 91—97.
15. *Флетчер Э.* (25.01.2022). Социальные сети — золотая жила для мошенников в 2021 г. / Федеральная торговая комиссия // URL: <https://www.ftc.gov/news-events/data-visualizations/data-spotlight/2022/01/social-media-gold-mine-scammers-2021> (дата обращения: 15.03.2025).
16. *Хармаев Ю. В.* К вопросу об особенностях преступности несовершеннолетних в Монголии на современном этапе // Конституционные основы противодействия преступности в России: к 30-летию Конституции Российской Федерации : сборник статей по материалам Всероссийской (национальной) научно-практической конференции. — Ставрополь, 2024. — С. 139—144.

Уголовно-правовое регулирование незаконного привлечения средств через ICO на основе технологий блокчейн

Аннотация. ICO представляет собой механизм выпуска и предложения инвесторам токенов, который может быть классифицирован на три основные категории: краудфандинговые ICO, доходные ICO и ICO, соответствующие характеристикам ценных бумаг. Большинство ICO-проектов относятся к категории продуктивного краудфандинга. Доходные ICO делятся на два типа: обеспеченные реальными активами и необеспеченные реальными активами. Токены с характеристиками ценных бумаг могут быть признаны как выпуск акций или инвестирование в фонды в зависимости от их характеристик. Будучи носителем и прикладным продуктом технологии блокчейн, ICO предоставляют современному бизнесу возможность радикально трансформировать экономическую модель, однако также порождают множество новых форм незаконной и даже преступной деятельности. В связи с этим представляется целесообразным осуществить комплексный анализ теоретических основ и норм национального уголовного законодательства с целью обеспечения правовой регламентации в отношении незаконных ICO. Основанные на обмане схемы ICO следует квалифицировать как мошенничество (ст. 266 УК КНР). В частности, многоуровневый маркетинг, направленный на получение токенов, может быть расценен как организация и руководство финансовой пирамидой (ст. 224.1 УК КНР). Противоправные действия, связанные с недефицитными формами ICO, могут быть отнесены к категории незаконной хозяйственной деятельности (ст. 225 УК КНР).
Ключевые слова: ICO, блокчейн-технология, мошенничество, организация и руководство финансовой пирамидой, незаконная хозяйственная деятельность



Пан Дунмэй,
профессор
Юридического института
Хэйлунцзянского
университета,
доктор юридических наук
pangdongmei71@163.com
150080, КНР, г. Харбин,
ул. Сюэфу, д. 74

DOI: 10.17803/2311-5998.2025.129.5.169-180

Pang Dongmei,

Professor, Law Institute

Heilongjiang University,

Dr. Sci. (Law)

pangdongmei71@163.com

74, Xuefu Road, Harbin, China, 150080

Criminal Law Regulation of Illegal Funds Raising through ICO Based on Blockchain Technology

Abstract. *ICO is a mechanism for issuing and offering tokens to investors, which can be classified into three main categories: crowdfunding ICOs, profitable ICOs, and ICOs that meet the characteristics of securities. Most ICO projects fall into the category of productive crowdfunding. Profitable ICOs are divided into two types: those backed by real assets and those that are not backed by real assets. Tokens with the characteristics of securities can be recognized as issuing shares or investing in funds, depending on their characteristics. As a carrier and application of blockchain technology, ICOs provide modern businesses with the opportunity to radically transform their economic models, but they also give rise to many new forms of illegal and even criminal activity. In this regard, it seems expedient to carry out a comprehensive analysis of the theoretical foundations and norms of national criminal legislation in order to ensure legal regulation of illegal ICOs. Deceptive ICO schemes should be classified as fraud (Article 266 of the Criminal Code of the People's Republic of China). In particular, multi-level marketing aimed at obtaining tokens may be considered as the organization and management of a financial pyramid (Article 224.1 of the Criminal Code of the People's Republic of China); Unlawful actions related to non-deficit forms of ICO may be classified as illegal economic activities (Article 225 of the Criminal Code of the People's Republic of China).*

Keywords: *ICO, blockchain technology, fraud, organization and management of a financial pyramid, illegal economic activities*

Введение

ICO (Initial Coin Offering) — это термин, не имеющий строгого юридического определения. Поскольку на втором и третьем этапах привлечения инвестиций в рамках некоторых проектов также используется понятие ICO, более точным определением данного явления следует считать выпуск токенов и привлечение средств с использованием технологии блокчейн. Данная модель является как носителем, так и прикладным продуктом блокчейн-технологий¹. С развитием финансовых инструментов онлайн появилась новая парадигма выпуска токенов и привлечения

¹ Цзян Хуэйюй. Проблемы привлечения капитала через ICO: анализ путей уголовно-правового регулирования незаконного сбора средств в Китае и соответствующих стратегических решений // Теория и практика финансов и экономики. 2019. № 2. С. 12.

финансирования. Данная система предоставляет современным предприятиям возможность радикально трансформировать экономическую модель, но она также стала источником множества новых форм незаконной и преступной деятельности, что оказывает влияние на стабильность рыночной экономики и другие аспекты хозяйственной деятельности. В настоящее время уголовно-правовая система Китая не способна полностью соответствовать возрастающим потребностям динамично развивающегося рынка цифровых технологий.

1. Признаки ICO и классификация ICO-проектов

ICO — это проектное финансирование, в котором используется цифровая валюта, генерируемая на основе технологии блокчейн². Основной целью ICO является выпуск цифровых токенов, а средства собираются преимущественно в виде основных виртуальных валют, таких как биткоин, которыми владеет широкая группа инвесторов. Технология блокчейн, лежащая в основе ICO, представляет собой систему распределенных реестров, основанную на интернет-инфраструктуре. Она обеспечивает доверие между участниками торговых операций благодаря децентрализованному хранению данных, коллективному ведению зашифрованных реестров и характеризуется такими свойствами, как децентрализация, открытость, анонимность и высокий уровень безопасности³.

Опираясь на технологию блокчейн, инициаторы ICO-проектов имеют возможность привлекать капитал от неограниченного круга инвесторов, после чего использовать собранные средства для реализации запланированных целей проекта. В целом ICO можно классифицировать на три основные категории: продукт-ориентированные краудфандинговые проекты, проекты ICO, предполагающие генерацию дохода для инвесторов, а также проекты, соответствующие характеристикам эмиссии ценных бумаг⁴.

1. Краудфандинговые проекты на основе продуктов, такие как Ether, Bitshares, Augur и Lisk, представляют собой модель сбора средств, при которой продукты или услуги используются для возмещения инвестиций.

С точки зрения законодательства краудфандинг на основе продуктов часто рассматривается как форма предварительной продажи товаров. Данная модель получила широкое распространение в китайской практике и обычно рассматривается как предварительная продажа продуктов⁵. При этом доходность от продуктов или услуг, предлагаемых через краудфандинг, ориентирована преимущественно на конечных пользователей, что ограничивает ликвидность данных активов. Хотя вторичные транзакции возможны, их масштаб остается относительно небольшим.

² Дэн Цзяньпэн. Юридическое мышление по вопросу незаконного привлечения средств на ICO // Цзинань. Философия и общественные науки. 2018. № 8. С. 41.

³ Ян Хуэйцин, Сунь Лэй, Чжао Сичао. Создание информационной платформы для взаимного доверия и бесприигрышной цепочки поставок, основанной на технологии блокчейн // Научно-технический прогресс и политика. 2018. № 5. С. 22.

⁴ Сюй Минь. Виды финансирования и их уголовно-правовая оценка // Журнал Цзянсийской полицейской академии. 2020. № 1. С. 26.

⁵ Чжан Минь. О контрактно-правовом регулировании краудфандингового издания // Китайский издательский журнал. 2015. № 16. С. 68.



В отличие от традиционного краудфандинга, виртуальные валюты обладают высокой ликвидностью и относятся к категории рискованных финансовых инструментов. Следовательно, вопрос об определении правовой природы виртуальных валют — как обычных товаров или финансовых продуктов — требует дальнейшего уточнения со стороны регулирующих органов Китая.

2. Доходные ICO. Данный род ICO можно классифицировать на два типа: токены, эмитированные с подтверждением реальных активов, и токены, не обеспеченные реальными активами.

Основная характеристика необеспеченных реальными активами ICO-проектов заключается в том, что токены, полученные через краудфандинг, генерируют доход в виде криптовалюты согласно алгоритмическим правилам системы. Примером такого типа является проект NEO (ранее известный как AntShares)⁶. Доход инвесторов от краудфандинга в данном проекте представлен токенами NEO, которые фактически являются долей в капитале сети NEO. Владельцы NEO, согласно алгоритму системы, при создании новых блоков получают GAS пропорционально своим долям. Оба токена, NEO и GAS, используются для взаимодействия с системой. При этом NEO представляет собой долю в проекте, аналогичную акциям компании, а GAS выступает в роли платежного средства для использования функций платформы⁷. Ключевое отличие между ними заключается в том, что NEO предоставляет право на получение дивидендов.

Что касается обеспеченных реальными активами ICO-проектов, то такая валюта фактически представляет собой электронный сертификат, подкрепленный реальными активами. Доходность таких проектов напрямую связана с доходами от управления этими активами.

3. ICO-проекты, аналогичные выпуску ценных бумаг, классифицируются как предложения акций или инвестиционных фондов с учетом их структурных особенностей и правовой природы. Приведем в качестве примера ICO-проекты, связанные с токенами Lykke. Эмитентом данных токенов является компания Lykke AG, зарегистрированная в Швейцарии. Согласно условиям обмена, за каждые 100 токенов Lykke инвестор получает одну долю в капитале компании⁸.

Что касается ICO, структурированных как инвестиционные фонды, то их ключевые характеристики следующие: во-первых, основной целью является привлечение средств для инвестиций, а не выполнение конкретных работ; во-вторых, выпущенные токены могут выступать в качестве сертификатов на определенную долю капитала; в-третьих, данные доли подлежат свободной продаже на вторичном рынке, а также могут быть выкуплены эмитентом в рамках предусмотренных условий. Примеров такого типа ICO сравнительно немного. Одним из наиболее известных проектов данного формата был The DAO. В рамках этого проекта, который ранее считался крупнейшим ICO в США, организаторы собирали средства

⁶ NEO // URL: https://baike.baidu.com/item/%E5%B0%8F%E8%9A%81%E5%B8%81/22415322?fromModule=search-result_lemma (дата обращения: 19.06.2025).

⁷ Белая книга NEO // URL: <https://zhuanlan.zhihu.com/p/52691873> (дата обращения: 19.06.2025).

⁸ Цзян Бо. Исследование по судебной защите виртуальной собственности. Пекин : Издательство Пекинского университета. 2015. С. 31—33.

в виде криптовалюты Ethereum и осуществляли инвестиции через алгоритмизированные механизмы управления. Токены проекта выполняли функцию ваучеров, подтверждающих право участников на инвестиции и будущие дивиденды⁹.

Особенности модели ICO, такие как низкий порог и высокая эффективность, сделали ICO самым популярным методом финансирования на сегодняшний день¹⁰. Однако следует отметить, что действующая правовая система Китая пока не определила четкий правовой статус виртуальных токенов (или цифровых валют). Сочетание отсутствия отраслевых нормативов, ограничений доступа на рынок и недостаточности систем надзора и аудита делает деятельность в сфере ICO сопряженной с существенными социальными рисками и потенциально криминальными последствиями. При этом возможности инвесторов по защите своих прав и интересов остаются крайне ограниченными. В случае неудачи проекта или возникновения юридических и политических рисков инвесторы вынуждены самостоятельно нести все связанные с этим последствия¹¹.

2. Криминальные риски, сопутствующие проведению ICO

Основной особенностью проведения ICO являются использование виртуальных криптовалют вместо фиатных валют для публичного сбора капитала, и выпуск новых виртуальных валют в качестве вознаграждения для инвесторов. В последнее время ICO все чаще становятся эффективным инструментом для онлайн-финансирования проектов. В первой половине 2017 г. Национальный комитет технических экспертов по финансовой безопасности в Интернете Китая опубликовал Отчет о развитии ICO в Китае за первую половину 2017 года¹². Согласно Отчету, в Китае функционировали 43 платформы, осуществляющие проведение ICO, и было запущено и завершено 65 проектов. Общий объем привлеченного финансирования составил 63 523,64 BTC (Bitcoin), 852 753,36 ETH (Ethereum), а также другие виртуальные валюты, что эквивалентно 2,616 млрд юаней при конвертации по курсу на нулевой час 19 июля 2017 г. Общее количество участников составило 105 000 человек¹³.

Следует отметить, что проведение ICO сопряжено с рядом потенциальных рисков, таких как финансовые риски из-за высокой волатильности цен, риск потери капитала вследствие неудачи проекта или бегства спонсоров проекта, а также

⁹ Сюй Минь. Виды финансирования и их уголовно-правовая оценка // Журнал Цзянсийской полицейской академии. 2020. № 1. С. 26.

¹⁰ Фань Цзячэнь. Исследование бизнес-модели краудфандинга // Экономика предприятия. 2013. № 8. С. 72—75.

¹¹ Цзинь Лу, Хуан Чжихуа. Анализ рисков и уголовно-правовое регулирование проведения ICO на основе технологии блокчейн // Труды Пекинского технологического института. Общественные науки. 2020. № 6. С. 123.

¹² Отчет о развитии ICO в Китае за первую половину 2017 года // URL: <https://www.528btc.com/blocknews/40869.html> (дата обращения: 19.06.2025).

¹³ Ван Линь, Нин Ди, Чжан Цзюнь. Проблема регулирования виртуальных валют после запрета ICO остается нерешенной // Китайская молодежная ежедневная газета. 12 сентября 2017 г. 10-е изд.



правовые риски, связанные с незаконным сбором средств, финансовыми пирамидами, мошенничеством и другими противозаконными действиями¹⁴.

С точки зрения эмитентов ICO-проектов, инвесторов и рынка в целом, существуют как криминальные, так и рыночные риски. Во-первых, с позиции эмитента, проведение ICO может быть связано с незаконным публичным размещением ценных бумаг, а также подразумевать криминальные риски, такие как отмывание денег, незаконное привлечение депозитов населения и осуществление противоправных коммерческих операций. Во-вторых, для инвесторов участие в ICO сопряжено с рисками мошенничества и инсайдерской торговли. В-третьих, распространение спекулятивной краткосрочной торговли, хакерские атаки и высокая волатильность цифровых валют представляют собой основные рыночные риски для ICO, которые могут привести к значительным и часто необратимым потерям со стороны инвесторов, а также способствовать развитию спекулятивного поведения на рынке. Следовательно, деятельность, связанная с ICO, характеризуется как значительными рыночными рисками, так и серьезными уголовно-правовыми последствиями.

Принимая во внимание вышеизложенную ситуацию, 4 сентября 2017 г. «один банк, три комиссии» совместно с семью министерствами опубликовали документ под названием «Объявление о предотвращении рисков финансирования выпуска токенов» (далее — «Объявление...»)¹⁵, в котором проведение ICO было квалифицировано как форма несанкционированного и незаконного публичного финансирования. В соответствии с данным Объявлением, все проекты ICO были немедленно приостановлены, а указанная финансовая деятельность полностью запрещена. Тем не менее, учитывая характер ICO как развивающейся и эффективной инновационной модели интернет-финансирования, полный и постоянный запрет на эту деятельность представляется малореалистичным. В условиях действующего нормативно-правового регулирования существует вероятность перемещения ICO в теневой сектор или реализация за пределами страны для обхода регуляторных ограничений¹⁶. Можно предположить, что текущая приостановка деятельности ICO не приведет к ее прекращению. В противном случае могут увеличиться случаи незаконной и преступной деятельности в этой сфере.

3. Квалификация действий в форме незаконного привлечения средств, связанного с ICO

В «Объявлении...» 2017 г. также указывалось, что ICO-проекты могут быть связаны с различными правонарушениями и такими преступными деяниями, как незаконное обращение ценных бумаг и финансовое мошенничество, несанкционированный сбор средств у населения, деятельность финансовых пирамид

¹⁴ Чэнь Ланьлань, Цзо Лимин. Анализ характеристик экономических преступлений, связанных с ICO, и их регулирование // Журнал Хунаньской полицейской академии. 2019. № 3. С. 79.

¹⁵ Объявление Народного банка Китая и других семи ведомств о предотвращении финансовых рисков, связанных с выпуском токенов // URL: https://www.gov.cn/xinwen/2017-09/04/content_5222657.htm (дата обращения: 19.06.2025).

¹⁶ Ван Гуань. Уголовно-правовое регулирование проведения ICO на основе технологий блокчейн // Восточное право. 2019. № 3. С. 138.

и т.д. Согласно статистическим данным некоторых исследователей¹⁷, среди 526 судебных решений по уголовным делам, связанным с ICO, доля преступлений, касающихся несанкционированной эмиссии акций (ст. 179 УК КНР)¹⁸, составила 5,58 %, преступлений, связанных с незаконным привлечением средств населения (ст. 176 УК КНР)¹⁹, — 7,92 %, случаев мошенничества (ст. 266 УК КНР)²⁰ — 29,06 %, а доля преступлений, связанных с организацией и руководством финансовой пирамидой (ст. 224.1 УК КНР), достигла 56,98 %²¹.

Следует отметить, что существуют различные теоретические подходы к оценке уголовно-правовой характеристики действий, связанных с ICO, в современном Китае.

Профессор Дэн Цзяньпэн полагает, что в рамках судебной практики Китая противоправные действия, связанные с ICO, могут быть квалифицированы как преступления, связанные с незаконным привлечением капитала²².

Профессор Цзинь Лу подчеркнул, что квалификация всех действий, связанных с ICO, как преступления в виде незаконного привлечения капитала противоречит принципу законности. В связи с этим он предлагает применять дифференцированный подход для квалификации указанных действий²³. Так, проведение ICO с целью незаконного завладения средствами общественности мошенническим путем может быть квалифицировано как мошенничество с привлечением капитала (ст. 192 УК КНР)²⁴; деятельность ICO, связанная с привлечением депозитов или средств с обещанием выплаты основной суммы долга и процентов, может быть рассмотрена как незаконное привлечение средств населения (ст. 176 УК

¹⁷ Ли Сян. Недоразумения в сфере уголовно-правового регулирования проведения ICO и пути их устранения // Журнал Юньчэнского университета. 2022. № 2. С. 67.

¹⁸ Несанкционированная эмиссия акций, корпоративных облигаций // url: <https://baike.baidu.com/item/%e6%93%85%e8%87%aa%e5%8f%91%e8%a1%8c%e8%82%a1%e7%a5%a8%e3%80%81%e5%85%ac%e5%8f%b8%e3%80%81%e4%bc%81%e4%b8%9a%e5%80%ba%e5%88%b8%e7%bd%aa/657549> (дата обращения: 20.06.2025).

¹⁹ Незаконное привлечение средств населения // URL: https://baike.baidu.com/item/%e9%9d%9e%e6%b3%95%e5%90%b8%e6%94%b6%e5%85%ac%e4%bc%97%e5%ad%98%e6%ac%be%e7%bd%aa?frommodule=lemma_search-box (дата обращения: 20.06.2025).

²⁰ Мошенничество // URL: https://baike.baidu.com/item/%e8%af%88%e9%aa%97%e7%bd%aa?frommodule=lemma_search-box (дата обращения: 20.06.2025).

²¹ Организация и руководство деятельностью MLM // URL: https://baike.baidu.com/item/%e7%bb%84%e7%bb%87%e3%80%81%e9%a2%86%e5%af%bc%e4%bc%a0%e9%94%80%e6%b4%bb%e5%8a%a8%e7%bd%aa/4276174?frommodule=search-result_lemma (дата обращения: 20.06.2025).

²² Дэн Цзяньпэн. Юридическое мышление по вопросу незаконного привлечения средств на ICO // Цзинань. Философия и общественные науки. 2018. № 8. С. 40.

²³ Цзинь Лу, Хуан Чжихуа. Анализ рисков и уголовно-правовое регулирование проведения ICO на основе технологии блокчейн // Труды Пекинского технологического института. Общественные науки. 2020. № 6. С. 123—129.

²⁴ Мошенничество с привлечением средств // URL: https://baike.baidu.com/item/%e9%9b%86%e8%b5%84%e8%af%88%e9%aa%97%e7%bd%aa?frommodule=lemma_search-box (дата обращения: 20.06.2025).



КНР); деяние, основанное на модели «привлечения новых участников» и «взимания вступительных взносов», характеризуется как организация и руководство финансовой пирамидой (ст. 224.1 УК КНР).

Профессор Ван Гуань утверждает, что цифровые валюты не являются объектом незаконного сбора средств и деятельность ICO не относится к операциям с ценными бумагами. Следовательно, такие действия не могут быть квалифицированы как преступления незаконного сбора средств или незаконной операции с ценными бумагами²⁵.

Представляется, что теоретически единая позиция относительно уголовно-правовой характеристики действий, связанных с ICO, в Китае пока не сформирована.

Автор подчеркивает позицию о том, что ICO-проекты не соответствуют критериям, необходимым для классификации как незаконное привлечение средств или незаконное обращение с ценными бумагами. Следовательно, противоправные деяния в сфере данных проектов не могут быть отнесены к категории соответствующих преступлений²⁶.

Во-первых, денежные средства являются необходимым условием для совершения преступлений, связанных с незаконным привлечением капитала в Китае. Однако виртуальная валюта в качестве предмета ICO по привлечению средств не может быть обязательным признаком данных преступлений²⁷. Более того, в «Объявлении...» 2017 г. было подчеркнуто, что виртуальная валюта лишена таких атрибутов традиционной валюты, как законность обращения и возможность использования в качестве платежного средства, и не обладает юридическим статусом официального платежного инструмента. В Китае виртуальная валюта классифицируется как особый вид виртуальной собственности. Поскольку государство не наделило виртуальную валюту статусом легального платежного средства, сбор виртуальных валют у населения не может быть квалифицирован как преступления, связанные с незаконным привлечением капитала.

Во-вторых, правовым благом, подлежащим защите от преступлений, таких как незаконное привлечение средств населения (ст. 176 УК КНР) и мошенничество с привлечением капитала (ст. 192 УК КНР), признается финансовая система. Однако нарушение финансового порядка возможно только в случае, если указанные противоправные действия направлены на легальные платежные инструменты. Незаконный сбор имущества (включая виртуальные валюты) даже при значительном объеме и масштабах операций не может напрямую повлиять на стабильность финансовой системы. Следовательно, в рамках ICO-проектов виртуальные валюты не могут рассматриваться как преступный объект незаконного

²⁵ Ван Гуань. Уголовно-правовое регулирование проведения ICO на основе технологий блокчейн // Восточное право. 2019. № 3. С. 137—148.

²⁶ Дин Юй. Дилемма уголовно-правового регулирования незаконного привлечения средств через ICO и пути ее решения // Современные финансы. 2023. № 8. С. 25.

²⁷ Лю Вэйбо. Понимание и применение «Разъяснения некоторых вопросов, касающихся конкретного применения закона при рассмотрении уголовных дел о незаконном сборе средств» // Народное правосудие. 2011. № 5. С. 24—31.

привлечения средств²⁸. Иными словами, незаконный сбор виртуальных валют, таких как биткоин, не подпадает под квалификацию как преступления, предусмотренные ст. 176 и 192 УК КНР.

В-третьих, внешние характеристики токенов, предлагаемых в рамках ICO, демонстрируют значительное сходство с характеристиками ценных бумаг. На основе этого факта некоторые исследователи подчеркивают, что такие токены обладают функцией свободной передачи и проявляют имущественные, инвестиционные и ликвидные свойства. Это позволяет участникам получить права, аналогичные правам акционеров, включая получение дивидендов и участие в распределении прибыли компании.

Следовательно, токены могут быть классифицированы как ценные бумаги²⁹. Кроме того, существует точка зрения, согласно которой выпуск виртуальных валют, которые могут использоваться в качестве сертификатов акций, следует рассматривать как эмиссию акций. Если по истечении определенного периода времени эти токены накапливаются в установленном объеме или обмениваются на сертификаты акций, это может быть квалифицировано как скрытая эмиссия акций³⁰. Вместе с тем в «Объявлении...» 2017 г. было указано, что некоторые противоправные действия в сфере ICO могут быть квалифицированы как преступления в виде незаконной эмиссии ценных бумаг.

Вышеуказанные точки зрения прямо или косвенно классифицируют виртуальные валюты в ICO-проектах как ценные бумаги. Данное обстоятельство предполагает, что мошенническое размещение или несанкционированная эмиссия виртуальных валют может рассматриваться как деяние, соответствующее составу преступления, связанного с мошеннической эмиссией ценных бумаг (ст. 160 УК РФ)³¹, либо как преступление, связанное с несанкционированной эмиссией акций, корпоративных облигаций (ст. 179 УК РФ).

Позиция автора состоит в том, что виртуальные валюты, эмитируемые через механизм ICO, не могут быть отнесены к категории юридически признанных ценных бумаг, так что противоправные действия в данной сфере не могут быть квалифицированы как преступления против эмиссии ценных бумаг в соответствии с УК КНР.

Основные доводы заключаются в том, что в рамках существующей правовой системы Китая отсутствует нормативная база для классификации виртуальных

²⁸ Ке Да. Уголовно-правовое регулирование незаконного сбора средств с использованием цифровых валют на основе технологии блокчейн // Журнал Северо-Восточного университета. Общественные науки. 2020. № 6. С. 23—29.

²⁹ Сунь Гофэн, Чэнь Ши. Об атрибутах цифровых ценных бумаг в рамках ICO и их правовых аспектах регулирования // Мир управления. 2019. № 12. С. 47—49.

³⁰ Сюй Минь. Виды финансирования и их уголовно-правовая оценка // Журнал Цзянсийской полицейской академии. 2020. № 1. С. 28.

³¹ Мошенническая эмиссия ценных бумаг // URL: https://baike.baidu.com/item/%e6%ac%ba%e8%af%88%e5%8f%91%e8%a1%8c%e8%af%81%e5%88%b8%e7%bd%aa?frommodule=lemma_search-box (дата обращения: 20.06.2025).



валют как ценных бумаг. Согласно ст. 2 Закона КНР о ценных бумагах³², помимо акций, корпоративных облигаций и депозитарных расписок, к категории ценных бумаг могут быть отнесены и «другие виды ценных бумаг», утвержденные Государственным советом в установленном порядке. Однако на текущий момент Государственный совет не включал никаких дополнительных предметов в перечень указанных ценных бумаг.

В этой связи, несмотря на наличие у виртуальных валют определенных признаков, характерных для ценных бумаг, в судебной практике ICO не следует рассматривать как выпуск ценных бумаг³³. Иными словами, незаконное обращение виртуальных валют (ICO) не может быть квалифицировано как преступления, предусмотренные ст. 160 и 179 УК КНР.

Заключение

Китайское уголовное законодательство не содержит прямого определения юридической квалификации деятельности, связанной с ICO. Неправомерные действия в данной сфере подпадают под составы преступлений УК КНР, связанные с незаконным сбором средств и незаконной эмиссией ценных бумаг, исключительно на основании положений «Объявления...» министерств и комиссий, принятого в 2017 г.

Автор не согласен с этой официальной позицией и считает, что преступления в данной сфере должны подлежать классифицированному уголовно-правовому регулированию в зависимости от того, используют ли инициаторы ICO-проектов средства, полученные обманным путем. Инициаторы проектов ICO часто используют средства, полученные различными обманными путями для привлечения цифровых валют населения. Однако в реальном мире также существуют ICO без использования полученных подобным образом средств.

Деятельность, связанная с проведением ICO при использовании основанных на обмане методов, может быть квалифицирована как организация и руководство финансовой пирамидой (ст. 224.1 УК КНР) либо как мошенничество (ст. 266 УК КНР). В частности, мошеннические действия в рамках ICO, такие как привлечение новых участников путем взимания членских взносов, классифицируются как создание и управление финансовыми пирамидами. Если эмитент ICO намеренно осуществляет сбор цифровых токенов обманным путем, не имея объективно осуществимого проекта, данное деяние рассматривается как уголовно наказуемое мошенничество.

Проведение ICO без применения основанных на обмане методов может быть квалифицировано как незаконная хозяйственная деятельность по ст. 225 УК КНР³⁴. Согласно данной статье, противоправные действия, связанные с незаконным ведением хозяйственной деятельности, включают такие операции, как

³² Закон Китайской Народной Республики о ценных бумагах // URL: https://www.gov.cn/xinwen/2019-12/29/content_5464866.htm (дата обращения: 20.06.2025).

³³ Ли Сян. Уголовно-правовое регулирование проведения ICO в рамках технологий блокчейн // Журнал Цзянсиской полицейской академии. 2022. № 1. С. 89—90.

³⁴ Гао Минсюань. Зарождение, становление и развитие, совершенствование уголовного законодательства в Китайской Народной Республике : монография / под науч. ред.

привлечение средств через выпуск акций фонда без соответствующего законного разрешения, осуществление валютных операций вне установленных государством биржевых площадок и ведение бизнеса с ценными бумагами, фьючерсами или страхованием без одобрения компетентных органов регулирования. Все указанные виды деятельности имеют значительное сходство с операциями по проведению ICO.

В случае если деятельность, связанная с ICO, существенно нарушает порядок управления рыночными транзакциями и причиняет серьезный ущерб законным интересам участников рынка, такая деятельность должна быть отнесена к категории преступных деяний, предусмотренных ст. 225 УК КНР.

БИБЛИОГРАФИЯ

1. Ван Гуань. Уголовно-правовое регулирование проведения ICO на основе технологий блокчейн // Восточное право. — 2019. — № 3.
2. Ван Линь, Нин Ди, Чжан Цзюньи. Проблема регулирования виртуальных валют после запрета ICO остается нерешенной // Китайская молодежная ежедневная газета. — 12 сентября 2017 г. — 10-е изд.
3. Гао Минсюань. Зарождение, становление и развитие, совершенствование уголовного законодательства в Китайской Народной Республике : монография / под науч. ред. Н. А. Сидоровой, И. А. Васильева ; пер. Пан Дунмэй, Ван Гуанлуна. — М. : Проспект, 2021.
4. Дин Юй. Дилемма уголовно-правового регулирования незаконного привлечения средств через ICO и пути ее решения ; Современные финансы. — 2023. — № 8.
5. Дэн Цзяньпэн. Юридическое мышление по вопросу незаконного привлечения средств на ICO // Цзинань. — Философия и общественные науки. — 2018. — № 8.
6. Ке Да. Уголовно-правовое регулирование незаконного сбора средств с использованием цифровых валют на основе технологии блокчейн // Журнал Северо-Восточного университета. — Общественные науки. — 2020. — № 6.
7. Ли Сян. Недоразумения в сфере уголовно-правового регулирования проведения ICO и пути их устранения // Журнал Юньчэнского университета. — 2022. — № 2.
8. Ли Сян. Уголовно-правовое регулирование проведения ICO в рамках технологий блокчейн // Журнал Цзянсиской полицейской академии. — 2022. — № 1.
9. Лю Вэйбо. Понимание и применение «Разъяснения некоторых вопросов, касающихся конкретного применения закона при рассмотрении уголовных дел о незаконном сборе средств» // Народное правосудие. — 2011. — № 5.
10. Сунь Гофэн, Чэнь Ши. Об атрибутах цифровых ценных бумаг в рамках ICO и их правовых аспектах регулирования // Мир управления. — 2019. — № 12.

Н. А. Сидоровой, И. А. Васильева ; пер. Пан Дунмэй, Ван Гуанлуна. М. : Проспект, 2021. С. 349—351.



11. Сюй Минь. Виды финансирования и их уголовно-правовая оценка // Журнал Цзянсиской полицейской академии. — 2020. — № 1.
12. Фань Цзячэнь. Исследование бизнес-модели краудфандинга // Экономика предприятия. — 2013. — № 8.
13. Цзинь Лу, Хуан Чжихуа. Анализ рисков и уголовно-правовое регулирование проведения ICO на основе технологии блокчейн // Труды Пекинского технологического института. — Общественные науки. — 2020. — № 6.
14. Цзян Бо. Исследование по судебной защите виртуальной собственности. — Пекин : Издательство Пекинского университета, 2015.
15. Цзян Хуэйюй. Проблемы привлечения капитала через ICO: анализ путей уголовно-правового регулирования незаконного сбора средств в Китае и соответствующих стратегических решений // Теория и практика финансов и экономики. — 2019. — № 2.
16. Чжан Минь. О контрактно-правовом регулировании краудфандингового издания // Китайский издательский журнал. — 2015. — № 16.
17. Чэнь Ланьлань, Цзо Лимин. Анализ характеристик экономических преступлений, связанных с ICO, и их регулирование // Журнал Хунаньской полицейской академии. — 2019. — № 3.
18. Ян Хуэйцин, Сунь Лэй, Чжао Сичао. Создание информационной платформы для взаимного доверия и бесприигрышной цепочки поставок, основанной на технологии блокчейн // Научно-технический прогресс и политика. — 2018. — № 5.

Криминологическое противодействие киберпреступлениям

Проблемы предупреждения преступлений, совершаемых посредством информационных технологий работниками банков

Аннотация. Статья посвящена анализу проблем предупреждения преступлений, совершаемых посредством информационных технологий работниками банков. Актуальность исследования определяется тем, что в последние годы фиксируется рост рассматриваемых преступлений, а также рост ущерба в результате их совершения, который причиняется не только банку, но и его клиентам. Банки несут также и репутационные риски. Сделан вывод о том, что первостепенное значение имеют применение превентивных мер непосредственно в банках, а также поиск новых форм предупреждения рассматриваемых преступлений. В качестве таких мер выделены: оптимизация деятельности подразделений службы безопасности банков; создание новых компьютерных программ, позволяющих всесторонне контролировать деятельность работников банков, совершенствование форм взаимодействия банков с правоохранительными органами. Результаты работы могут быть использованы в дальнейших научных исследованиях рассматриваемой проблемы, а также для разработки практических рекомендаций, применяемых в деятельности по предупреждению преступлений, совершаемых посредством информационных технологий работниками банков.

Ключевые слова: преступление, информационные технологии, преступное поведение, предупреждение преступлений, работники банков, правоохранительные органы



**Елена Николаевна
КЛЕЩИНА,**
профессор кафедры
криминологии
и уголовно-
исполнительного права
имени В. Е. Эминова
Университета имени
О.Е. Кутафина (МГЮА),
доктор юридических наук,
профессор
enkleschina@msal.ru
125993, Россия, г. Москва,
ул. Садовая-Кудринская,
д. 9

DOI: 10.17803/2311-5998.2025.129.5.181-188

Elena N. KLESCHINA,

*Professor of the Chair of Criminology and Executive Law Chair named after
E. V. Eminov of the Kutafin Moscow State Law University (MSAL),*

Dr. Sci. (Law), Associate Professor

enkleschina@msal.ru

9, ul. Sadovaya-Kudrinskaya, Moscow, Russia, 125993

Problems of Preventing Crimes Committed by Bank Employees Using Information Technology

Abstract. *The article is devoted to the analysis of the problems of preventing crimes committed through information technology by bank employees. The relevance of the study is determined by the fact that in recent years there has been an increase in the crimes under consideration, as well as the damage caused not only to the bank, but also to its customers. Banks also carry reputational risks. It is concluded that the application of preventive measures directly in banks, as well as the search for new forms of prevention of the crimes under consideration, is of paramount importance. Such measures include: optimization of the activities of the bank's security service units; creation of new computer programs that allow comprehensive monitoring of the activities of bank employees, and improvement of banks' interaction with law enforcement agencies. The results of the work can be used in further scientific research of the problem under consideration, as well as for the development of practical recommendations used in the prevention of crimes committed through information technology by bank employees.*

Keywords: *crime, information technology, criminal behavior, crime prevention, bank employees, law enforcement agencies*

Число преступлений, совершаемых посредством информационных технологий, в последние годы возрастает, растет и ущерб в результате их совершения.

Так, по данным ГИАЦ МВД России, в 2024 г. всего зарегистрировано 1 911,3 тыс. преступлений. Из них количество преступлений с использованием информационно-коммуникационных технологий составляет 765,4 тыс., что на 13,1 % больше, чем за аналогичный период 2023 г. В общем числе зарегистрированных преступлений их удельный вес увеличился с 34,8 % в январе — декабре 2023 г. до 40,0 %. Четыре преступления из пяти (84,8 %) совершаются с использованием сети Интернет (649,1 тыс.; +23,2 %), почти половина (45,2 %) — с использованием средств мобильной связи (346,0 тыс.; +14,3 %)¹.

На тенденцию роста преступлений, совершенных с использованием информационно-телекоммуникационных технологий, обращает внимание Президент Российской Федерации В. В. Путин, подчеркивая необходимость совершенствования

¹ Состояние преступности в России за 2024 год / ГИАЦ МВД России // URL: https://docs.yandex.ru/docs/view?tm=1751012961&tld=ru&lang=ru&name=Sbornik_UOS_2024.pdf&text.

методов борьбы с преступностью в этой сфере, взаимодействия МВД России с профильными ведомствами².

Распространенными являются преступления, совершаемые посредством информационных технологий работниками банков, в том числе такие, как мошенничество в сфере компьютерной информации, неправомерный доступ к компьютерной информации, незаконное использование и (или) передача, сбор и (или) хранение компьютерной информации, содержащей персональные данные, а равно создание и (или) обеспечение функционирования информационных ресурсов, предназначенных для ее незаконных хранения и (или) распространения.

Председатель правления ПАО «Сбербанк» Г. Греф еще в 2019 г. подчеркивал, что «самая большая проблема в киберрисках — это не внешние риски, а внутренние», однако бывают также ситуации, «когда мошенники снаружи и внутри договариваются»³.

С. Кузнецов, являющийся заместителем председателя правления ПАО «Сбербанк», указал на то, что «банку удается защитить своих клиентов от атак мошенников в 97 % случаев. Но, сосредоточившись на внешней угрозе, Сбербанк не заметил ее изнутри»⁴.

С учетом отмеченного, важнейшее значение имеет оптимизация мер предупреждения преступлений, совершаемых посредством информационных технологий работниками банков, поскольку ущерб от таких преступлений причиняется не только банку, но и его клиентам. Банки несут также и репутационные риски.

Приведем примеры судебной практики, в которых очевиден процесс совершения преступлений работниками банка.

Так, приговором Батайского городского суда Ростовской области от 20.06.2024 № 1-111/2024 установлено, что у С., которая являлась старшим менеджером группы продаж частным клиентам отделения регионального управления ПАО «Мин-Банк», возник умысел на хищение денежных средств клиентов банка с использованием своего служебного положения. С. после устройства на работу в банк был выдан логин. Используя логин, путем введения известного лишь ей пароля, она имела право доступа к электронной системе. Реализуя свой преступный умысел, С. совершала вмешательство в функционирование средств хранения и обработки компьютерной информации, похищая денежные средства клиентов банка. По результатам рассмотрения уголовного дела действия С. были квалифицированы судом по ч. 4 ст. 159⁶ и по ч. 3 ст. 272 УК РФ.

Приговором Дзержинского районного суда г. Волгограда от 13.03.2023 № 1-33/2023 установлено, что подсудимый К. в 2019 г. был принят на работу в ООО «ХКФ Банк» на должность менеджера. В январе 2021 г. у К., который в этом банке уже являлся ведущим менеджером, возник преступный умысел,

² Президент Российской Федерации В. В. Путин выступил на Ежегодном расширенном заседании коллегии МВД России. 05.03.2025 // URL: <http://kremlin.ru/events/president/news/76408> (дата обращения: 06.03.2025).

³ Греф сообщил о случаях мошенничества с участием сотрудников Сбербанка // URL: <https://amp.rbc.ru/rbcnews/finances/19/05/2019/5ce14eed9a79473f540ecc5e>

⁴ Кузнецов С. О мошенничестве методом социальной инженерии, защите данных и проблемах кибербезопасности // Ведомости. 17.02.2020.



направленный на хищение чужого имущества, принадлежащего банку и его клиентам, путем ввода и модификации компьютерной информации. Зная о порядке удаленного оформления кредитных договоров в банке, имея доступ к базе данных клиентов, К. получил сведения о клиенте Ф., включая абонентский номер оператора сотовой связи ПАО «ВымпелКом», используемый для получения кодов посредством смс-сообщений, необходимых для удаленного подписания простой электронной подписью документов с банком и получения денежных средств в виде потребительского кредита. После этого он узнал от менеджера по прямым продажам ООО «Атон-Р», осуществляющего продажу сим-карт оператора сотовой связи ПАО «ВымпелКом», что данный абонентский номер находится в продаже. После этого К., зная, что абонентский номер Ф. не используется, приобрел в г. Волгограде у И., не осведомленного о его преступных намерениях, сим-карту оператора сотовой связи ПАО «ВымпелКом» с данным абонентским номером.

Затем К., действуя как ведущий менеджер банка, путем удаленного доступа, с использованием сети Интернет, посредством служебной программы банка сформировал от имени Ф. заявление о предоставлении потребительского кредита по карте и открытии текущего счета, без обращения Ф. в банк, т.е. произвел без согласия клиента банка ввод и модификацию компьютерной информации. Имея доступ к счету кредитной карты «Карта Кредитная Польза», он совершил хищение денежных средств с банковского счета в размере 94 919 руб. Аналогичными преступными действиями он оформил еще ряд потребительских кредитов на общую сумму 995 040 руб.

Преступные действия К. были раскрыты работниками отдела защиты бизнеса данного банка. Из показаний представителя этого отдела следует, что в банке действует система, в которой фиксируются все договоры, которые заключают сотрудники. Если по ним возможны какие-либо риски, то проводится проверка. Поступило большое количество дефолтных договоров, всего их было 41, по которым не осуществлялось погашение, заключенных именно К. в период с января по май. В ходе проверки было обнаружено, что договоры заключались онлайн, с телефонных номеров, принадлежащих клиентам банка, но телефонных разговоров с клиентами не было. При дальнейшей проверке было установлено, что часть денежных средств от этих кредитных договоров была переведена на счета К.

Из приведенных примеров судебной практики очевиден и процесс виктимизации банка и клиентов банка. Поэтому важнейшее значение имеет совершенствование мер предупреждения преступности в этой сфере.

В криминологии предупреждение преступности рассматривается как многоуровневая система государственных и общественных мер, направленных на выявление, устранение, ослабление или нейтрализацию причин и условий преступности, ее отдельных видов и конкретных деяний⁵, реализуемых разными субъектами⁶.

⁵ См., например: Криминология : учебник / под ред. Н. Ф. Кузнецовой, В. В. Лунеева. 2-е изд., перераб. и доп. М., 2004. С. 185 ; *Мацкевич И. М.* Причины экономической преступности : учебное пособие. М., 2019. С. 249.

⁶ Криминология : учебник / под ред. А. И. Долговой. 4-е изд., перераб. и доп. М., 2010. С. 484.

Сложный характер развития причинных связей требует разностороннего комплексного подхода к организации работы по предупреждению преступности⁷.

Как отмечал В. Н. Кудрявцев, в зависимости от типа причинно-следственных связей и характера условий преступности такая работа должна строиться по различным направлениям, в том числе путем устранения организационных и других дефектов, способствующих достижению противоправного результата⁸. Поэтому в деятельности по предупреждению рассматриваемых преступлений необходим комплексный и системный подход. В статье остановимся на отдельных аспектах.

Первостепенное значение, по нашему мнению, имеет применение действенных превентивных мер непосредственно в банках. Эти меры должны включать как контроль за деятельностью работников, осуществляющих оформление договоров с клиентами банков, другие финансовые операции, так и изучение личности работников банка, проведение мониторинга их личностного поведения в рамках трудовой деятельности.

Важным является проведение проверок претендента на замещение соответствующей должности при устройстве его на работу в банк, а также проведение периодических проверок работников банка в процессе их деятельности.

Во втором приведенном нами примере судебной практики очевидно, что подсудимый К., реализуя свой преступный умысел на хищение чужого имущества, оформил 41 договор о потребительском кредите на клиентов банка путем ввода и модификации компьютерной информации. По этим договорам, как установили работники отдела защиты бизнеса данного банка, не осуществлялось погашение кредитов, заключенных К. в период с января по май, что является достаточно длительным периодом. В этой связи очевидна необходимость сокращения сроков проверки заключаемых с клиентами договоров, проведения других финансовых операций, выполнения клиентами обязательств по договорам и т.д., что позволит в том числе выявить нарушения в деятельности работников банка.

Для предупреждения совершения работниками банков рассматриваемых преступлений следует также предусмотреть такую меру, как формирование характеристики (профиля) «благонадежного работника банка» и использование положений, составляющих этот профиль, в практической деятельности при проведении проверок в отношении них. Так, к характеристике (профилю) благонадежного работника банка следует отнести: критерии нормативного поведения работников; признаки, которые обеспечивают устойчивость личности и защищают от девиантного, в том числе делинквентного, поведения.

Кроме того, следует сформировать систему факторов, с учетом которых работники банков могут совершать преступления, а также определить особенности поведения работника банка на разных этапах совершения преступления.

Рассмотрим характеристики (профиля) благонадежного работника банка. К критериям нормативного поведения работника следует отнести: выполнение работы в соответствии с регламентом (согласно установленным требованиям в банке); осуществление деятельности согласно распорядку трудового дня; реализация

⁷ Криминология : учебник / отв. ред. И. М. Мацкевич. М., 2023. С. 132.

⁸ Кудрявцев В. Н. Причинность в криминологии. О структуре индивидуального преступного поведения. М., 2019. С. 106.



на высоком уровне своих профессиональных компетенций; качественное выполнение порученной работы.

К признакам, которые обеспечивают устойчивость личности и защищают от девиантного, в том числе делинквентного, поведения, следует отнести: высокий уровень правового сознания (имеет значение и в том случае, если деятельность не связана с применением норм права в банковской сфере); корпоративную солидарность; стремление не подвести руководство и коллектив; способность нести личную ответственность за свои поступки, отстаивать свои позиции; адекватная оценка работником складывающейся ситуации, имеющей противозаконный характер, оценка ее последствий, а также адекватность реагирования на предложения, имеющие противоправный характер; психологическая устойчивость; отсутствие (невыраженность) рискованных акцентуаций характера.

Приведенная модель профиля благонадежного работника банка может быть использована в практической деятельности подразделений службы безопасности банка.

Выделим систему факторов, с учетом которых работники банков могут совершать преступления, а также определим особенности поведения работника банка на разных этапах совершения преступления. Так, к факторам, носящим условно нейтральный характер, которые в зависимости от характера ситуации могут повлиять на принятие решения о совершении преступления, следует отнести: круг общения как в коллективе (организации), так и вне его; проявление интереса к профессиональным навыкам (роду, направлению деятельности) конкретного работника со стороны другого (других работников).

Рассмотрим особенности поведения работников банка на разных этапах реализации преступления.

Следует учитывать, что механизм преступного поведения включает: формирование мотивации совершения преступления; планирование преступных действий; исполнение преступления и наступление общественно опасных последствий.

На формирование мотивации к совершению преступления могут оказывать влияние среда общения; медиапространство, где, например, продемонстрированы реализация преступления и безнаказанность за его совершение; перспективы получения значительного (солидного) для работника банка дохода от преступной деятельности; исключительные ситуации, связанные с финансовыми трудностями (например, долги, болезнь близкого человека и т.д.).

При планировании преступления банковский работник может стремиться получить доступ к личным данным клиентов банка, в том числе и vip-клиентам (если это не входит в его должностные обязанности); совершать какие-либо операции во время перерыва, после окончания трудового дня, что является нестандартным временем; совершать какие-либо операции, которые не входят в круг его должностных обязанностей. В составе группы лиц по предварительному сговору (организованной группы) работник на этапе планирования и подготовки к совершению преступления может неоднократно контактировать с работниками, выполняющими деятельность на различных других направлениях банковской деятельности, пытаться в качестве подготовки выполнять определенные действия или проверять возможность их выполнения.

В механизме преступного поведения этап исполнения преступления и наступления общественно опасных последствий предполагает совершение непосредственно преступных действий как лично работником банка, так и совместно с другими работниками в составе группы лиц по предварительному сговору или организованной группы.

Изучение и выявление указанных факторов, с учетом которых работники банков могут совершать преступления, и особенностей поведения на разных этапах совершения преступления представляется важным, поскольку работники службы безопасности банков в своей деятельности могут их выявлять.

В качестве превентивной меры следует обозначить информирование работников банков о произошедших нарушениях в банке, правовых аспектах в связи с выявленными нарушениями, в том числе об ответственности.

В качестве еще одной профилактической меры следует назвать организацию работы службы экономической безопасности банка по изучению причин и условий, способствующих совершению преступлений работниками банка посредством информационных технологий. Получить соответствующую информацию возможно путем изучения судебной практики, находящейся в открытом доступе, например приговоров судов общей юрисдикции. Обобщение судебной практики позволит выделить ряд факторов, обуславливающих рассматриваемые преступления, и своевременно принять превентивные меры.

Одной из проблем предупреждения преступлений, совершаемых работниками банка посредством информационных технологий, на современном этапе является нехватка квалифицированных кадров IT-специалистов. В этой связи нередко принимаются на работу специалисты, требования к которым снижены, что прямо влияет на качество их деятельности и ее результаты в области обеспечения безопасности.

Важное значение в предупреждении рассматриваемых преступлений имеет эффективное взаимодействие между банками и органами внутренних дел. Учитывая «закрытость» деятельности банков, взаимодействие в основном осуществляется в связи с выявленным преступлением в банке и сообщением о преступлении.

Следует отметить, что чрезвычайно важен поиск новых эффективных форм взаимодействия и предупреждения совершения преступлений в банках посредством информационных технологий. Например, после внесения изменений и дополнений в ст. 26 Федерального закона «О банках и банковской деятельности» Федеральным законом от 20.10.2022 сотрудники МВД России имеют полномочия оперативно получать данные о финансовых операциях из автоматизированной системы Банка России ФинЦЕРТ с соблюдением требований закона о банковской тайне. В то же время информацию, полученную от правоохранительных органов, банки могут учитывать для предотвращения мошеннических операций.

В качестве новой меры можно указать «создание компьютерной программы, позволяющей пользователю, загрузив комплекс переменных, получить результат планируемой или проведенной банковской операции. Использование такого инструмента позволит перепроверять действия банковских служащих небольших по штату банковских офисов, в которых зачастую один работник совмещает



несколько должностей и может практически без согласования совмещать многие операции»⁹.

Таким образом, на современном этапе важнейшее значение имеет оптимизация мер предупреждения преступлений, совершаемых посредством информационных технологий работниками банков, поскольку ущерб от таких преступлений причиняется не только банку, но и его клиентам. Банки несут также репутационные риски.

Первостепенное значение имеют применение превентивных мер непосредственно в банках, а также поиск новых форм предупреждения рассматриваемых преступлений. В качестве таких мер выделены: формирование характеристики (профиля) благонадежного работника банка; формирование системы факторов, с учетом которых работники банков могут совершать преступления, использование этих моделей в практической деятельности подразделений службы безопасности банков; оптимизация деятельности службы экономической безопасности банков; создание новых компьютерных программ, позволяющих всесторонне контролировать деятельность работников банков; совершенствование форм взаимодействия банков с правоохранительными органами.

БИБЛИОГРАФИЯ

1. Долганов С. И., Желудков А. С. Некоторые аспекты использования информационных технологий в предупреждении корпоративного мошенничества в сфере банковской деятельности // Академическая мысль. — 2020. — № 2 (11).
2. Криминология : учебник / под ред. А. И. Долговой. — 4-е изд., перераб. и доп. — М., 2010.
3. Криминология : учебник / под ред. Н. Ф. Кузнецовой, В. В. Лунеева. — 2-е изд., перераб. и доп. — М., 2004.
4. Криминология : учебник / отв. ред. И. М. Мацкевич. — М., 2023.
5. Кудрявцев В. Н. Причинность в криминологии. О структуре индивидуального преступного поведения. — М., 2019.
6. Мацкевич И. М. Причины экономической преступности : учебное пособие. — М., 2019.

⁹ Долганов С. И., Желудков А. С. Некоторые аспекты использования информационных технологий в предупреждении корпоративного мошенничества в сфере банковской деятельности // Академическая мысль. 2020. № 2 (11). С. 57.

Криминологическое противодействие экономическим преступлениям, совершаемым с использованием информационно-телекоммуникационных технологий

Аннотация. В статье анализируются новые средства и способы совершения экономических преступлений в эпоху цифровизации. Автор исследует новые способы совершения преступлений при покупке, продаже товаров на маркетплейсах и приходит к выводу, что основными мерами предупреждения экономических преступлений в условиях цифровой экономики являются совершение платежей на интернет-ресурсах с отдельной банковской карты, на которой находится небольшая денежная сумма; игнорирование пользователем сторонних ссылок в момент осуществления покупок на сайте маркетплейса. При этом в случае технического сбоя на маркетплейсе, в результате которого пользователь без оплаты приобретает товары, лицо подлежит уголовной ответственности. В статье обращается внимание на распространение использования технологии дипфейк при осуществлении хищения денежных средств, предлагается в целях предупреждения таких преступлений поддержать законопроект, согласно которому необходимо установить квалифицирующие признаки в ст. 158 и ст. 159 УК РФ, предполагающие совершение преступления с использованием подмены признаков личности. Автор приходит к выводу, что введение в гражданский оборот цифрового рубля и внесение изменений в отдельные постановления Пленума Верховного Суда РФ в части признания криптовалюты объектом хищения поможет снизить уровень некоторых экономических преступлений.

Ключевые слова: дипфейк, криптовалюта, цифровой рубль, виртуальные активы, киберпреступление, блокчейн, фишинг, хищение



Ирина Сергеевна МОЧАЛКИНА,
преподаватель кафедры
криминологии и уголовно-
исполнительного права,
заместитель директора
Института публичного
права и управления
Университета имени
О.Е. Кутафина (МГЮА),
кандидат
юридических наук
ismochalkina@msal.ru
125993, Россия, г. Москва,
ул. Садовая-Кудринская,
д. 9

DOI: 10.17803/2311-5998.2025.129.5.189-196

Irina S. MOCHALKINA,

Lecturer of the Department of Criminology and
Criminal-Executive Law, Deputy Director of the
Institute of Public Law and Management
of the Kutafin Moscow State Law University (MSAL),
Cand. Sci. (Law)

ismochalkina@msal.ru

9, ul. Sadovaya-Kudrinskaya, Moscow, Russia, 125993

Criminological counteraction to economic crimes committed using information and telecommunication technologies

Abstract. *The article analyzes new means and methods of committing economic crimes in the digital era. The author examines new ways of committing crimes when buying and selling goods on marketplaces and comes to the conclusion that the main measures to prevent economic crimes in the digital economy are making payments on Internet resources from a separate bank card with a small amount of money; ignoring third-party links by the user when making purchases on the marketplace website. At the same time, in the event of a technical failure on the marketplace, as a result of which the user purchases goods without payment, the person is subject to criminal liability. The article draws attention to the widespread use of deepfake technology in theft of funds, and proposes to support the bill in order to prevent such crimes, according to which it is necessary to establish qualifying features in Art. 158 and Art. 159 of the Criminal Code of the Russian Federation, which involve committing a crime using the substitution of personality traits. The author concludes that the introduction of the digital ruble into civil circulation and amendments to certain Resolutions of the Plenum of the Supreme Court of the Russian Federation in terms of recognizing cryptocurrency as an object of theft will help reduce the level of certain economic crimes.*

Keywords: *deepfake, cryptocurrency, digital ruble, virtual assets, cybercrime, blockchain, phishing, theft*

Согласно отчету МВД РФ о состоянии преступности в Российской Федерации за январь — декабрь 2024 г., за указанный период было зарегистрировано 765,4 тыс. преступлений, совершенных с использованием высоких технологий, что на 13,1 % больше, чем в 2023 г. Удельный вес преступлений, совершенных при помощи информационно-телекоммуникационных технологий, в общем числе зарегистрированных преступлений составил 40 %, что указывает на рост преступлений в цифровой среде¹. Стоит отметить, что около половины таких деяний относятся к категориям тяжких и особо тяжких преступлений;

¹ Краткая характеристика состояния преступности в Российской Федерации за январь — декабрь 2024 года // URL: <https://мвд.рф/reports/item/60248328/> (дата обращения: 25.03.2025).

с использованием сети Интернет совершались 4 преступления из 5. При этом две трети указанных преступлений (63,5 %) составили кражи и мошенничества.

По заявлению Президента РФ, ущерб от киберпреступлений в 2024 г. составил около 200 млрд рублей, уровень раскрываемости преступлений в сфере информационно-телекоммуникационных технологий снизился, но при этом злоумышленники находят новые способы совершения преступлений². Вышесказанное обуславливает необходимость изучения и разработки мер противодействия экономическим преступлениям, совершенным с использованием цифровых инструментов.

Согласно оценкам аналитиков больше 3 млрд записей, которые содержат персональные данные людей, находятся в открытом доступе в сети Интернет, при этом в большинстве случаев источниками утечки информации являются не банки и финансовые организации³. Например, в 2024 г. была организована крупнейшая кибератака на государственную систему, использующуюся для управления судебными процессами, — ГАС «Правосудие». Злоумышленники получили информацию о состоянии судебных дел граждан, а также персональные данные лиц, участвующих в процессах.

Зачастую пользователи сети Интернет собственноручно вручают данные о себе представителям криминального мира при регистрации на маркетплейсах и иных ресурсах, которые плохо защищены. Нередко, получив логин и пароль от входа в личный кабинет маркетплейса, мошенники совершают у подконтрольных лиц множество покупок на сумму, не превышающую 1 000 руб. для обхода ввода кода подтверждения от банка, после чего полученные денежные средства выводятся. При покупке товаров в сети Интернет существуют и иные уловки недобросовестных продавцов: создание фишинговых сайтов, которые визуально трудно отличимы от официальных; появление всплывающего окна со скидкой в момент совершения покупки на сайте, при клике на которое злоумышленнику передаются банковские данные пользователя.

Вместе с тем не только продавцы, но и покупатели маркетплейсов могут являться субъектом совершения экономических преступлений в эпоху цифровизации. Так, в 2024 г. 23-летняя жительница Красноярска зарегистрировала аккаунт на Wildberries, далее при добавлении товаров в корзину она обнаружила технический сбой. Все товары, выбранные покупателем, автоматически приобретали статус «оплачено». Заметив данный факт, девушка не сообщила о сбое в службу поддержки, а продолжила совершать покупки различных товаров, в том числе смартфоны, золотые украшения. Общая сумма покупок злоумышленницы составила 1,2 млн руб., после чего приобретенные товары были выставлены ею на продажу в других магазинах⁴. Прокуратура утвердила обвинение в мошенничестве в особо крупном размере.

² Ущерб от киберпреступлений в 2024 году составил порядка 200 млрд рублей // URL: <https://www.kommersant.ru/doc/7552645> (дата обращения: 25.03.2025).

³ Действия мошенников в Интернете в 2024 году обойдутся в 1 трлн рублей // URL: <https://www.vedomosti.ru/technology/articles/2024/11/06/1073370-deistviya-moshennikov-1-trln> (дата обращения: 25.03.2025).

⁴ В Красноярске женщина обманула Wildberries на 1,2 миллиона рублей // URL: <https://ria.ru/20241021/wildberries-1979117404.html> (дата обращения: 25.03.2025).



Рассмотренный случай не является единичным. В 2024 г. к уголовной ответственности был привлечен житель Крыма, который из-за технического сбоя приобрел без оплаты товары на маркетплейсе на сумму свыше 13 млн руб. Суд приговорил злоумышленника к 4 годам колонии общего режима со штрафом в 130 тыс. руб.⁵

Для анализа и изучения интересен вопрос, связанный со снижением стоимости товара на маркетплейсе в случае технического сбоя или по иным причинам, его последующей покупкой пользователем маркетплейса и необходимостью привлечения покупателя к ответственности. Согласно определению Верховного Суда РФ от 04.04.2023 № 49-КГ22-28-К6, в 2021 г. на сайте ООО «Сеть Связной» пользователь дистанционным способом приобрел телевизор, уплатив за него 480 руб.⁶ При оформлении заказа была определена дата доставки товара, но в этот день покупатель не получил телевизор, а уплаченные денежные средства были возвращены пользователю сайта. Несмотря на заниженную почти в 80 раз стоимость товара, суд пришел к выводу, что магазин не вправе отказаться от передачи оплаченного товара. В рассматриваемом случае покупатель действовал правомерно, требуя доставки купленного товара за 480 руб. в определенные сроки; в его действиях не содержатся признаки состава преступления.

В качестве основных мер предупреждения экономических преступлений, совершаемых при покупке и продаже товаров на маркетплейсах, можно выделить следующие: совершение платежей на интернет-ресурсах с отдельной банковской карты, на которой находится небольшая денежная сумма; отключение опции «сохранение пароля и логина» на сайте маркетплейса; проверка рейтинга продавца; игнорирование пользователем сторонних ссылок в момент осуществления покупок на сайте маркетплейса; периодическая смена пароля покупателем; совершение покупок через защищенную домашнюю сеть вместо открытых сетей Wi-Fi, поскольку с помощью анализатора трафика можно получить данные для входа на некоторые сайты, используемые жертвой.

Развитие компьютерных технологий привело к созданию на основе образцов голоса и изображения человека видео-, аудиоматериалов, иллюстрирующих несуществующие события, явления и процессы, — дипфейков. В настоящее время отличить оригинальное видеоизображение лица от сконструированного искусственным интеллектом зачастую не представляется возможным без привлечения специалиста. Несколько лет назад мошенники из Гонконга, используя технологию дипфейк, смогли похитить 26 млн долларов у крупной корпорации, позвонив по видеосвязи сотрудникам, выдав себя за старшего менеджера компании и попросив перевести денежные средства на банковский счет⁷.

⁵ Житель Крыма обманул маркетплейс на 13 млн рублей // URL: <https://crimea.ria.ru/20241029/zhitel-kryma-obmanul-marketpleys-na-13-mln-rublej-1141452360.html> (дата обращения: 20.03.2025).

⁶ Определение Верховного Суда РФ № 49-КГ22-28-К6 от 04.04.2023 // URL: <https://ur29.ru/resheniya-sudov/vsrf-49-kg22-28-k6-ot-04042023/> (дата обращения: 20.03.2025).

⁷ В Гонконге с помощью дипфейка украли миллионы долларов у крупнейшей корпорации // URL: <https://rg.ru/2024/02/04/v-gonkonge-s-pomoshchiu-dipfejka-moshenniki-ukrali-milliony-dollarov-u-krupnejshij-korporacii.html> (дата обращения: 15.03.2025).

Сегодня одной из распространенных схем мошенничества с использованием дипфейков является фейковый розыгрыш денежных средств среди подписчиков в социальной сети блогера, которая предварительно взламывается злоумышленником. На основе опубликованных автором оригинальных аудио-, фото-, видеоматериалов преступник создает дипфейк с просьбой к подписчикам поучаствовать в конкурсе, для чего необходимо перейти по ссылке на определенный сайт. После совершения описанного действия жертве приходит сообщение о выигрыше, для получения которого необходимо заплатить комиссию. Так, один из самых популярных YouTube-блогеров MrBeast, имеющий более 300 млн подписчиков, опубликовал в своей социальной сети в 2023 г. информацию о том, что мошенники при помощи нейросетей создали фейковое видео, в рамках которого он призывает к участию в конкурсе, а для получения выигрыша пользователю необходимо зайти на специальный сайт и оплатить комиссию⁸. При переходе по ссылке подписчики не только оплачивали необходимый взнос, но и лишались гораздо более крупных денежных сумм в результате проведенной транзакции. Стоит отметить, что описанная схема мошенничества распространена и на территории нашей страны.

В целях противодействия преступлениям, совершаемым с использованием технологии дипфейк, в 2024 г. в Государственную Думу был внесен законопроект, в котором предлагалось внести в УК РФ изменения, в частности, в ст. 158 и 159 УК РФ, дополнив их квалифицирующими признаками: «с использованием изображения или голоса (в том числе фальсифицированных или искусственно созданных) потерпевшего или иного лица, а равно с использованием биометрических персональных данных потерпевшего или иного лица»⁹. За совершение мошенничества с использованием рассматриваемой технологии законопроектом предусмотрено самое строгое наказание в виде лишения свободы на срок до шести лет.

Несмотря на имеющуюся в настоящее время возможность квалификации содеянного по действующим нормам УК РФ, представляется, что введение квалифицирующего признака в статьях, регламентирующих хищения, будет являться сдерживающим фактором для злоумышленников из-за усиления уголовной ответственности. Однако прежде чем устанавливать уголовную ответственность, в рамках отраслевого законодательства необходимо урегулировать правовое положение и вопросы использования технологий подмены признаков личности.

При совершении хищений в информационно-телекоммуникационной сети злоумышленники используют не только технологию дипфейк, но и новые методы посягательства на криптовалюту. По данным аналитической компании Chainalysis, общая сумма хищений указанного виртуального актива за 2024 г. киберпреступниками составила свыше 2,2 млрд долларов, что больше на 21 % по сравнению с 2023 г.¹⁰

⁸ MrBeast разоблачает мошенничество с дипфейками // URL: <https://www.cryptopolitan.com/ru/mrbeast-exposes-deepfake-scam/> (дата обращения: 18.03.2025).

⁹ Законопроект № 718538-8 «О внесении изменений в Уголовный кодекс Российской Федерации» // URL: <https://sozd.duma.gov.ru/bill/718538-8> (дата обращения: 18.03.2025).

¹⁰ В 2024 году хакеры украли криптовалюту на \$ 2,2 млрд // URL: <https://www.kommersant.ru/doc/7399554> (дата обращения: 10.03.2025).



Одной из новых схем совершения хищения, предметом которого выступает криптовалюта, является привлечение злоумышленниками к завладению цифровыми активами иных представителей преступного мира. Так, притворяясь неопытными пользователями криптовалют, преступники в социальных сетях или тематических чатах пишут сообщения, в которых просят помочь вывести криптовалюту с цифрового кошелька, а также указывают определенную фразу, которая служит ключом доступа к хранилищу.

Данная схема рассчитана на тех пользователей, которые решат воспользоваться оставленным в сообщении ключом и вывести чужую криптовалюту на свой криптовалютный кошелек. При вводе ключа пользователь замечает, что для оплаты комиссии за осуществление транзакции на кошельке отсутствует необходимая сумма, после чего он переводит необходимые средства на адрес криптовалютного кошелька, но комиссия уходит на другой адрес, подконтрольный злоумышленнику. В настоящее время с такими сообщениями пользователи все чаще сталкиваются на Youtube и Telegram, модераторы которых в целях предупреждения хищений денежных средств стараются оперативно удалять подобные комментарии.

Новым способом совершения хищений, предметом которых выступает криптовалюта, является рассылка приглашений в фейковые видеоконференции Zoom. После того как пользователь перейдет по ссылке и нажмет «начать конференцию», на его устройство устанавливается вредоносное программное обеспечение, которое позволяет получить множество данных о человеке, в том числе ключи от криптовалютных кошельков. Собранная информация о пользователе передается на сервера, подконтрольные злоумышленникам. Поскольку возбуждение уголовных дел по факту хищения криптовалюты во многих случаях затруднительно и вызывает вопросы, что создает простор для дальнейшей деятельности злоумышленников, предлагается внести изменения в постановления Пленума Верховного Суда РФ о судебной практике по делам о мошенничестве, присвоении и растрате, краже, грабеже и разбое и признать криптовалюту предметом хищений.

Еще одним инструментом противодействия экономическим преступлениям является введение в гражданский оборот цифрового рубля, который в 2023 г. был включен в ст. 128 ГК РФ в перечень объектов гражданских прав. Цифровые рубли представляют собой третью форму национальной валюты, среди них могут появиться такие средства платежа, которые позволят определять его назначение. В частности, в рамках бюджетного финансирования государством могут быть выделены цифровые рубли для выполнения каких-либо работ или оказания услуг, которые будет невозможно израсходовать иным образом, кроме целевого назначения. В случае попытки перевода цифровых рублей не по корректному платежному адресу система не позволит выполнить транзакцию. Таким образом, цифровой рубль является новым инструментом противодействия финансовым, коррупционным преступлениям, который активно тестируется в настоящее время в целях его дальнейшего запуска на территории Российской Федерации.

Вместе с тем хищение цифрового рубля также становится затруднительным. Взлом блокчейна, на основе которого будет функционировать цифровой рубль, теоретически возможен, но на практике маловероятен. Самая большая проблема в данном случае будет заключаться в методах социальной инженерии, которые

повсеместно используются мошенниками. Например, злоумышленник в телефонном звонке может представиться сотрудником Центробанка и попросить пользователя перевести цифровой рубль на другой цифровой кошелек. Одной из основных мер предупреждения таких хищений является систематическое информирование граждан о новых средствах платежа, принципах их функционирования, запрете передачи данных от входа в цифровой кошелек.

Таким образом, среди основных мер противодействия экономическим преступлениям, совершаемым при покупке и продаже товаров на маркетплейсе с использованием технологии дипфейк и новых методов получения ключей от криптовалютных кошельков, можно выделить следующие:

- 1) совершение платежей на интернет-ресурсах с отдельной банковской карты, на которой находится небольшая денежная сумма;
- 2) отключение опции «сохранение пароля и логина» на сайте маркетплейса;
- 3) проверка рейтинга продавца;
- 4) игнорирование пользователем сторонних ссылок в момент осуществления покупок на сайте маркетплейса;
- 5) периодическая смена пароля покупателем;
- 6) совершение покупок через защищенную домашнюю сеть вместо открытых сетей Wi-Fi;
- 7) введение квалифицирующего признака в статьях, регламентирующих хищения, в рамках которого будет предусмотрена повышенная уголовная ответственность за использование технологии дипфейк;
- 8) введение в гражданский оборот цифрового рубля;
- 9) повышение уровня правового сознания граждан, систематическое информирование общества о новых средствах платежа.

БИБЛИОГРАФИЯ

1. В 2024 году хакеры украли криптовалюту на \$2,2 млрд // URL: <https://www.kommersant.ru/doc/7399554> (дата обращения: 10.03.2025).
2. В Гонконге с помощью дипфейка украли миллионы долларов у крупнейшей корпорации // URL: <https://rg.ru/2024/02/04/v-gonkonge-s-pomoshchiu-dipfejka-moshenniki-ukrali-millions-dollarov-u-krupnejshej-korporacii.html> (дата обращения: 15.03.2025).
3. В Красноярске женщина обманула Wildberries на 1,2 миллиона рублей // URL: <https://ria.ru/20241021/wildberries-1979117404.html> (дата обращения: 25.03.2025).
4. Действия мошенников в интернете в 2024 году обойдутся в 1 трлн рублей // URL: <https://www.vedomosti.ru/technology/articles/2024/11/06/1073370-deistviya-moshennikov-1-trln> (дата обращения: 25.03.2025).
5. Житель Крыма обманул маркетплейс на 13 млн рублей // URL: <https://crimea.ria.ru/20241029/zhitel-kryma-obmanul-marketpleys-na-13-mln-rublej-1141452360.html> (дата обращения: 20.03.2025).
6. Краткая характеристика состояния преступности в Российской Федерации за январь — декабрь 2024 года // URL: <https://мвд.рф/reports/item/60248328/> (дата обращения: 25.03.2025).



7. Ущерб от киберпреступлений в 2024 году составил порядка 200 млрд рублей // URL: <https://www.kommersant.ru/doc/7552645> (дата обращения: 25.03.2025).
8. MrBeast разоблачает мошенничество с дипфейками // URL: <https://www.cryptopolitan.com/ru/mrbeast-exposes-deepfake-scam/> (дата обращения: 18.03.2025).

Формирование криминогенных ситуаций в сфере социальных медиа и их влияние на процесс криминализации личности

Аннотация. В статье рассматриваются условия, способствующие формированию криминогенных ситуаций в сфере социальных медиа, обозначаются их виды. Анализируется влияние криминогенных ситуаций на личность, отмечается, что процесс криминализации личности в медиаполе выстраивается через воздействие ряда ключевых механизмов. К ним относятся: длительное либо мгновенное воздействие медиаконтента на личность; широкое распространение деструктивного и дезинформационного контента через тематические сообщества, чаты и группы и его нормализация; анонимность профиля, которая создает иллюзию безнаказанности; низкий уровень социального контроля и др. Последствиями для личности в результате такого воздействия становятся: искаженное восприятие социальных норм; формирование установок на оправдание противоправного поведения; снижение терпимости и, как следствие, рост агрессии. Выводы о влиянии социальных медиа на процесс криминализации личности основаны на анализе существующих исследований в области криминологии, психологии и статистики, которые приводятся в данной статье. На основе проведенного исследования формулируются предложения по применению современных инструментов оценки криминогенных ситуаций через системы мониторинга информационного поля как одного из перспективных направлений изучения преступлений и их предупреждения.

Ключевые слова: криминогенная ситуация, социальные медиа, медиаконтент, мониторинг соцсетей, криминализация личности, предупреждение преступлений, медиаресурсы, социальная сеть, кибербуллинг, дезинформация, социальное заражение



**Елена Валерьевна
ЧЕРВОННЫХ,**
преподаватель кафедры
криминологии и уголовно-
исполнительного права
имени В. Е. Эминова
Университета
имени О.Е. Кутафина,
кандидат
юридических наук
evchervonnyh@msal.ru
125993, Россия, г. Москва,
ул. Садовая-Кудринская,
д. 9

DOI: 10.17803/2311-5998.2025.129.5.197-207

Elena V. CHERVONNYKH,

teacher of the Department of Criminology and Penal Law
of the Kutafin Moscow State Law University (MSAL),
Cand. Sci. (Law)

evchervonnyh@msal.ru

9, ul. Sadovaya-Kudrinskaya, Moscow, Russia, 125993

Formation of Criminogenic Situations in the Sphere of Social Media and their Influence on the Process of Criminalization of the Individual

Abstract. *The article examines the conditions that contribute to the formation of criminogenic situations in the sphere of social media, and identifies their types. The influence of criminogenic situations on the individual is analyzed, and it is noted that the process of criminalization of the individual in the media field is built through the influence of a number of key mechanisms. These include: long-term or instantaneous impact of medical content on the individual; widespread distribution of destructive and disinformation content through thematic communities, chats and groups and its normalization; profile anonymity, which creates the illusion of impunity; low level of social control and others. The consequences for the individual as a result of such influence are: a distorted perception of social norms; the formation of attitudes to justify illegal behavior; a decrease in tolerance and, as a consequence, an increase in aggression. The conclusions about the influence of social media on the process of criminalization of the individual are based on the analysis of existing research in the field of criminology, psychology and statistics, which are presented in this article.*

Based on the conducted research, proposals are formulated for the use of modern tools for assessing criminogenic situations through information field monitoring systems, as one of the promising areas of studying crimes and their prevention.

Keywords: *crime situation, social media, media content, social media monitoring, criminalization of personality, crime prevention, media resources, social network, cyberbullying, disinformation, social contagion*

Криминогенные ситуации могут формироваться в сфере социальных медиа, которые изменили традиционные модели потребления информации. Пользователи становятся не только потребителями, но и создателями контента. Профессор Е. Л. Вартанова рассматривала этот процесс как децентрализацию информационного пространства, когда у потребителя информации появляется больше свободы¹. Е. Л. Вартанова также отмечала, что за счет увеличения объема информации в новых медиа снижается ее достоверность и медиаграмотность

¹ Вартанова Е. Л. Новые медиа как фактор модернизации СМИ // URL: http://www.vartanova.ru/articles/ru/novue_media.html (дата обращения: 29.03.2025).

населения, а цифровое неравенство приводит к появлению цифровых неграмотных².

Недостаток цифровых навыков и цифровой грамотности исключает пользователей из глобального информационного пространства³. О снижении способности пользователей социальных медиа к критическому мышлению — способности сомневаться в получаемой информации и своих убеждениях — писала в 2019 г. директор Исследовательского центра медиапсихологии в Калифорнии Памела Ратледж. Отсутствие навыка критического восприятия информации делает пользователей наиболее уязвимыми к разного рода манипуляциям в социальных медиа, включая неосознанное участие в противоправной деятельности.

Усложняет процесс критического восприятия информации обилие форматов пользовательского контента — текстовых сообщений, комментариев, цифровых фотографий и видеороликов, полученных с помощью всех взаимодействий онлайн и влияющих на модели поведения. Пользовательский контент — жизненная основа социальных сетей. Его обилие и трудности верификации формируют криминогенную ситуацию, включая массовую дезинформацию, фейковые новости, недостоверные сведения. Результат — искажение общественного восприятия реальности и формирование неверных убеждений⁴.

Мануэль Кастельс в своей работе «Информационная эпоха: экономика, общество и культура» в 2009 г. написал, что через социальные медиа формируется общественное мнение⁵. Массовая дезинформация в социальных медиа влияет на общественное мнение, провоцируя такие негативные последствия, как подрыв доверия к традиционным институтам власти, рост социальной напряженности, закрепление ложных стереотипов, провоцирование массовой паники и другие вредные процессы. Ярким примером является пандемия COVID-19, когда распространение недостоверных сведений о вирусе в информационном поле и методах его лечения приводило к опасным последствиям для здоровья и жизни людей⁶.

² «У революции в медиасфере есть свои жертвы», — считает Елена Вартанова // URL: <https://ria.ru/20110624/392657912.html?ysclid=m8ymmauhe533805242> (дата обращения: 30.03.2025).

³ Гладкова А. А., Гарифуллин В. З., Массимо Р. Модель трех уровней цифрового неравенства: современные возможности и ограничения (на примере исследования Республики Татарстан) // Вестник Моск. ун-та. Сер. 10 : Журналистика. 2019. № 4. С. 56.

⁴ Миронова А. В., Загоруйко В. И. Влияние социальных медиа на общественное мнение: актуальные проблемы и перспективы исследования // Вестник Южно-Уральского государственного университета. Серия : Социология. 2018. № 18 (4). С. 84—93 ; Очагов Н. А. Влияние социальных медиа на формирование общественного мнения и политические процессы // URL: <https://na-journal.ru/7-2023-sociologiya/6085-vliyanie-socialnyh-media-na-formirovanie-obshchestvennogo-mneniya-i-politicheskie-processy> (дата обращения: 30.03.2025).

⁵ Castells M. The Rise of the Network Society. Information Age. Vol. 1 ; 2nd edition with a New Preface edition. Wiley-Blackwell, 2009.

⁶ Демченко А. А. Психологические механизмы восприятия и распространения дезинформации в социальных сетях как фактор дестабилизации общественного сознания // Молодой ученый. 2025. № 2 (553). С. 437—439.



Таким образом, криминогенную ситуацию в социальных медиа следует рассматривать как любое действие, совокупность факторов и условий, которые способствуют совершению преступлений посредством использования социальных сетей: кибербуллинга, мошенничества, нарушения авторских прав, дезинформации, провокаций, распространения незаконного контента, организации преступных действий, угроз безопасности и др.

Формированию криминогенных ситуаций способствует и популярность социальных медиа за счет открывающихся возможностей — общения независимо от местонахождения, многомерности способов коммуникации, влияния на формирование общественного мнения, особенно среди молодежи, возможности формировать и выражать свою идентичность и т.д.

С ростом возможностей социальных медиа⁷ растет их влияние и внимание к ним со стороны разных государственных институтов. Одна из значимых черт, которую не могут контролировать власти, как пишет А. А. Шнайдер, — способность социальных медиа собирать большое количество единомышленников. Это стимулирует коллективную социальную активность⁸. Д. Бакунов отмечает, что социальные медиа через алгоритмы могут быть инструментом для манипуляции общественным мнением за счет усиленной коммуникационной составляющей. Об этом писали и исследователи в области психологии — А. М. Столяренко, Н. В. Сердюк, В. В. Вахнина, Л. Л. Грищенко и О. М. Боева⁹.

Таким образом, в сфере социальных медиа (платформ и всевозможных приложений, позволяющих пользователям взаимодействовать друг с другом) могут формироваться негативные условия и факторы через поток информации, общественное мнение, групповую динамику, психологическое воздействие, слежку и контроль. Закладываемые неочевидно негативные нарративы способны создать почву для деструктивного поведения.

Социальные медиа, в частности социальные сети и мессенджеры, являются одним из основных каналов криминогенного воздействия на личность в сети Интернет. Через них распространяются материалы, способствующие героизации и романтизации преступников и преступности в целом. Такой контент становится нормальным для пользователя. На этот факт обращали внимание В. В. Боровикова, О. П. Дубягина, А. В. Токарев¹⁰.

В сфере социальных медиа интерес для исследования представляют типы ситуаций, основанные на восприятии пользователя (явные и неявные) и на времени воздействия на пользователя (накопительные или мгновенные).

⁷ Их платформы — социальные сети, блоги, интернет-форумы, видеоблоги, мобильные и онлайн-продукты, мессенджеры и др.

⁸ Шнайдер А. А. Новые медиа — новые возможности // URL: <https://cyberleninka.ru/article/n/novye-media-novye-vozmozhnosti/viewer> (дата обращения: 30.03.2025).

⁹ Психологические аспекты деструктивного информационно-психологического воздействия / А. М. Столяренко, Н. В. Сердюк, В. В. Вахнина [и др.] // Психология и право. 2019. Т. 9. № 4. С. 75—89.

¹⁰ Токарев А. А. Роль средств массовой информации в предупреждении преступности : автореф. дис. ... канд. юрид. наук. М., 2012.

Явные ситуации, например, формирующиеся в социальных медиа протесты, практически всегда очевидны и легко просчитываются.

Неявные криминогенные ситуации распознать сложнее. К неявным криминогенным ситуациям в социальных медиа можно отнести распространение контента, формирующее у пользователя искаженное восприятие насилия как приемлемого или желаемого поведения (через популярные видеоигры, фильмы или даже мемы). Неявные криминогенные ситуации могут возникать в результате кибербуллинга, когда жертвы подвергаются длительному систематическому запугиванию, оскорблениям и преследованию других пользователей в сети Интернет. Это приводит к таким последствиям, как нарушение психического здоровья, самоубийство. Другим примером криминогенной ситуации является неосознанное участие пользователей в мошеннических схемах, например, через участие в лотереях или конкурсах, которые на самом деле являются обманом. Социальные медиа могут служить платформой для сексуальной эксплуатации и торговли людьми. Неявные ситуации могут включать в себя манипуляцию и вовлечение несовершеннолетних в опасные отношения. Появляется возможность вербовки, подготовки и координации действий организованных преступных групп и сообществ, что способствует совершению преступлений в реальной жизни. Платформы социальных медиа используются для распространения радикальных идеологий.

Влияние социальных медиа на формирование криминогенной ситуации осуществляется также, как указано выше, за счет накопительного или мгновенного воздействия.

Накопительное воздействие происходит постепенно. Медиаконтент потребляется длительно (от нескольких месяцев до нескольких лет). Воздействие на восприятие личностью тех или иных видов ситуаций происходит через повторяющиеся нарративы. Исследования показывают, что постоянное воздействие медиа на личность может изменять ее ценностные ориентации и формировать устойчивые установки, такие как нормализация насилия или правовой нигилизм, скептическое отношение к правоохранительным органам¹¹. В качестве примеров такого воздействия можно назвать рост социальной терпимости к мелким правонарушениям, рост латентных преступлений из-за опасения осуждения при обнаружении какой-либо чувствительной информации.

Мгновенное воздействие, как правило, возникает в виде быстрой реакции на конкретные освещаемые события, которые способны вызвать сильные эмоциональные реакции и спонтанные действия. Реакция практически всегда связана с сильными эмоциями (страх, гнев, подражание преступнику). Критическое мышление на фоне сильных эмоций при мгновенном воздействии не успевает работать. Наблюдаются всплески преступности или агрессии после определенных медийных событий, триггерами могут стать громкие жестокие преступления, например теракты. Мгновенное воздействие, особенно «в моменте» и на большое число пользователей, способно вывести на улицы массы людей¹².

¹¹ Давыдова М. А. Влияние медиа на формирование паттернов поведения современной молодежи // Инновационная наука: психология, педагогика, дефектология. 2021. № 4 (3). С. 6—19.

¹² Берковиц Л. Агрессия: причины, последствия и контроль. М. : Олма-Пресс, 2002.



Спонтанные погромы, особенно после трансляции сильных эмоциональных событий, протестных акций, — характерное при данном механизме поведение. Протест может и не выйти в офлайн, но остро протекать в социальных медиа, вынуждая на него реагировать органы государственной власти. Например, после теракта в «Крокус Сити Холле» и иных последовавших резонансных происшествий с участием мигрантов в социальных медиа наблюдается радикализация антимигрантских настроений: усилилась не только неприязнь к приезжим, но и социальная дистанция между людьми разных национальностей.

Одним из ярких примеров социального протеста против мигрантов стала отмена заказов такси в случае, если водитель оказывался родом из Таджикистана. Массово в тг-каналах публиковали скриншоты из мобильных сервисов такси, где клиенты спрашивали у водителей, принявших заказ, их национальность. В таджикских диаспорах рекомендовали проживающим в России соотечественникам не выходить из дома в вечернее время и не посещать массовые мероприятия. Люди стали в целом более внимательны к своему окружению. Публикации в информационном поле выходили под такими заголовками: «Мигранты против русских детей. Отцы готовы вершить самосуд. Диаспора заступает за насильников», «Мигранты оккупируют Россию ради будущего своих детей? Демография наравне с атомной доктриной». В регионах активно обсуждались предложения о возвращении смертной казни.

В тг-каналах ультраправых организаций после теракта в «Крокус Сити Холле» чаще стали наблюдаться сообщения с призывами к нападениям на лиц «неславянской внешности», включая угрозы расправ и самосуда над мигрантами. Существенно увеличилось количество видеороликов с нападениями на уроженцев Узбекистана, Таджикистана, Дагестана и других людей «неславянской внешности», цыган и женщин в хиджабах. Лишь за выходные дни после теракта в тг-каналах радикальных националистов было размещено более 300 публикаций, направленных на раскрутку криминальных инцидентов с участием мигрантов: с 4 по 22 марта (до теракта) таких постов было 460, а с 23 марта по 14 апреля — около 850 (рост практически в два раза)¹³.

Высокую опасность несет такое характерное для социальных медиа явление, как социальное заражение. Внутри социальных сетей через алгоритмы социальных медиа распространяются идеи, эмоции, поведение. Алгоритмы социальных медиа предназначены для показа пользователям контента, который соответствует их убеждениям и предпочтениям. Для этого создаются своего рода эхо-камеры, где пользователи подвергаются воздействию только информации и мнений, основанных на их собственных взглядах и убеждениях. Возможный результат — быстрое распространение поведения толпы. Пользователи в этих эхо-камерах укореняются в своих убеждениях и не воспринимают противоположные точки зрения, критическое мышление не работает¹⁴.

¹³ Тг-канал «Карельский бальзам. Новости» // URL: https://t.me/s/kb_announcements?before=188923 (дата обращения: 30.03.2025).

¹⁴ Чентола Д. Законы социального заражения. 7 стратегий изменения общественного мнения и поведения. М., 2022.

Одним из аспектов социального заражения является сила подражания, когда люди бессознательно имитируют поведение других. Исследуя феномен подражания, Р. М. Пэн экспериментально установила следующую закономерность: «...в процессе подражания у ребенка образуются условные рефлексy быстрее, чем классическим способом»¹⁵. Зарубежные социологи и психологи склонны считать подражание всеобщим законом взаимодействия, на котором основана социальная жизнь. Подражание объявляется простым копированием или эхом, «попугайничеством»¹⁶.

Благоприятными условиями для социального заражения являются деиндивидуализация, групповая поляризация и групповое мышление. Наиболее яркие примеры последствий этого явления в истории: массовое убийство-самоубийство более 900 членов культа «Храм народов» в Гайане в 1978 г.¹⁷; серия антиправительственных протестов и восстаний, охвативших Ближний Восток и Северную Африку в 2010—2011 гг.¹⁸; пандемия COVID-19, вызвавшая такие поведенческие реакции, как панические покупки, карантин, социальное дистанцирование, неуверенность в вакцинации и теории заговора.

Криминализация платформ напрямую коррелирует с их популярностью, особенно среди молодежи, и уровнем цифровой грамотности пользователей¹⁹. Аудитория социальных медиа исчисляется сотнями миллионов. Так, по данным DataReportal, в начале 2024 г. в России зарегистрировано 106 млн пользователей соцсетей (81,3 %), среди них 54,8 % женщин и 45,2 % мужчин, а медианный возраст российских пользователей составил 39,4 года²⁰.

Согласно исследованиям, наиболее криминогенной социальной сетью в российском цифровом пространстве является соцсеть «ВКонтакте». По данным судебной практики, в 2024—2025 гг. через нее были совершены финансовые мошенничества (47 % случаев через взломанные аккаунты), распространение

¹⁵ Божович Л. И., Славина Л. С. Психология детского подражания (экспериментально-психологическое исследование) // Культурно-историческая психология. 2007. Т. 3. № 2. С. 101—107.

¹⁶ Тард Г. Преступления толпы / пер. д-ра И. Ф. Иорданского ; под ред. проф. А. И. Смирнова. Казань : Н. Я. Башмаков, 1893.

¹⁷ Самое массовое самоубийство XX века // URL: <https://www.kommersant.ru/doc/2347175> (дата обращения: 30.03.2025).

¹⁸ Арабская весна. Страны Ближнего и Среднего Востока во второй половине XX — начале XXI в. // Молодой ученый. 2023. № 20 (467).

¹⁹ Захаров С. С. Социальная сеть как источник криминалистической информации // Молодой ученый. 2023. № 20 (467). С. 530—532.

²⁰ Digital 2024: The Russian Federation // URL: <https://datareportal.com/reports/digital-2024-russian-federation> (дата обращения: 30.03.2025).



экстремистского контента²¹, вербовки в преступные сообщества²²; 32 % приговоров были связаны с незаконным оборотом наркотиков с использованием этой платформы²³.

В 2024 г. сеть «ВКонтакте» представила «Месяц борьбы с кибербуллингом». Согласно опубликованным данным, 47 % случаев связаны с кибербуллингом, 65 % — с троллингом. Примерно 48 % респондентов отметили, что сталкивались с разжиганием ненависти в свой адрес, 43 % — с распространением клеветы²⁴.

Несмотря на то что криминогенное влияние социальных медиа на личность пока изучено недостаточно, ученые склоняются к мнению, что их влияние на формирование преступной личности существенно. Наибольшей уязвимостью обладают лица с: несформированными социальными установками²⁵ и низким уровнем самоконтроля, испытывающие потребности в негативном контенте²⁶. Среди всех категорий пользователей наиболее уязвимой категорией являются несовершеннолетние. С 2020 по 2024 г., по данным МВД России, в 74 раза выросло число интернет-преступлений, совершенных детьми. Оценить реальный масштаб сложно, что связано с высокой степенью латентности таких преступлений. Наблюдается увеличение количества тяжких преступлений, в частности диверсий, на которые несовершеннолетних в социальных сетях подталкивают кураторы, часто находящиеся в недружественных странах.

Криминализация личности в социальных медиа происходит под влиянием нескольких условий:

- *анонимность профилей*, которая создает иллюзию безнаказанности и позволяет разделять «виртуальную» и реальную личности. Психологи отмечают, что анонимность в социальных медиа может снижать социальные нормы и увеличивать вероятность агрессивного поведения. Постоянное потребление негативного контента провоцирует тревожность, агрессию и правовой нигилизм²⁷;

²¹ Бельков В. А., Бальжинимеева А. Б. Социальные сети как поле преступной деятельности: проблемные аспекты и пути их решения // Уголовный процесс, криминалистика, судебная экспертиза; оперативно-разыскная деятельность 2016. № 1(11). С. 55—57. URL: <https://cyberleninka.ru/article/n/sotsialnye-seti-kak-pole-prestupnoy-deyatelnosti-problemnye-aspekty-i-puti-ih-resheniya> (дата обращения: 30.03.2025).

²² Бельков В. А., Бальжинимеева А. Б. Указ. соч.

²³ Соловьев В. С. Преступность в социальных сетях Интернета (криминологическое исследование по материалам судебной практики) // Криминологический журнал Байкальского государственного университета экономики и права. 2016. Т. 10. № 1. С. 60—72.

²⁴ VK представил «Месяц борьбы с кибербуллингом» // URL: <https://adindex.ru/news/digital/2024/11/6/327135.phtml> (дата обращения: 30.03.2025).

²⁵ Анализ воздействия информационных потоков СМИ на социально-психологические характеристики личности // URL: <https://science-education.ru/ru/article/view?id=17770> (дата обращения: 30.03.2025).

²⁶ Анализ воздействия информационных потоков СМИ на социально-психологические характеристики личности.

²⁷ Анализ воздействия информационных потоков СМИ на социально-психологические характеристики личности.

- *простота и скорость получения информации.* В социальных медиа легко найти информацию о способах совершения преступлений, а также о методах уклонения от ответственности. Это может способствовать формированию преступных намерений;
- *быстрый поиск единомышленников:* насилие и преступление могут восприниматься как нормальные явления, как приемлемый вариант решения своих проблем.

Все это подчеркивает важность мониторинга и модерации контента в социальных сетях, а также проведения образовательных программ по безопасному поведению в Интернете.

Снижение уровня криминальных проявлений в социальных медиа — задача комплексная. Ее нельзя решить без участия государственных структур, образовательных учреждений, родителей и самих пользователей.

Могут помочь в снижении остроты следующие меры:

Обучение пользователей, особенно подростков, тому, как безопасно вести себя в Интернете. В ряде зарубежных стран, например в Австралии, на разных уровнях и в разных сферах внедряются программы по обучению цифровой грамотности, включая курсы для школьников и студентов вузов²⁸. Эти и иные программы учат детей не только безопасному поведению в Интернете, но и тому, как реагировать на случаи агрессии, для формирования полезных привычек в отношении безопасного поведения в социальных сетях.

Влияние на ситуацию через правовое поле. Полный или значительный государственный контроль ввели Северная Корея, Китай, Белоруссия, ОАЭ. В то же время США, Великобритания, Германия и некоторые другие страны Евросоюза вмешиваются в этот процесс незначительно, оставляя относительную свободу и допуская саморегуляцию²⁹.

Развитие партнерства государственных органов с технологическими компаниями, работающими в сфере Digital. Разрабатываемые такими компаниями алгоритмы мониторинга триггерного контента позволяют своевременно выявлять уровень социальной напряженности, социальные риски в информационной среде, деструктивный контент; прогнозировать эскалацию каких-либо событий через поведение пользователей в социальных сетях, а как результат — создавать более безопасную онлайн-среду.

Развитие культуры критического мышления в информационном потоке. Критическое мышление помогает анализировать информацию, не доверять поддельным новостям и принимать лучшие решения. В 2009 г. в Великобритании был опубликован доклад о введении нового предмета в школах, посвященного проблемам

²⁸ Соколов Д. В. Цифровая грамотность в условиях инновационной экономики // Управление наукой: теория и практика. 2021. Т. 3. № 3. С. 90—91.

²⁹ Король Д. П. Несовершеннолетнее лицо как субъект преступлений в сети Интернет // Киберпреступность: риски и угрозы : материалы Всероссийского студенческого круглого научно-практического стола с международным участием (11 февраля 2021 г.). СПб. : Астерион, 2021. С. 47—50.



преподавания критического мышления³⁰. За период с 2001 по 2009 г. количество британских школ с курсами критического мышления увеличилось со 130 до 1 000³¹.

Повышение осведомленности о преступлениях, совершаемых в социальных медиа. Например, в Канаде проводятся общественные компании, направленные на повышение осведомленности о кибербуллинге и его последствиях. Эти инициативы помогают создать более безопасную онлайн-среду и поддерживают жертв травли.

БИБЛИОГРАФИЯ

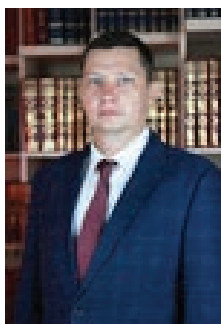
1. Бельков В. А., Бальжинимаева А. Б. Социальные сети как поле преступной деятельности: проблемные аспекты и пути их решения // Уголовный процесс, криминалистика, судебная экспертиза; оперативно-розыскная деятельность. — 2016. — № 1 (11). — С. 55—57.
2. Берковиц Л. Агрессия: причины, последствия и контроль. — М. : Олма-Пресс, 2002. — 512 с.
3. Божович Л. И., Славина Л. С. Психология детского подражания (экспериментально-психологическое исследование) // Культурно-историческая психология. — 2007. — Т. 3. — № 2. — С. 101—107.
4. Вартанова Е. Л. Новые медиа как фактор модернизации СМИ // URL: http://www.vartanova.ru/articles/ru/novue_media.html.
5. Гладкова А. А., Гарифуллин В. З., Массимо Р. Модель трех уровней цифрового неравенства: современные возможности и ограничения (на примере исследования Республики Татарстан) // Вестник Моск. ун-та. — Серия 10 : Журналистика. — 2019. — № 4.
6. Давыдова М. А. Влияние медиа на формирование паттернов поведения современной молодежи // Инновационная наука: психология, педагогика, дефектология. — 2021. — № 4 (3). — С. 6—19.
7. Демченко А. А. Психологические механизмы восприятия и распространения дезинформации в социальных сетях как фактор дестабилизации общественного сознания // Молодой ученый. — 2025. — № 2 (553). — С. 437—439.
8. Захаров С. С. Социальная сеть как источник криминалистической информации // Молодой ученый. — 2023. — № 20 (467). — С. 530—532.
9. Король Д. П. Несовершеннолетнее лицо как субъект преступлений в сети Интернет // Киберпреступность: риски и угрозы : материалы Всероссийского студенческого круглого научно-практического стола с международным участием (11 февраля 2021 г.). — СПб. : Астерион, 2021. — С. 47—50.

³⁰ Introducing a new subject and its assessment in schools: the challenges of introducing Critical Thinking AS/A level in the UK // URL: <https://www.cambridgeassessment.org.uk/images/126122-introducing-a-new-subject-and-its-assessment-in-schools-the-challenges-of-introducing-critical-thinking-as-a-level-in-the-uk.pdf> (дата обращения: 30.03.2025).

³¹ Результаты опроса Statista: как использовать критическое мышление в информационном потоке // URL: <https://trends.rbc.ru/trends/education/5e81f1339a7947c0a7a6eef3?from=sory> (дата обращения: 30.03.2025).

10. *Миронова А. В., Загоруйко В. И.* Влияние социальных медиа на общественное мнение: актуальные проблемы и перспективы исследования // Вестник Южно-Уральского государственного университета. — Серия : Социология. — 2018. — № 18 (4). — С. 84—93.
11. *Очагов Н. А.* Влияние социальных медиа на формирование общественного мнения и политические процессы // URL: <https://na-journal.ru/7-2023-sociologiya/6085-vliyanie-socialnyh-media-na-formirovanie-obshchestvennogo-mneniya-i-politicheskie-processy>.
12. Психологические аспекты деструктивного информационно-психологического воздействия / А. М. Столяренко, Н. В. Сердюк, В. В. Вахнина [и др.] // Психология и право. — 2019. — Т. 9. — № 4. — С. 75—89.
13. *Соколов Д. В.* Цифровая грамотность в условиях инновационной экономики // Управление наукой: теория и практика. — Т. 3. — № 3. С. 90—91.
14. *Соловьев В. С.* Преступность в социальных сетях Интернета (криминологическое исследование по материалам судебной практики) // Криминологический журнал Байкальского государственного университета экономики и права. — 2016. — Т. 10. — № 1. — С. 60—72.
15. *Тард Г.* Преступления толпы / пер. д-ра И. Ф. Иорданского ; под ред. проф. А. И. Смирнова. — Казань : Н. Я. Башмаков, 1893. — 44 с.
16. *Токарев А. А.* Роль средств массовой информации в предупреждении преступности : автореф. дис. ... канд. юрид. наук. — М., 2012. — 30 с.
17. *Чентола Д.* Законы социального заражения. 7 стратегий изменения общественного мнения и поведения. — М., 2022. — 140 с.
18. *Шнайдер А. А.* Новые медиа — новые возможности // URL: <https://cyberleninka.ru/article/n/novye-media-novye-vozmozhnosti/viewer>.
19. *Castells M.* The Rise of the Network Society. Information Age, vol. 1; 2nd Edition with a New Preface edition. — Wiley-Blackwell, 2009. — 625 p.





**Никита Сергеевич
ЕМЕЛЬЯНОВ,**

преподаватель кафедры
криминологии и уголовно-
исполнительного права
имени В. Е. Эминова
Университета имени
О.Е. Кутафина (МГЮА),
кандидат юридических наук
nikita-e@inbox.ru
125993, Россия, г. Москва,
ул. Садовая-Кудринская,
д. 9

Пенитенциарная киберпреступность как угроза стабильного функционирования исправительного учреждения

Аннотация. Приводится подход к определению дефиниции «пенитенциарная киберпреступность», рассмотрены различные виды пенитенциарных киберпреступлений. Определены внешние и внутренние угрозы киберпреступности для исправительных учреждений с указанием субъектов совершения этих преступлений и рассмотрением конкретных примеров. Основными субъектами совершения рассматриваемой категории преступлений выступают как сотрудники уголовно-исполнительной системы, так и осужденные, отбывающие наказание (внутренняя угроза). Одновременно рассмотрены иные субъекты — злоумышленники из числа профессиональных специалистов в области информационных технологий, так называемые хакеры (внешняя угроза).

С учетом значения служебной информации в обеспечении безопасности персонала и осужденных, а также тенденции к цифровизации различных управленческих процессов пенитенциарная киберпреступность изучена в контексте глобальной угрозы нормальному стабильному функционированию исправительного учреждения. Рассмотренные реальные примеры совершенных киберпреступлений указывают на недостатки в организации пенитенциарной кибербезопасности. В целях снижения уровня киберугроз предложен профилактический комплекс, включающий в себя управленческие, уголовно-правовые и научно-технические меры.

Ключевые слова: исполнение уголовных наказаний в виде лишения свободы, пенитенциарная киберпреступность, субъекты пенитенциарных киберпреступлений, объект пенитенциарного киберпреступления

DOI: 10.17803/2311-5998.2025.129.5.208-213

Nikita S. YEMELYANOV,

teacher V. E. Eminov Department of Criminology

and Penal Enforcement Law

of the Kutafin Moscow State Law University (MSAL),

Cand. Sci. (Law)

nikita-e@inbox.ru

9, ul. Sadovaya-Kudrinskaya, Moscow, Russia, 125993

Penitentiary Cybercrime as a Threat to the Stable Functioning of Correctional Institutions

Abstract. *The article provides an approach to defining the definition of “penitentiary cybercrime” and examines various types of penitentiary cybercrimes. External and internal threats of cybercrime for correctional institutions have been identified, indicating the subjects of these crimes and considering specific examples. The main subjects of the commission of this category of crimes are both employees of the penal enforcement system and convicts serving their sentences (internal threat). At the same time, other subjects are considered — intruders from among professional specialists in the field of information technology, the so-called hackers (an external threat).*

Given the importance of official information in ensuring the safety of staff and convicts, as well as the trend towards digitalization of various management processes, penitentiary cybercrime has been studied in the context of a global threat to the stable normal and stable functioning of correctional institutions. The considered real examples of cybercrimes committed indicate that there is a shortage in the organization of penitentiary cybersecurity. In order to reduce the level of cyber threats, a preventive package has been proposed that includes management, criminal law, and scientific and technical measures.

Keywords: *execution of criminal penalties in the form of imprisonment, penitentiary cybercrime, subjects of penitentiary cybercrime, object of penitentiary cybercrime, criminality among convicts, network attacks, unlawful access to official information of the penal enforcement system, corruption, disorganization, prevention of penitentiary crimes, penitentiary cybersecurity*

В соответствии с Концепцией развития уголовно-исполнительной системы Российской Федерации до 2030 г.¹ (далее — Концепция) совершенствование организации деятельности исправительных учреждений, наряду с прочим, включает в себя, с одной стороны, проведение цифровой трансформации и научно-техническое развитие, с другой — обеспечение безопасности уголовно-исполнительной системы (УИС). Проведение цифровой трансформации, в свою очередь, предусматривает внедрение цифровых технологий во все сферы деятельности

¹ Распоряжение Правительства РФ от 29.04.2021 № 1138-р «Об утверждении Концепции развития уголовно-исполнительной системы РФ на период до 2030 года» // СПС «КонсультантПлюс».



учреждений и органов УИС, а обеспечение безопасности — комплексную защиту информационной инфраструктуры уголовно-исполнительной системы. Последняя мера обусловлена в том числе наличием реальных и потенциальных угроз, связанных с ростом и совершенствованием различных видов киберпреступлений.

Термин «киберпреступление» происходит от слова «кибернетика». В свою очередь, кибернетика — это научно-практическая область, охватывающая закономерности получения, хранения, преобразования и передачи информации в различных системах, в том числе искусственных.

Согласно решению, принятому на Десятом конгрессе ООН по предупреждению преступности и обращению с правонарушителями (Вена, 2000 г.), основными категориями киберпреступлений принято считать: несанкционированный доступ к компьютерной информации, повреждение данных и программ, нарушение работы компьютерной системы или сети, несанкционированный перехват данных и компьютерный шпионаж². Исходя из этого, в Уголовном кодексе РФ четко определен перечень преступлений в сфере компьютерной информации (гл. 28), который соответствует вышеназванным критериям.

Таким образом, объектом преступного посягательства киберпреступников является *информация*, которая создается, хранится, обрабатывается и используется на компьютере и в компьютерной сети. Остальные виды преступлений, совершаемые с использованием информационных технологий, не являются в чистом виде киберпреступлениями.

Исходя из этого, можно предположить, что к категориям пенитенциарных киберпреступлений будут относиться те противоправные деяния, которые, во-первых, направлены на подрыв информационной безопасности учреждений и органов уголовно-исполнительной системы (ФСИН России), во-вторых, связаны с неправомерным и несанкционированным доступом к компьютерной информации, охраняемой законом (служебной информации), образуемой в ходе профессиональной деятельности сотрудников уголовно-исполнительной системы, в-третьих, совершаются путем незаконного взлома и получения личной информации о сотрудниках уголовно-исполнительной системы.

Подрыв информационной безопасности представляет собой комплекс угроз, направленных на блокировку или полную парализацию информационных систем. Для этого могут использоваться различные вредоносные программы либо применяться сетевые атаки (DDoS, XSS и т.д.). При общегосударственной тенденции на цифровизацию управленческих и иных процессов в деятельности уголовно-исполнительной системы активно применяются информационные технологии для хранения, обработки и использования служебной информации. Со временем многие данные будут доступны только в электронном формате. Так, в соответствии с Концепцией развития УИС в деятельности исправительных учреждений предполагается создание и внедрение «единой информационной системы, обеспечивающей сквозную автоматизацию рабочих процессов, формирование баз данных по вопросам деятельности Службы». Таким образом, подрыв информационной безопасности будет

² Сухай Н. Б. Хакерство и киберпреступность : материалы 1-й ежегодной конференции по разработке учебных программ по информационной безопасности. Нью-Йорк, США : АСМ, 2004. С. 128—132.

негативно сказываться на деятельности всей уголовно-исполнительной системы, в частности всех учреждений и органов, исполняющих уголовные наказания.

Служебная информация выступает важным ресурсом, который связан как с управлением исправительным учреждением, так и с обеспечением его безопасности. Информация, выступающая объектом незаконного копирования или иных преступных посягательств, может включать в себя схемы исправительных учреждений, сведения об их силах и средствах, фактическом состоянии охраны и надзора и т.д. Утечка данной информации представляет собой потенциальную угрозу пенитенциарной безопасности в целом и безопасности как персонала, так и осужденных в частности. Подобные сведения в дальнейшем могут быть использованы для совершения тяжких преступлений, таких как побег, захват заложников, посягательство на жизнь сотрудников, массовые беспорядки.

Личная информация о сотрудниках уголовно-исполнительной системы, как и служебная информация, должна охраняться надлежащим образом, чтобы не стать объектом преступных посягательств. В первую очередь речь идет о сведениях, касающихся адреса места жительства, состава семьи, средств передвижения, личной переписки и др. В случае утечки данная информация может быть использована преступниками с целью шантажа, склонения должностного лица к противоправным действиям, связанным с его профессиональной деятельностью, или причинения прямого физического ущерба сотруднику либо его родственникам.

Учитывая изложенное, можно определить, что пенитенциарная киберпреступность — это разновидность преступлений в сфере компьютерной информации, направленных на подрыв информационной безопасности уголовно-исполнительной системы, а также хищение служебной и (или) личной информации сотрудников ФСИН России с целью создания угроз нормальному, стабильному функционированию исправительных учреждений.

Субъектами таких преступлений могут выступать как осужденные, отбывающие наказание в местах лишения свободы, так и сотрудники уголовно-исполнительной системы (внутренняя угроза), а также иные лица (внешняя угроза). Принципиальное отличие внешней и внутренней угроз заключается в том, что в первом случае отсутствует фактический доступ к информации или информационной системе, но отмечается определенный уровень профессионализма в IT-сфере. Во втором случае, напротив, необязательно наличие специальных знаний, они компенсируются фактическим доступом к объектам преступного посягательства.

Внешняя угроза исходит от высококвалифицированных специалистов в области информационных технологий и зависит от уязвимости служебного компьютерного оборудования и локальной компьютерной сети ФСИН России. Самой распространенной внешней угрозой для функционирования информационных систем ФСИН России на сегодняшний день являются сетевые атаки. В частности, их рост отмечался в 2024 г., когда количество DDoS-атак выросло в шесть раз по сравнению с аналогичным периодом 2023 г. Одновременно эксперты отмечали не только количественные, но и качественные изменения в самой тактике сетевых атак, которые становятся более массовыми³.

³ URL: <https://www.myeconomy.ru/tehnologii/chislo-ddos-atak-v-rossii-vyroslo-v-shest-raz-za-dekabr-fevral/> (дата обращения: 05.03.2025).



Также в контексте внешних угроз стоит упомянуть про резонансный случай взлома информационной системы по предоставлению услуг осужденным и их родственникам, с последующим хищением оттуда персональных данных о 800 тыс. лицах, отбывающих наказание⁴. Несмотря на то что данная информационная система не принадлежит ФСИН России, необходимо учитывать мотивы и устремления злоумышленников нанести вред именно органам государственной власти Российской Федерации любыми доступными способами.

Внутренняя угроза связана с наличием фактического доступа злоумышленника к служебной информации. Наличие специальных знаний в области информационных технологий не является определяющим условием совершения подобных преступлений и может быть минимальным. Фактический доступ к служебной информации ФСИН России может быть только у соответствующих сотрудников, согласно их должностным инструкциям. В основном данные преступления, совершаемые непосредственно сотрудниками, имеют коррупционную направленность, так как связаны с передачей служебной информации третьим лицам за денежное или иное нематериальное вознаграждение. Можно предположить, что объектом незаконного копирования выступают персональные данные осужденных, места отбывания наказания и проч. Так, в 2024 г. в отношении сотрудника одного из подразделений ФСИН России возбуждены уголовные дела по ст. 272 «Неправомерный доступ к компьютерной информации» и ст. 290 «Получение взятки» УК РФ⁵.

Следующая категория субъектов пенитенциарных киберпреступлений — лица, отбывающие наказание, т.е. осужденные. Мотивы совершения данных преступлений могут быть различными, но в любом случае их действия направлены на дестабилизацию обстановки в конкретном исправительном учреждении. Вместе с тем необходимо уточнить, что осужденные могут получить доступ к служебной информации либо из-за халатности сотрудников, либо при прямом превышении ими полномочий. В любом случае стоит говорить о необходимости дачи правовой оценки действиям сотрудников при выявлении рассматриваемой категории преступлений.

Так, в ИК-18 УФСИН России по Мурманской области осужденный произвел копирование служебной информации о персональных данных сотрудников, тем самым совершил преступление, предусмотренное ст. 272 УК РФ. Совершение данного преступления стало возможным из-за противоправных действий сотрудника исправительного учреждения, который допустил осужденного к работе на служебном компьютере. В этой связи следственные органы квалифицировали действия сотрудника по ст. 286 «Превышение должностных полномочий» УК РФ⁶.

Наибольшую угрозу пенитенциарной кибербезопасности представляют осужденные, отбывающие наказание за совершение преступлений в сфере информационных технологий. Негативным фактором в первую очередь выступает наличие специальных знаний. Вместе с тем эксперты также говорят о наличии

⁴ URL: <https://edition.cnn.com/> (дата обращения: 05.03.2025).

⁵ URL: <https://smotrim.ru/article/4296198> (дата обращения: 05.03.2025).

⁶ URL: <https://www.murmansk.kp.ru/online/news/6200039/?ysclid=m7w1001vl5538236285> (дата обращения: 05.03.2025).

корыстного мотива в их поведении⁷, что может служить поводом для продолжения преступной деятельности и в местах лишения свободы. В этой связи целесообразно рассмотреть вопрос о введении дополнительного вида профилактического учета данной категории осужденных как склонных к совершению преступлений в сфере высоких технологий.

Совершенные преступления свидетельствуют о наличии недостатков в организации пенитенциарной кибербезопасности. Учитывая разносторонность угроз, профилактика пенитенциарных киберпреступлений должна носить комплексный характер, включать в себя, помимо управленческих мер, уголовно-правовые и научно-технические меры.

Управленческие меры должны предусматривать как подготовку кадров в области обеспечения информационной безопасности, так и их рациональное распределение с учетом наличия угроз. Также к мерам управленческого характера может относиться организация пенитенциарного процесса, исключающего допуск осужденных к информационным системам ФСИН России.

Меры уголовно-правового характера заключаются в первую очередь в рассмотрении вопроса об отдельной квалификации пенитенциарных киберпреступлений и дополнительной ответственности для сотрудников, ответственных за доступ к служебной информации.

Учитывая общую негативную тенденцию развития киберпреступности, ужесточение уголовной политики в данной области является действенной превентивной мерой. Так, в конце 2024 г. введена уголовная ответственность за незаконные использование и (или) передачу, сбор и (или) хранение компьютерной информации, содержащей персональные данные, а равно создание и (или) обеспечение функционирования информационных ресурсов, предназначенных для ее незаконных хранения и (или) распространения (ст. 272¹ УК РФ). По мнению экспертов, это «позволит результативнее противостоять их (персональных данных. — Н. Е.) утечке».⁸

Научно-технические меры — это разработка и внедрение программного обеспечения и оборудования, способного обеспечить безопасность информационных систем как от внешних, так и от внутренних угроз.

БИБЛИОГРАФИЯ

1. Мочалкина И. С. Характеристика личности осужденных, совершивших преступление в сфере высоких технологий // Российская правовая система: в поисках национальной идентичности : сборник докладов XIV Московской юридической недели : в 6 ч. — М., 2025.
2. Сухай Н. Б. Хакерство и киберпреступность : материалы 1-й ежегодной конференции по разработке учебных программ по информационной безопасности. — Нью-Йорк, США : ACM, 2004. — С. 128—132.

⁷ Мочалкина И. С. Характеристика личности осужденных, совершивших преступление в сфере высоких технологий // Российская правовая система: в поисках национальной идентичности : сборник докладов XIV Московской юридической недели : в 6 ч. М., 2025. С. 360.

⁸ Выступление Владимира Колокольцева на расширенном заседании коллегии МВД России // URL: <https://xn--b1aew.xn--p1ai/news/item/62189090> (дата обращения: 07.03.2025).





**Андрей Викторович
БОРИСОВ,**

доцент кафедры
уголовного права
Военного университета
имени князя
Александра Невского
Министерства
обороны РФ,
доктор юридических наук,
доцент
av-borisov@mail.ru
123001, Россия, г. Москва,
ул. Большая Садовая,
д. 14, стр. 1

Киберпреступность на транспорте: состояние и тенденции

Аннотация. В статье проводится анализ криминологической характеристики киберпреступности на транспорте, рассматривается ее состояние и тенденции ее развития. В контексте глобализации ИКТ стали неотъемлемым элементом функционирования общества, включая транспортную инфраструктуру. Вместе с тем использование ИКТ в транспортной сфере порождает новые вызовы и угрозы, в том числе криминального характера. Данный тезис подтверждается результатами многочисленных исследований, проведенных как отечественными, так и зарубежными специалистами в области кибербезопасности и криминологии. Современные киберугрозы, направленные на обеспечение транспортной безопасности Российской Федерации, требуют комплексного и всестороннего анализа. В связи с этим автором статьи предпринята попытка определения количественных и качественных параметров киберпреступности в транспортной сфере, а также выявления основных тенденций ее развития. В рамках исследования проведен анализ положений криминологических работ, посвященных как теоретическим аспектам противодействия киберпреступности, так и практическим вопросам обеспечения транспортной безопасности. Кроме того, была изучена ведомственная статистическая отчетность Министерства внутренних дел Российской Федерации за период с 2018 по 2024 г.

Ключевые слова: транспортная преступность, транспортная безопасность, киберпреступность, киберпреступность на транспорте, состояние киберпреступности на транспорте, показатели киберпреступности на транспорте, тенденции киберпреступности на транспорте

DOI: 10.17803/2311-5998.2025.129.5.214-220

Andrey V. BORISOV,

Associate Professor of the Department of Criminal Law
of the Military University named after the Prince Alexander Nevsky
of the Ministry of Defense,

Dr. Sci. (Law), Associate Professor
av-borisov@mail.ru

14/1, ul. Bolshaya Sadovaya, Moscow, Russia, 123001

Cybercrime in Transport: Status and Trends

Abstract. The article is devoted to the criminological characteristics of cybercrime in transport, its state and trends of its development are considered. One of the significant factors influencing the formation and development of

the digital economy in the Russian Federation is the active introduction of advanced information and telecommunication technologies (hereinafter — ICT) into various sectors of activity. In the context of globalization, ICTs have become an integral part of the functioning of society, including transport infrastructure. At the same time, the use of ICT in the transport sector generates new challenges and threats, including criminal ones. This thesis is supported by the results of numerous studies conducted by both domestic and foreign experts in the field of cybersecurity and criminology. Modern cyber threats aimed at ensuring the transport security of the Russian Federation require a comprehensive and comprehensive analysis. In this regard, the author of the article attempts to determine the quantitative and qualitative characteristics of cybercrime in the transport sector, as well as to identify the main trends in its development. The study analyzes the provisions of criminological works devoted to both theoretical aspects of countering cybercrime and practical issues of ensuring transport security. In addition, the departmental statistical reports of the Ministry of Internal Affairs of the Russian Federation for the period from 2018 to 2024 were studied.

Keywords: *transport crime, transport security, cybercrime, cybercrime in transport, the state of cybercrime in transport, indicators of cybercrime in transport, trends in cybercrime in transport*

Транспорт является фундаментальным элементом экономической и инфраструктурной системы государства. Он обеспечивает оптимизацию управления потоками материальных и нематериальных ресурсов, способствуя доступности отдаленных территорий и концентрации населения в ключевых местностях. Транспортные системы играют значительную роль в активизации экономического роста и выступают стимулятором повышения уровня жизни населения страны. Тем не менее их работа сопряжена с рядом сложных проблем и опасностей. Среди них можно выделить техногенные катастрофы, дорожно-транспортные происшествия, антропогенные катастрофы, загрязнение окружающей среды вредными веществами, повышенный уровень шумового загрязнения, потенциальные угрозы общественной безопасности, включая террористические акты и преступления против личности и собственности¹.

Комплексный анализ криминогенной ситуации в транспортной сфере включает исследование как традиционных преступных деяний, свойственных данной области, так и проблем, связанных с киберпреступностью, которая демонстрирует волнообразную динамику в рассматриваемый период. Согласно официальным данным статистического учета, в 2024 г. было зарегистрировано 6 502 случая киберпреступлений, что на 4,9 % меньше по сравнению с прошлым годом². Несмотря на снижение количества киберпреступлений, отмечается увеличение их

¹ Борисов А. В. Состояние и тенденции преступности на отдельных видах транспорта // Вестник Московской академии Следственного комитета РФ. 2024. № 3 (41). С. 37—44.

² Борисов А. В. Криминологическая профилактика транспортной преступности // Вестник Академии права и управления. 2019. № 2 (55). С. 30—34.





Рис. 1. Динамика и доля киберпреступлений, совершенных на транспорте в Российской Федерации в 2018—2024 гг.³



Рис. 2. Структура (по степени тяжести) киберпреступлений, совершенных на транспорте в Российской Федерации в 2018—2024 гг.

доли в структуре транспортной преступности, которая достигла максимальных значений в рассматриваемый период и составила 22,24 % (рис. 1).

Снижение числа киберпреступлений на транспорте можно объяснить несколькими ключевыми факторами:

— во-первых, разработкой и внедрением комплексных систем киберзащиты, обеспечивающих высокий уровень резистентности к кибератакам. Такие системы минимизируют потенциальные потери от инцидентов и гарантируют способность транспортной организации адекватно реагировать на будущие вызовы в сфере информационной безопасности;

— во-вторых, организацией систематического обучения сотрудников и повышением их осведомленности о новейших методах атак, основанных на социальной инженерии. Это включает в себя анализ поведенческих паттернов злоумышленников и разработку соответствующих контрмер;

— в-третьих, интеграцией механизмов кибербезопасности во все используемые организацией информационные сервисы и продукты. Это предполагает внедрение стандартов информационной безопасности на всех этапах разработки и эксплуатации систем;

— в-четвертых, внедрением и поддержанием процессов управления уязвимостями, включая регулярное обновление систем безопасности и мониторинг потенциальных угроз, что, в свою очередь, позволяет оперативно идентифицировать и устранять слабые места в защите⁴.

В 2024 г. в общей массе киберпреступлений, регистрируемых на транспорте, преобладают особо тяжкие деяния. Их удельный вес составляет 48,95 %. Наблюдается тенденция к снижению количества киберпреступлений на транспорте по всем категориям преступных деяний (рис. 2).

³ В статистических формах ГИАЦ МВД России сведения о большинстве киберпреступлений, в том числе совершаемых на транспорте, выделяются с 2018 г. Здесь и далее использовалась форма ведомственной статистической отчетности № 494 «Сведения о состоянии преступности и результатах расследования преступлений» за 2018—2024 гг.

⁴ Борисов А. В. Состояние и основные тенденции развития преступности на объектах транспорта Российской Федерации // Расследование преступлений: проблемы и пути их решения. 2019. № 2 (24). С. 42—49.

В перечне часто встречающихся киберпреступлений, совершенных на объектах транспортной инфраструктуры в 2024 г., выделяются следующие виды: кражи — 294, разнообразные виды мошенничества — 494, а также преступные деяния, связанные с незаконным оборотом наркотических средств — 4 922.

Киберпреступления в транспортной сфере совершались в 2024 г. следующими основными способами: использование информационно-телекоммуникационной сети Интернет — 5 964 деяния (91,73 %); применение средств мобильной связи — 2 161 деяние (33,24 %); использование программных средств — 1 147 (17,64 %); применение платежных инструментов в виде расчетных (пластиковых) карт — 386 (5,93 %); использование компьютерной техники — 246 (3,78 %); осуществление фиктивных электронных платежей — 20 деяний (0,31 %).

Внедрение информационных технологий в транспортную отрасль способствует значительному повышению эффективности функционирования транспортных систем. Это выражается в оптимизации процессов управления, снижении временных и ресурсных затрат, а также в повышении общей производительности транспортных систем. Кроме того, внедрение информационных технологий открывает новые перспективы для всех участников и пользователей в транспортной отрасли, способствуя инновациям и развитию.

Научные исследования, посвященные применению кибертехнологий в транспортной сфере, направлены на унификацию процессов обработки и транспортировки грузов и пассажиров. В рамках этих исследований разрабатываются алгоритмы и системы, обеспечивающие оптимизацию логистических цепочек и повышение безопасности перевозок⁵. Кроме того, ведется работа по созданию единых международных стандартов уровня шума в различных странах. В то же время разрабатывается и внедряется система законов и правил, которые регулируют использование беспилотных транспортных средств. Это создает основу для широкого применения не только автономных наземных транспортных средств, таких как автомобили и электропоезда, но и более компактных и специализированных беспилотных летательных аппаратов.

Современные беспилотные транспортные системы, включая воздушные, наземные и водные, представляют собой передовые технологии, обладающие значительным потенциалом для применения в различных сферах, однако они также сопряжены со следующими потенциальными рисками и угрозами для транспортной безопасности:

- 1) уязвимость к кибератакам. Беспилотные транспортные средства, не оснащенные адекватными средствами киберзащиты, могут стать целями для злоумышленников. Возможность несанкционированного доступа к управлению такими системами создает риски их использования в террористических или иных преступных целях;
- 2) риски, связанные с отказом оборудования. Сбои в работе ключевых компонентов беспилотных транспортных систем могут привести к их неконтролируемому поведению, что представляет угрозу для жизни и здоровья людей, а также для инфраструктуры;

⁵ *Варыгин А. Н.* Особенности преступности на железнодорожном транспорте // Проблемы правоохранительной деятельности. 2017. № 3. С. 62—65.



3) нарушение воздушного пространства. Беспилотные летательные аппараты могут проникать в контролируемые зоны воздушного пространства, создавая потенциальные помехи для полетов пилотируемых воздушных судов. Это может угрожать безопасности воздушного движения и приводить к нарушению установленных процедур и регламентов.

В современных условиях беспилотные транспортные средства (БТС) являются значимым компонентом киберпространства и вносят существенный вклад в формирование актуальных киберугроз. Интеграция БТС в транспортные системы требует комплексного подхода к обеспечению безопасности и киберзащиты⁶.

Особую опасность представляет несанкционированный запуск беспилотных летательных аппаратов в непосредственной близости от авиационных объектов, таких как аэродромы, вертодромы и посадочные площадки. Подобные инциденты могут привести к нарушению процедур обеспечения безопасности полетов, а также вызвать угрозу жизни и здоровью людей. Кроме того, возможны повреждения объектов транспортной инфраструктуры.

В подавляющем большинстве случаев нарушения использования воздушного пространства совершаются владельцами беспилотных летательных аппаратов с взлетной массой, не превышающей 30 килограммов. Такие аппараты, как правило, применяются в личных целях.

Основные причины данных нарушений включают:

- недостаток осведомленности о нормативных правовых актах, регулирующих использование воздушного пространства Российской Федерации;
- недооценка потенциальных рисков и опасностей, ассоциированных с эксплуатацией беспилотных летательных аппаратов;
- отсутствие обязательной регистрации воздушных судов в соответствии с действующими законодательными актами, а также отсутствие надлежащих сертификатов, подтверждающих соответствие эксплуатантов и воздушных судов требованиям к летной годности, создает значительные риски для обеспечения безопасности полетов.

В настоящее время беспилотные летательные аппараты, производимые такими крупными компаниями, как DJI и Parrot, оснащены системами, ограничивающими их полеты в зонах с высокой аэронавигационной активностью, например, над аэродромами. Однако киберпреступниками разработаны методы обхода данных ограничительных систем.

После начала специальной военной операции на территории Украины была проведена продуктивная работа по внесению изменений в нормативные правовые акты, регламентирующие порядок использования воздушного пространства Российской Федерации, и по использованию беспилотных летательных аппаратов. В ходе СВО стало очевидно, насколько значимой и необходимой является такая деятельность. В рамках СВО противник активно использует беспилотные летательные и надводные аппараты для атак на объекты транспортной инфраструктуры Российской Федерации. Так, в Севастополе 29.10.2022 была совершена

⁶ Коимшиди Г. Ф., Саркисян А. Ж. Прогноз динамики преступности в Российской Федерации на 2020 год // Вестник Академии Следственного комитета Российской Федерации. 2020. № 1 (23). С. 68—77.

атака на военные корабли Черноморского флота и гражданские суда с использованием надводных беспилотных аппаратов. Согласно информации Министерства обороны РФ, теракт был организован 73-м специальным центром морских операций Вооруженных сил Украины. 02.11.2022 Президент Украины Владимир Зеленский заявил о своем намерении создать флот морских беспилотных аппаратов⁷.

Результатом работы по противодействию беспилотным летательным и надводным аппаратам стало принятие Федерального закона от 04.08.2023 № 440-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации»⁸, который расширил круг субъектов противодействия беспилотным летательным и надводным аппаратам и наделил их соответствующими полномочиями.

Применение беспилотных летательных аппаратов в противоправных целях является серьезной угрозой для общественной безопасности и государственного устройства. Данные устройства могут быть задействованы для осуществления террористических атак на объекты транспортной инфраструктуры (что, собственно, активно и происходит в период проведения СВО), незаконного оборота оружия, включая его компоненты и боеприпасы, а также для перевозки отравляющих веществ.

Кроме того, БПЛА могут использоваться для сбора и передачи информации. Развитие информационных технологий, в том числе применение БПЛА, привело к возникновению новых форм терроризма, таких как кибертерроризм и биотерроризм. В соответствии с приказом Минтранса России № 52, ФСБ России № 112, МВД России № 134 от 05.03.2010 «Об утверждении Перечня потенциальных угроз совершения актов незаконного вмешательства в деятельность объектов транспортной инфраструктуры и транспортных средств», угрозы террористического характера классифицируются как потенциальные угрозы, способные привести к актам незаконного вмешательства в деятельность указанных объектов⁹.

Беспилотный транспорт является многообещающим вектором развития транспортной отрасли. Однако для успешной интеграции беспилотных транспортных средств необходима комплексная модернизация дорожно-транспортной и информационно-телекоммуникационной инфраструктуры. Эта инфраструктура должна предоставлять беспилотным транспортным средствам актуальные данные и обеспечивать функционирование необходимых сервисов. Вместе с тем научные исследования указывают на потенциальные риски, связанные с внедрением интеллектуальных транспортных систем. Эти угрозы связаны с наличием уязвимостей в программном обеспечении и в каналах передачи данных. Наличие таких уязвимостей может создать условия для осуществления потенциальных кибератак на транспортные системы.

Таким образом, анализ статистических данных о зарегистрированных преступных деяниях, совершенных с использованием информационно-телекоммуникационных

⁷ Проект федерального закона № 323987-8 «О внесении изменений в отдельные законодательные акты Российской Федерации» (ред., внесенная в Государственную Думу, текст по состоянию на 28.03.2023) // СПС КонсультантПлюс.

⁸ Российская газета. 09.08.2023. № 175.

⁹ Диканова Т. А. О состоянии преступности на железнодорожном, водном и воздушном транспорте в 2015—2019 гг. // Транспортное право и безопасность. 2020. № 2 (34). С. 84—99.



технологий на транспорте, позволяет сделать определенные выводы. Исследование показывает, что уровень киберпреступности в рассматриваемой сфере подвержен волнообразной динамике.

В структуре киберпреступности на транспорте в 2024 г. доминировали особо тяжкие преступные деяния. Их доля составила 48,95 %. С использованием информационно-телекоммуникационных технологий на транспорте совершались преступные деяния, связанные с незаконным оборотом наркотиков (4 922), различные виды мошенничества (494) и кражи (294). Характерными способами совершения киберпреступлений на транспорте стали использование сети Интернет — 5 964 преступления (91,73 %), использование мобильной связи — 2 161 (33,24 %), применение программных средств — 1 147 преступлений (17,64 %).

БИБЛИОГРАФИЯ

1. *Борисов А. В.* Криминологическая профилактика транспортной преступности // Вестник Академии права и управления. — 2019. — № 2 (55). — С. 30—34.
2. *Борисов А. В.* Состояние и основные тенденции развития преступности на объектах транспорта Российской Федерации // Расследование преступлений: проблемы и пути их решения. — 2019. — № 2 (24). — С. 42—49.
3. *Борисов А. В.* Состояние и тенденции преступности на отдельных видах транспорта // Вестник Московской академии Следственного комитета Российской Федерации. — 2020. — № 1. — С. 43—51.
4. *Борисов А. В.* Состояние и тенденции преступности на отдельных видах транспорта // Вестник Московской академии Следственного комитета Российской Федерации. — 2024. — № 3 (41). — С. 37—44.
5. *Варыгин А. Н.* Особенности преступности на железнодорожном транспорте // Проблемы правоохранительной деятельности. — 2017. — № 3. — С. 62—65.
6. *Диканова Т. А.* О состоянии преступности на железнодорожном, водном и воздушном транспорте в 2015—2019 годах // Транспортное право и безопасность. — 2020. — № 2 (34). — С. 84—99.
7. *Коимшиди Г. Ф., Саркисян А. Ж.* Прогноз динамики преступности в Российской Федерации на 2020 год // Вестник Академии Следственного комитета Российской Федерации. — 2020. — № 1 (23). — С. 68—77.
8. Официальная статистика Министерства внутренних дел Российской Федерации // URL: <https://xn--b1aew.xn--p1ai/reports> (дата обращения: 30.03.2025).
9. Промышленный интернет вещей : доклад. — М. : Агентство промышленного развития Москвы, 2020.

Применение технологии искусственного интеллекта для оценки исправления осужденных при досрочном освобождении от наказания

Аннотация. Технология искусственного интеллекта все больше проникает в различные сферы современной жизни и вызывает острые дискуссии о возможности ее применения при осуществлении правосудия. В работе анализируются позиции сторонников и противников применения искусственного интеллекта непосредственно в роли судьи и особенно при принятии оценочных решений при разрешении вопросов условно-досрочного освобождения или замены неотбытой части наказания более мягким видом наказания. Анализ результатов тестирования нейросети GigaChat показал, что искусственный интеллект не способен брать ответственность при принятии решения об удовлетворении или отказе в удовлетворении ходатайств об условно-досрочном освобождении, однако способен к структурированию положительных и отрицательных критериев, характеризующих поведение осужденного, которые могут оказывать влияние на решение суда. Искусственный интеллект, сравнивая профессионально значимые качества судьи-человека и ИИ-судьи, отдает предпочтение человеку, поскольку он обладает уникальными характеристиками, не свойственными для технологии. Результаты работы могут быть использованы для осмысления рисков формально-механической замены человека в системе правосудия.

Ключевые слова: осужденный, исправление, условно-досрочное освобождение, искусственный интеллект, правосудие, наказание, поведение осужденного, нейросеть, IT-технология



**Елена Эдуардовна
ПОПОВА,**
профессор кафедры
уголовного права
Российского
государственного
университета
правосудия имени
В. М. Лебедева,
профессор кафедры
уголовно-правовых
дисциплин
Международного
юридического института,
доктор юридических наук,
доцент
kup@rsuj.ru
117418, Россия, г. Москва,
ул. Новочеремушкинская,
д. 69

DOI: 10.17803/2311-5998.2025.129.5.221-227

Elena E. POPOVA,

Professor of the Department of Criminal Law
of the Russian State University of Justice named after V. M. Lebedev,
Professor of the Department of Criminal Law Disciplines
International Law Institute,
Dr. Sci. (Law), Associate Professor
kup@rsuj.ru

69, ul. Novocheremushkinskaya, Moscow, Russia, 117418

Application of Artificial Intelligence Technology to Assess the Correction of Convicts on Early Release from Punishment

Abstract. Artificial intelligence technology is increasingly penetrating into various spheres of modern life and causes heated discussions about the possibility of its use in the administration of justice. The paper analyzes the positions of supporters and opponents of the use of artificial intelligence directly in the role of a judge and especially when making evaluative decisions when resolving issues of conditional early release or replacing the unserved part of the sentence with a milder type of punishment. Analysis of the results testing the GigaChat neural network showed that artificial intelligence is not able to take responsibility when deciding whether to grant or refuse to grant parole requests, but it is capable of structuring positive and negative criteria that characterize the behavior of the convict, and which can influence the court's decision. Artificial intelligence, comparing the professionally significant qualities of a human judge and an AI judge, gives preference to a human, since he has unique characteristics that are not typical for technology.
Keywords: convict, correction, parole, artificial intelligence, justice, punishment, convict behavior, neural network, IT technology

В нашу жизнь прочно вошли IT-технологии, которые завоевывают новые и новые сферы (транспорт, образование, услуги и т.д.). Не является исключением и сфера правосудия. Вопросы применения технологии искусственного интеллекта в судебной практике вызывают острые дискуссии как среди судей, так и в научной среде.

Сторонники активного применения искусственного интеллекта в судебной деятельности обосновывают свою позицию возможностью совершенствования различных рутинных процессов, документирования, быстрой обработки огромного массива информации и т.п. При этом, отмечают ученые, «машина всегда будет оставаться объективной, беспристрастной и сохранять нейтралитет, имея безупречную репутацию. С этой точки зрения роботы могут стать практически идеальными судьями»¹. Кроме того, по мнению И. Н. Глебова, «искусственный

¹ Коваленко К. Е., Печатнова Ю. В., Стаценко Д. А., Коваленко Н. Е. Судья-робот как преодоление противоречий судебного усмотрения (юридические аспекты) // Юридический вестник Дагестанского государственного университета. 2020. Т. 36. № 4. С. 171.

интеллект в киберпространстве может вершить правосудие по простым и ясным процессуальным правилам, в режиме профессиональных диалогов с применением всей оцифрованной мудрости общепризнанных авторитетов юридической науки и практики»².

Оппоненты такой позиции обоснованно обращают внимание, что искусственный интеллект как инстанцию, решающую судьбы людей, общество принять не готово, поскольку не исключает с его стороны судебных ошибок, дискриминационного аспекта, несоблюдения прозрачности и подотчетности в принятии решений и представлении результатов, попрания свободы воли человека, проблем субординации между судьей-человеком и ИИ-судьей, ущемления моральных, религиозных ценностей и достоинства граждан и др.³

Вполне оправданно ученые придерживаются позиции, что недопустимо подменять интеллектуальную деятельность судьи-человека искусственным интеллектом, «поскольку любое решение будет основано на использовании машины определенной программы, созданной для принятия решения, при этом за ее качество создатели не смогут нести ответственность, поскольку просчитать возможности искусственного интеллекта, связанные с собственным перепрограммированием, весьма проблематично»⁴.

Вместе с тем технология «искусственного интеллекта» все более прочно входит в сферу правосудия. Применяются на практике такие системы, как ГАС «Правосудие», «Мой Арбитр», видео-конференц-связь и т.д. В постановлении X Всероссийского съезда судей № 1 от 01.12.2022 отмечается, что в деятельности судебной системы «в условиях технического прогресса речь идет не только об интеграции в судебную деятельность электронных баз данных и сервисов подачи обращений в суд, которые уже успешно используются в судах. В настоящее время встает вопрос об использовании систем искусственного интеллекта, принимающего на себя обширную часть аналитической работы судьи. Съезд, не отрицая использования его отдельных элементов в судопроизводстве и дальнейшего развития в этой части процессуального законодательства, исходит из невозможности полной замены судьи искусственным интеллектом. Ряд оценочных категорий, таких как справедливость, соразмерность и т.д., не могут быть доверены компьютерному алгоритму»⁵.

К вопросам принятия оценочных решений относятся применение условно-досрочного освобождения к осужденным или замена неотбытой части наказания более мягким видом наказания.

² Глебов И. Н. Искусственный интеллект // URL: <https://humanlaw.ru/9-article/26-artificial-intelligence.html> (дата обращения: 20.03.2025).

³ Гаспарян Д. Э., Стырин Е. М. Прикладные проблемы внедрения этики искусственного интеллекта в России: отраслевой анализ и судебная система. М. : ИД Высшей школы экономики, 2020. С. 23—24.

⁴ Татьяна Л. Г., Решетнева Т. В., Решетникова Г. А. Принципы правосудия как правовые барьеры ограничения деятельности искусственного интеллекта // Юридический вестник Кубанского государственного университета. 2023. № 4 (15). С. 99.

⁵ Постановление X Всероссийского съезда судей от 01.12.2022 № 1 «О развитии судебной системы Российской Федерации» // СПС «КонсультантПлюс».



Законодательное определение «исправление осужденных» закреплено в ст. 9 Уголовно-исполнительного кодекса РФ, где определяются критерии, формирующие изменение личности осужденного в их процессном выражении. УИК РФ не определяет конкретные критерии исправления осужденных как результат такой деятельности, а закладывает базовую основу для их понимания и применения в процессе исполнения наказания, а также исправительного воздействия на осужденных.

Вместе с тем именно оценка степени изменения личности в социально-позитивную сторону выступает принципиальной категорией, на которой базируется решение об удовлетворении или отказе в нем при рассмотрении ходатайства о досрочном освобождении.

Постановление Пленума Верховного Суда РФ «О судебной практике условно-досрочного освобождения от отбывания наказания, замены неотбытой части наказания более мягким видом наказания» устанавливает обязательный индивидуальный подход к каждому осужденному при решении вопроса о возможности применения указанных досрочных видов освобождения (п. 1). При этом обращается внимание на тот факт, что основной оценочной категорией выступает поведение осужденного, а также обязательно учитывается вся совокупность данных о личности осужденного, его отношение к труду и учебе во время отбывания наказания (п. 4).

Попробуем разобраться в возможностях нейросети⁶ при оценке исправления осужденного. Перед нейросетью был поставлен вопрос: «Может ли технология искусственного интеллекта обеспечить индивидуальный подход при оценке исправления осужденного?» Нейросеть, оценивая свои возможности в этом вопросе, не дала однозначного ответа. Она указала на наличие потенциальной способности оказать помощь судам в обеспечении индивидуального подхода при оценке исправления осужденных, но тут же добавила, что использование технологии искусственного интеллекта требует тщательной проработки и осторожного подхода. Вместе с тем нейросеть обратила внимание на положительные факторы, где ее использование может быть оправданным при оказании помощи суду или сотруднику уголовно-исполнительной системы для определения готовности осужденных к условно-досрочному освобождению или замене неотбытой части наказания более мягким видом наказания.

Так, нейросеть выделила следующие разделы, где она видит возможность своего применения:

«1. **Анализ большого объема данных.** ИИ способен обрабатывать большие объемы данных о поведении осужденного, включая историю его правонарушений, результаты психологической оценки, медицинские заключения и другие факторы. Это позволяет создать более полную картину состояния осужденного и учесть множество нюансов, которые могут быть упущены при ручном анализе.

2. **Прогнозирование риска рецидива.** Некоторые модели электронных программ могут анализировать совокупность данных и прогнозировать вероятность повторного совершения преступления осужденным. Эти прогнозы могут

⁶ В процессе проводимого исследования использовалась русскоязычная нейросеть от «Сбера» (GigaChat // URL: <https://gigs.chat>).

использоваться судами для принятия решений о виде наказания или условий условно-досрочного освобождения.

3. Автоматизация административных процессов. Использование ИИ может ускорить обработку заявлений и ходатайств осужденных, автоматизировать некоторые этапы рассмотрения дел, например сбор и анализ характеристик, что позволит сократить время на принятие решений.

4. Поддержка судей в принятии решений. ИИ может представлять судьям аналитическую поддержку, предлагая рекомендации на основе анализа данных и моделей, что поможет судьям лучше понять содержание дела и учесть большее количество факторов при вынесении решений».

Объективности ради необходимо отметить, что нейросеть довольно критично отнеслась к своим возможностям и выделила ряд факторов, которые могут негативно сказаться на ее применении. К таким факторам нейросеть отнесла: **«этические соображения:** использование алгоритмов для принятия решений, касающихся человеческой жизни и свободы, вызывает серьезные этические опасения. Необходимо убедиться, что ИИ не усиливает предвзятость и дискриминацию, которые могут возникать с учетом тех или иных особенностей; **объяснимость решений:** алгоритмы ИИ часто работают как “черные ящики”, что затрудняет понимание, почему именно было принято конкретное решение. Для судебных процессов важны прозрачность и объяснимость, поэтому потребуются разработка интерпретируемых моделей ИИ; **данные и точность:** совокупность данных может быть неполной или искаженной, что повлияет на точность прогноза и рекомендаций ИИ. Также важно постоянно обновлять модели, чтобы они соответствовали текущим реалиям; **правовые барьеры:** законодательство многих стран ограничивает использование автоматизированных систем для принятия юридически значимых решений, требуя человеческой оценки и проверки».

Далее нейросети было предложено проанализировать возможность применения условно-досрочного освобождения к осужденным на основе описания вынесенных судебных решений, имеющихся в открытом доступе СПС «КонсультантПлюс»⁷ с использованием метода случайной выборки. Нейросеть структурно выделила основные аргументы в пользу применения условно-досрочного освобождения. К ним она отнесла: отсутствие взысканий, наличие поощрений, активное участие в мероприятиях, положительное отношение к окружающим, признание вины, поддержку социальных связей, отсутствие ущерба по приговору суда, привлечение к труду, образование и профессиональную подготовку, участие в общественной жизни колонии, отсутствие конфликтов и нарушений режима. Также ею были выделены и негативные факторы, которые могут повлиять на оценку степени исправления осужденных: отсутствие стабильности в поведении осужденного, что может вызвать сомнения в устойчивости исправления; отсутствие поощрений от администрации колонии, что может свидетельствовать о недостаточной активности осужденного в исправительных мероприятиях, необходимости дополнительного контроля за поведением осужденного.

Нейросеть не представила точного определенного вывода о возможности или невозможности применения условно-досрочного освобождения или замены

⁷ Все данные обезличены.



неотбытой части наказания более мягким видом наказания. Ее вывод основывается на заключении, что поведение осужденного «соответствует требованиям законодательства для **рассмотрения** (здесь и далее выделения мои. — Е. П.) вопроса об условно-досрочном освобождении. Суд, **скорее всего**, учтет положительные стороны его поведения и примет решение в пользу условно-досрочного освобождения, **если сочтет**, что осужденный действительно исправился, не представляет угрозы обществу и готов к возвращению в общество. **Окончательное решение остается за судом, который оценивает совокупность всех факторов**».

Как видно, нейросеть не способна брать на себя ответственность в части вынесения решения на основе оценочных данных вместо судьи-человека. Кроме того, нейросети был задан вопрос: «Какие основные характеристики отличают судью-человека от ИИ-судьи?» В ответе нейросети обращают на себя внимание сравнительные характеристики таких ключевых аспектов, как:

«Эмоциональная составляющая. **Человек**: Судья-человек обладает эмоциями и может учитывать эмоциональные аспекты дела, такие как сострадание, эмпатия и справедливость. Это иногда помогает принимать взвешенные решения, основанные на интуиции и личном опыте. **ИИ**: Искусственный интеллект лишен эмоций и действует исключительно на основе данных и алгоритмов. Он не способен испытывать сочувствие и принимать решения, основываясь на субъективных оценках.

Адаптация к новым обстоятельствам. **Человек**: Человек способен адаптироваться к меняющимся условиям и новым обстоятельствам, принимая во внимание уникальные особенности каждого случая. Это делает процесс принятия решений гибким и открытым к изменениям. **ИИ**: ИИ ограничен рамками своих программных кодов и данных, на которых он обучен. Новые ситуации или нестандартные случаи могут вызвать трудности в интерпретации, если они не предусмотрены алгоритмами.

Ответственность. **Человек**: За действия судьи-человека несет ответственность сам человек, что создает стимулы для добросовестного выполнения обязанностей и стремления к справедливости. **ИИ**: Вопрос ответственности за решения ИИ остается сложным. Кто будет нести ответственность в случае ошибочного решения — разработчик программы, оператор или еще кто-то?

Прозрачность и понятность решений. **Человек**: Человеческие решения обычно легче объяснить и обосновать, так как они базируются на логике и опыте, которые можно обсудить и оспорить. **ИИ**: Решения ИИ могут быть менее понятны, особенно если используются сложные нейросетевые модели. Требуются специальные методы для объяснения решений ИИ, что может усложнять процесс.

Возможность ошибок. **Человек**: Люди склонны совершать ошибки, особенно в сложных ситуациях, когда приходится учитывать различные факторы. Однако ошибки людей легко выявить и исправить. **ИИ**: Ошибки ИИ тоже возможны, особенно если модель плохо обучена или используется некорректно. Они могут быть трудноуловимы и иметь далеко идущие последствия».

Как видно из сравнительного анализа качественных характеристик судьи-человека и ИИ-судьи, проведенного нейросетью, положительными качествами в части принятия оценочного решения в большей степени обладает человек. Человеку

свойственны такие уникальные качества, как способность к сопереживанию, интуитивное понимание сущности проблемы и способность адаптироваться к новым ситуациям, гибкость в принятии решений, что делает его незаменимым в юридической системе.

Как следует из проведенного исследования, применение технологии искусственного интеллекта имеет как положительные, так и отрицательные стороны. Нейросеть способна освободить человека от выполнения формальной, рутинной работы либо оказать помощь в анализе большого массива информации, что будет способствовать быстрому решению других, более важных задач, в том числе в сфере осуществления правосудия.

Кроме того, при решении вопросов социальной адаптации и реинтеграции освобождаемого от наказания лица нейросеть вполне может:

- спрогнозировать вероятность его трудоустройства с учетом наличия потребностей и вакансий в регионе и соотнести это с наличием или отсутствием у него профессии или специальности;
- выявить риск повторного совершения преступления на основе имеющихся данных психолого-воспитательной работы, проводимой с осужденным, наличия или отсутствия социальных и семейных связей и (или) поддержки;
- просчитать возможный потенциал освобождаемого для его реинтеграции в общество и определить наличие или отсутствие при этом определенных рисков, дать рекомендации по их снижению.

Вместе с тем анализ взаимодействия с искусственным интеллектом на профессиональном уровне показал, что он не может заменить человека в принятии оценочных решений, которые основываются на совокупности уникальных качественных характеристик, свойственных только человеку, ими не обладает никакая технология, что было подтверждено и нейросетью.

БИБЛИОГРАФИЯ

1. Гаспарян Д. Э., Стырин Е. М. Прикладные проблемы внедрения этики искусственного интеллекта в России: отраслевой анализ и судебная система. — М. : ИД Высшей школы экономики, 2020. — 112 с.
2. Глебов И. Н. Искусственный интеллект // URL: <https://humanlaw.ru/9-article/26-artificial-intelligence.html>.
3. Коваленко К. Е., Печатнова Ю. В., Стаценко Д. А., Коваленко Н. Е. Судья-робот как преодоление противоречий судебного усмотрения (юридические аспекты) // Юридический вестник Дагестанского государственного университета. — 2020. — Т. 36. — № 4. — С. 169—173.
4. Татьяна Л. Г., Решетнева Т. В., Решетникова Г. А. Принципы правосудия как правовые барьеры ограничения деятельности искусственного интеллекта // Юридический вестник Кубанского государственного университета. — 2023. — № 4 (15). — С. 90—101.





Юлия Викторовна

БЫСТРОВА,

заведующий кафедрой
уголовного процесса
и прокурорского надзора

Орловского

государственного

университета имени

И. С. Тургенева,

доктор юридических наук,

доцент

zukova57@mail.ru

302010, Россия, г. Орел,

ул. Комсомольская, д. 95

Киберпреступность в отношении несовершеннолетних: причины и направления предупреждения

Аннотация. Проблема предупреждения киберпреступности в отношении несовершеннолетних носит международный характер. В настоящее время наблюдается как рост рассматриваемой преступности, так и изменение ее структуры. Появление новых форм киберпреступности в отношении несовершеннолетних, таких как кибербуллинг, кибермошенничество, свидетельствует о развитии данного вида преступности. Проблемы снижения уровня киберпреступности в отношении несовершеннолетних должны быть решены в ближайшей перспективе путем внесения изменений в уголовное законодательство. В рамках правоприменительной деятельности должны быть выработаны эффективные рекомендации по нейтрализации деструктивного воздействия на ребенка в виртуальном пространстве. Данные количественные и качественные изменения рассматриваемой преступности требуют серьезных изменений. Правильное определение причинного комплекса киберпреступности в отношении несовершеннолетних позволит выработать эффективные меры противодействия киберпреступности в отношении несовершеннолетних. Статья посвящена анализу и систематизации причин рассматриваемой преступности и выработанных на этой основе предложений по ее предупреждению.

Ключевые слова: киберпространство, виртуальное пространство, киберпреступность, несовершеннолетняя кибержертва, уголовная ответственность, предупреждение

DOI: 10.17803/2311-5998.2025.129.5.228-233

Yulia V. BYSTROVA,

Head of the Department of Criminal Procedure and Prosecutor's Supervision
of the Oryol State University named after I. S. Turgenev,

Dr. Sci. (Law), Associate Professor

zukova57@mail.ru

95, ul. Komsomolskaya, Oryol, Russia, 302010

Cybercrime against Minors: Causes and Directions of Prevention

Abstract. The problem of preventing cybercrime against minors is of an international nature. Currently, there is an increase in the crime under consideration, as well as a change in its structure. The emergence of new forms of cybercrime against minors, such as cyberbullying and cyberbullying, indicates the development of this type of crime. The problems of reducing the level

of cybercrime against minors should be solved in the near future by making changes to criminal legislation. Effective recommendations should be developed within the framework of law enforcement activities to neutralize the destructive impact on the child in the virtual space. These quantitative and qualitative changes in the crime under consideration require serious changes. The correct definition of the causal complex of cybercrime against minors will make it possible to develop effective measures to counter cybercrime against minors. The article is devoted to the analysis and systematization of the causes of the crime under consideration and the proposals for their prevention developed on their basis.

Keywords: cyberspace, virtual space, cybercrime, juvenile cyber activity, criminal liability, prevention

Современное общество не представляет свое развитие без киберпространства. Цифровые технологии и виртуальная реальность становятся все более важными элементами повседневной жизни людей. Роль киберпространства в жизни каждого человека постоянно возрастает, что выражается в количестве проведенного времени в сети Интернет. Однако данная тенденция имеет двоякое значение для населения: с одной стороны, виртуальная реальность способствует саморазвитию и самосовершенствованию пользователей, с другой стороны — увеличивает вероятность влияния криминальных элементов на них через сеть Интернет. Все чаще в нашей повседневной жизни мы сталкиваемся с кибермошенничеством, кибервымогательством и другими преступными деяниями. Потенциально незащищенной группой лиц в виртуальной реальности являются несовершеннолетние. Это объясняется их психофизиологическим состоянием, отсутствием жизненного опыта, сверхдоверчивостью и другими качествами, присущими детскому возрасту.

Проблемы защиты прав детей были актуальными для государства во все исторические эпохи. Это связано с особым правовым статусом ребенка. Необходима защита несовершеннолетних граждан со стороны государства и в киберпространстве. В связи с этим кибербезопасность несовершеннолетнего стала одним из основных направлений государственной политики России.

Необходимо понимать, что киберпространство имеет трансграничный характер, в связи с чем вопросы кибербезопасности несовершеннолетних необходимо рассматривать в контексте международного права в рамках комплексного обеспечения безопасности детей в виртуальном пространстве.

В рамках уголовно-правовых наук нет единого подхода к пониманию киберпреступности в отношении несовершеннолетних. Ряд ученых-криминологов рассматривают данную преступность как часть общеуголовной преступности, направленной на нарушение прав детей. Другие считают, что данный вид преступности является частью киберпреступности. Однако абсолютно все криминологи сходятся во мнении, что данный вид преступности имеет место и активно развивается в настоящее время.

Киберпреступность представляет собой совокупность разнообразных противоправных действий, совершаемых в цифровом пространстве через мошенничество,



вымогательство, хищение средств, легализацию преступных доходов, сексуальную эксплуатацию, кибератаки, торговлю людьми и их личными данными, распространение наркотиков и оружия, а также пропаганду экстремистских идей. Высокая активность несовершеннолетних в виртуальном мире детерминирует киберпреступность в отношении них. Эта тенденция объясняется возрастом, социальными установками и психологическим состоянием несовершеннолетних жертв.

Статистика свидетельствует о том, что наблюдается ежегодный рост киберпреступлений в отношении несовершеннолетних. Можно выделить несколько причин такого положения.

Первая причина — совершенствование гаджетов, позволяющих реализовать беспрепятственный вход в сеть. Так, согласно социологическому исследованию, проведенному российской сетью Blink, каждый второй молодой человек в возрасте от 14 до 24 лет предпочитает использовать iPhone для выхода в Интернет (52 %). В ходе исследования не было обнаружено лиц в возрасте от 14 до 24 лет, которые пользуются кнопочными телефонами. Отказ от последних обусловливается невозможностью выхода с кнопочного телефона в Интернет¹.

Согласно анализу уголовных дел, киберпреступления, совершаемые в отношении детей старше 12 лет, имеют деструктивный характер. В настоящее время кибербуллинг представляет собой значительную угрозу в онлайн-мире, где примерно 23 % детей в России становятся жертвами этого явления как в сети, так и в реальной жизни, причем каждый пятый ребенок в России сталкивается с оскорблениями и унижениями ежедневно или 1—2 раза в неделю².

Вторая причина — отсутствие надлежащего контроля взрослых за посещением небезопасного контента несовершеннолетними. В нашем государстве разработана и действует программа «Родительский контроль», которая направлена на блокировку посещения несовершеннолетними небезопасных сайтов. Анализ применения данной программы показал, что она наиболее эффективна для детей в возрасте от 7 до 12 лет. Чем старше становится ребенок, тем больше способов обхода контролирующих программ он использует. Но стоит отметить, что родительский контроль, хотя и помогает сдерживать активность детей в Интернете, является лишь предупредительной мерой и не обеспечивает защиту ребенка от действий киберпреступников, с которыми он уже встретился в виртуальном пространстве и поддерживает контакт.

Рост киберпреступности в отношении несовершеннолетних обусловлен рядом проблем, среди которых необходимо выделить следующие:

1. Отсутствие единых мировых стандартов по противодействию данному виду преступности обусловлено различными законодательными подходами стран, различиями в терминологии и практике применения уголовного законодательства, особенностями правоохранительной системы. Например, в Германии установлена

¹ Краткая характеристика состояния преступности в Российской Федерации за январь — май 2023 года и январь — декабрь 2022 года // URL: <https://мвд.рф/reports/item/39336121/> (дата обращения: 31.03.2025).

² В России назвали самые популярные смартфоны 2024 года // URL: <https://hi-tech.mail.ru/news/117347-samye-populyarnye-smartfony-zumerov-2024/> (дата обращения: 31.03.2025).

уголовная ответственность за кибербуллинг в отношении несовершеннолетних, в России такой нормы уголовное законодательство не содержит.

2. Отсутствие официальной статистики по данной категории преступлений и скрытый характер информации об уголовных делах с участием детей создают трудности в выявлении данного вида преступности. Начиная с 2017 г. все виды преступных деяний, совершаемых в виртуальном мире, должны быть учтены статистически. По информации МВД России, каждый год в России регистрируется более 500 тыс. преступлений, связанных с ИТ-технологиями или компьютерной информацией. Однако отдельно киберпреступления, совершаемые против несовершеннолетних, официально не учитываются.

3. Латентность данного вида преступности обусловливается несколькими факторами: ребенок не понимает, что он общается с преступником и что в отношении него совершается преступление; ребенку комфортно общаться с преступником, и он не желает его выдавать родителям или иным родственникам.

4. Анонимность киберпреступника. Современные информационные технологии позволяют преступнику совершать противоправные деяния и при этом не находиться в одном месте с жертвой. Обезличенность киберпреступника в сети дает ему определенные гарантии безнаказанности и безопасности, избавляя от общественного порицания и осуждения.

5. Постоянное развитие и совершенствование ИТ-технологий позволяет беспрепятственно привлечь новых участников в информационное пространство, а также расширить киберпространство за счет роста числа пользователей сети Интернет и мобильных компьютерных устройств. Увеличение использования компьютеров, информационно-телекоммуникационных сетей и информационных технологий напрямую влияет на рост киберпреступности. Например, активное распространение коронавирусной инфекции COVID-19 существенно изменило ситуацию с киберпреступностью, увеличив ее в несколько раз. Высокая активность в сети Интернет способствует росту киберпреступности в отношении несовершеннолетних. В условиях нестабильной социально-экономической обстановки, вызванной пандемией 2020 г., увеличения уровня безработицы и снижения благосостояния населения люди все чаще обращаются к виртуальной реальности в поисках решения своих проблем. Влияние окружающей реальности и внешних факторов заставляет как взрослых, так и несовершеннолетних искать утешения и новых форм общения в сети Интернет. Это, в свою очередь, приводит к увеличению угроз в киберпространстве, прежде всего для детей. Экономический кризис, трудности на рынке труда и безработица вынуждают людей выходить за пределы обычной жизни, пытаясь самореализоваться в виртуальном мире.

6. География распространения киберпреступности охватывает не одно государство. В сфере борьбы с преступной деятельностью в киберпространстве возникают сложности из-за слияния виртуальной среды и реальной, что требует инновационного подхода для противодействия разнообразным киберугрозам. В структуре киберпреступности преобладают тяжкие и особо тяжкие преступления, что делает ее особенно опасной для общества и требует эффективного противодействия со стороны правоохранительных органов и международного сообщества.



Для эффективного противостояния киберпреступности в отношении несовершеннолетних необходимо изучить факторы, влияющие на совершение преступлений в сети Интернет. Мы считаем, что при исследовании причин киберпреступности в отношении несовершеннолетних важно придерживаться идеи причинности преступлений, предложенной В. Н. Кудрявцевым, который выделил два типа причин преступности — объективные и субъективные.

Для разработки эффективных методов борьбы с преступностью, включая киберпреступность против несовершеннолетних, следует обращать внимание на систему внешних и внутренних факторов, которые обуславливают поведение человека в различных условиях.

Среди важнейших направлений в государственной политике в целях предупреждения киберпреступности в отношении несовершеннолетних считаем необходимым выделить:

1) недостаточное внимание к образованию и культуре приводит к тому, что дети все чаще находятся в сети Интернет в поисках новых возможностей для обучения и развлечений, а риск киберугроз увеличивается;

2) отсутствие эффективных мер защиты детей от киберпреступности, включая законодательные пробелы и недостаток специалистов в правоохранительных органах, а также некомпетентность следователей при расследовании дел, способствует снижению уровня раскрываемости киберпреступлений;

3) формирование структуры киберпреступности в отношении несовершеннолетних подвержено воздействию различных внутренних факторов. Важным из них является социальная среда сетевого пространства, где представители с опасными взглядами объединяются в маргинальные группы. Эти криминально настроенные субъекты находят в Интернете удобные условия для общения не только с жителями своего региона или страны, но и со всем миром.

7. Растущее количество ресурсов, пропагандирующих экстремистские взгляды, включая сайты, где популяризируются преступные идеи и образ жизни, такие как вербовка в террористические организации, распространение детской порнографии, наркотиков и информации о их производстве, продажа баз данных с личной информацией граждан, кредитными картами, объясняется различными факторами.

В рамках эффективного предупреждения киберпреступности в отношении несовершеннолетних необходимо выработать меры воздействия на причины возникновения рассматриваемого вида преступности. Считаем, что данные меры должны реализовываться по следующим направлениям:

- виктимологическая профилактика;
- техническое оснащение правоохранительных органов;
- психологический комфорт в семье;
- установление уголовной ответственности за киберпреступления в отношении несовершеннолетних.

Реализация данных мер должна проводиться комплексно, это позволит повысить уровень кибербезопасности для несовершеннолетних.

БИБЛИОГРАФИЯ

1. Краткая характеристика состояния преступности в Российской Федерации за январь — май 2023 года и январь — декабрь 2022 года // URL: <https://мвд.рф/reports/item/39336121/> (дата обращения: 31.03.2025).
2. В России назвали самые популярные смартфоны 2024 года // URL: <https://hi-tech.mail.ru/News/117347-samye-populyarnye-smartfony-zumerov-2024/> (дата обращения: 31.03.2025).





Наталья Александровна

ГРИШКО,

доцент кафедры

уголовного права,

уголовного процесса

и правоохранительной

деятельности

Российского университета

транспорта (МИИТ),

кандидат юридических наук

grish.nat88@yandex.ru

127055, Россия, г. Москва,

ул. Образцова, д. 9, стр. 9

Защита потенциальных жертв киберпреступлений: виктимологический подход

Аннотация. В статье анализируется природа кибервиктимности, выделяются ключевые категории риска и основные формы виктимного поведения в киберсреде. Особое внимание уделяется профилактическим стратегиям, направленным на снижение виктимного потенциала личности, а также возможностям правового и социального реагирования. Предложены рекомендации по развитию системы виктимологической помощи, просветительских программ и межведомственного взаимодействия. Подчеркивается необходимость формирования культуры цифровой безопасности как элемента общей профилактики киберпреступности. Предлагаются рекомендации по совершенствованию системы защиты жертв в рамках виктимологической парадигмы. Важное значение отводится индивидуальной виктимологической профилактике. Отмечаются существенные особенности процесса кибервиктимизации как части общей виктимологической теории. Рассматриваются проблемы, возникающие при расследовании киберпреступлений, оказывающие, в свою очередь, влияние на виктимологическую составляющую киберпреступлений. Выделены и охарактеризованы ключевые компоненты поведенческой модели жертвы киберпреступлений: когнитивный, эмоциональный и поведенческий. Приведены типовые модели поведения, предрасполагающие к виктимизации в киберпространстве.

В работе приведены зарубежный и отечественный опыт реализации программ и проектов, направленных на виктимологическую профилактику в цифровом пространстве, так как международный опыт представляет ценность для формирования эффективной системы виктимологической профилактики в России и может служить основой для сравнительно-правового анализа.

Ключевые слова: киберпреступность, кибервиктимизация, модель поведения жертвы, индивидуальная виктимологическая профилактика

DOI: 10.17803/2311-5998.2025.129.5.234-243

Natalia A. GRISHKO,

Associate Professor of the Department of Criminal Law,
Criminal Procedure and Law Enforcement
at the Russian University of Transport (MIIT),
Cand. Sci. (Law)

grish.nat88@yandex.ru

9/9, ul. Obraztsova, Moscow, Russia, 127055

Protecting Potential Victims of Cybercrime: a Victimological Approach

Abstract. The article analyzes the nature of digital victimization, identifies key risk categories and the main forms of victim behavior in the cyber environment. Special attention is paid to preventive strategies aimed at reducing the victim potential of the individual, as well as the possibilities of legal and social response. Recommendations on the development of a system of victimological assistance, educational programs and interdepartmental cooperation are proposed. The need for the formation of a digital security culture as an element of the general prevention of cybercrime is emphasized. Recommendations for improving the victim protection system within the victimological paradigm are proposed. Individual victimological prevention is of great importance. The essential features of the process of cyber-victimization as part of the general victimological theory are noted. The problems that arise in the investigation of cybercrimes, which, in turn, have an impact on the victimological component of cybercrime, are considered. The problems that arise in the investigation of cybercrimes are considered, which, in turn, have an impact on the victimological component of cybercrimes. The key components of the behavioral model of a victim of cybercrime are identified and characterized: cognitive, emotional and behavioral. Typical patterns of behavior predisposing to victimization in cyberspace are given.

The paper presents foreign and domestic experience in the implementation of programs and projects aimed at victimological prevention in the digital space, as international experience is valuable for the formation of an effective system of victimological prevention in Russia and can serve as a basis for comparative legal analysis.

Keywords: cybercrime, cyber-victimization, victim's behavioral model, individual victimological prevention

Современная виктимология, ориентированная на анализ причин, способствующих становлению личности жертвой преступления, в условиях цифровизации сталкивается с новыми формами виктимности. Киберпреступность характеризуется высокой анонимностью, трансграничностью и социальной инженерией, что создает качественно иные условия для формирования виктимного поведения. Эффективная защита жертв невозможна без глубокого понимания виктимологических закономерностей цифрового пространства.



Виктимологический подход позволяет рассматривать защиту жертв киберпреступлений не как эпизодическую реакцию, а как системную превентивную деятельность. Цифровая виктимность — это новое явление, требующее мультидисциплинарного подхода. Важнейшим направлением становится формирование *цифровой культуры виктимологической осведомленности*, где каждый субъект понимает собственную уязвимость и знает способы ее снижения.

Уголовное законодательство РФ сегодня не предлагает легального определения киберпреступления, что непосредственно оказывает влияние на понятие «жертва киберпреступления». Чаще всего под киберпреступлением понимается деяние, совершенное с использованием информационных технологий или направленное на объекты информационной инфраструктуры¹.

Важно определить в этой связи ключевые признаки киберпреступлений:

- использование компьютерных технологий как инструмента совершения преступления;
- объект посягательства — информация, данные, системы и сети;
- сложность установления личности правонарушителя;
- часто носит трансграничный характер².

Расследование киберпреступлений представляет собой одно из самых сложных направлений в деятельности правоохранительных органов, поскольку такие деяния совершаются в условиях высокой технологической динамики, трансграничности и анонимности субъектов. При расследовании данного вида преступлений возникает множество препятствий: от пробелов в правовом регулировании и дефицита специалистов до международных барьеров и недостаточной технологической базы. Эффективное преодоление этих проблем требует:

- совершенствования уголовного и уголовно-процессуального законодательства;
- создания специализированных подразделений с технической экспертизой;
- расширения международной кооперации;
- внедрения современных методов цифровой криминалистики.

Процесс кибервиктимизации сегодня вовлекает все большее количество участников, а сам процесс становления жертвы киберпреступлений отличается следующими признаками:

- «коллективность» жертв;
- анонимность «преступника»;
- скоростной режим преступного воздействия;
- низкий уровень правосознания;
- доступность киберпространства;
- киберзависимость;
- психологические проблемы;
- разнообразие форм и методов киберпреступлений;
- нормативно-правовая ограниченность;
- удаленный режим воздействия преступника на жертву и др.

¹ Яковлев А. Ф. Преступления в киберпространстве: правовые аспекты // Уголовное право. 2022. № 5. С. 34—38.

² Соловьев Д. П. Киберугрозы и уголовная ответственность // Вестник Московского университета. Серия 11 : Право. 2021. № 6. С. 72—78.

Обозначенные причины оставляют небольшие шансы участнику киберпространства обеспечить свою безопасность от преступного посягательства. При этом гибкость «преступных возможностей» своевременно подстраивается под современные реалии практически всех сфер жизнедеятельности людей.

Кибервиктимизацию рассматривают сегодня многие научные междисциплинарные направления, среди которых: социология Интернета, киберпсихология, цифровая криминология, кибервиктимология, технические науки, опосредующие процесс взаимодействия операторов и машин в виртуальной среде³. Кибервиктимизация — сложный и многогранный феномен, сочетающий в себе как индивидуальные поведенческие установки жертвы, так и социальные и технологические риски.

Одним из ключевых механизмов кибервиктимизации является поведенческая модель личности, определяющая способ ее присутствия и взаимодействия в цифровом пространстве. В отличие от классических форм виктимного поведения, поведенческие и коммуникативные установки в Интернете приобретают новые характеристики, связанные с особенностями виртуальной среды: иллюзией анонимности, стремлением к самопрезентации, доступностью и быстротой коммуникаций. В отличие от традиционных форм виктимного поведения, поведенческая модель жертв киберпреступлений формируется под влиянием особых условий цифровой среды, в которой отсутствует физический контакт, преобладают дистанционные коммуникации и наблюдается смещение границ частного и публичного.

Современные криминологи и виктимологи выделяют три ключевых компонента поведенческой модели жертвы киберпреступлений:

- когнитивный компонент — уровень знаний о цифровых рисках, правовом регулировании онлайн-деятельности, принципах кибергигиены. Низкая информированность и отсутствие критического мышления повышают вероятность попадания в опасные ситуации;
- эмоциональный компонент — эмоциональное состояние личности, ее склонность к доверчивости, тревожности, одиночеству. Люди, испытывающие потребность в общении или признании, чаще вовлекаются в манипулятивные взаимодействия (например, скамеры, груминг, шантаж);
- поведенческий компонент — конкретные действия и практики пользователя в сети: размещение персональной информации, участие в онлайн-конфликтах, переход по сомнительным ссылкам, отсутствие защиты аккаунтов⁴.

Поведенческая модель жертвы киберпреступления — это результат взаимосвязи индивидуальных психологических характеристик, уровня цифровой культуры и особенностей онлайн-коммуникации. Поведенческая модель жертвы киберпреступления не является статичной — она может меняться под влиянием внешних обстоятельств (кризисы, изоляция, эмоциональные потрясения), что повышает вероятность вовлечения в преступную ситуацию. Более того, многие

³ Жмуров Д. В. Кибервиктимизация. Исследовательская матрица // Пролог: журнал о праве. 2021. № 3. С. 109—121.

⁴ Назаров Д. В. Киберповедение личности: между безопасностью и риском // Социальная психология и общество. 2021. № 3. С. 59—64.



пользователи одновременно могут выступать и жертвами, и участниками виктимогенных ситуаций, особенно в условиях массовой цифровой коммуникации.

Для части пользователей Интернет становится основным каналом общения, источником признания и самооценки. Это особенно характерно для подростков и представителей маргинализированных групп. Такое стремление к социальной валидации делает их восприимчивыми к манипуляциям и втягиванию в опасные отношения.

Анализ правоприменительной и эмпирической практики позволяет выделить *типовые модели поведения*, предрасполагающие к виктимизации в цифровой среде:

- наивно-доверчивый тип — характеризуется отсутствием осторожности, открытостью к незнакомцам, некритичным восприятием информации (часто — пожилые люди и подростки);
- самопрезентативный тип — склонен к демонстрации личной жизни в соцсетях, что делает жертву уязвимой к шантажу, буллингу и манипуляциям;
- рискованно-экспериментальный тип — участвует в опасных интернет-активностях (хакерские игры, флешмобы, подпольные чаты), часто не осознавая последствий;
- правонеосведомленный тип — не знает или игнорирует механизмы защиты своих прав в сети, не обращается в правоохранительные органы при столкновении с преступлением⁵.

Киберпреступность представляет собой многоплановую угрозу, требующую адаптивных и комплексных решений. Защита потенциальных жертв — это не только задача правоохранительных органов, но и приоритетное направление государственной политики в области цифрового развития и безопасности. В современных условиях необходим переход от реактивного подхода к проактивной модели, основанной на профилактике, просвещении и межсекторальном сотрудничестве.

В условиях цифровой среды особенно возрастает значение индивидуальной виктимологической профилактики, поскольку киберугрозы обладают высокой адаптивностью, а потенциальные жертвы все чаще становятся объектами *персонализированных атак*.

В отличие от групповой или массовой профилактики (например, информационных кампаний), *индивидуальная профилактика* позволяет учитывать личностные, психологические, социальные и технические особенности человека. Это особенно важно в киберпространстве, где один пользователь может быть защищен, а другой — в силу возраста, состояния здоровья или стиля поведения — оставаться крайне уязвимым.

Индивидуальный подход позволяет:

- выявлять скрытые формы виктимности, которые не видны в рамках общей статистики;
- адаптировать методы профилактики к уровню цифровой грамотности и психологической устойчивости субъекта;

⁵ Соколова И. А. Виктимологический анализ интернет-преступлений: поведенческий аспект // Криминология: научные труды. 2022. № 2. С. 42—47.

— снижать риск вторичной виктимизации, особенно у лиц, уже переживших киберпосягательство.

К целевым установкам индивидуальной виктимологической профилактики можно отнести:

а) снижение рисков, располагающих лицо (группу) к тому, чтобы стать жертвой киберпреступления;

б) воздействие на причины и условия индивидуального поведения потенциальных жертв;

в) противодействие негативным факторам ближайшего социального окружения жертвы, т.е. виктимогенным особенностям ее микросреды;

г) прямое воздействие на личность, которая в силу индивидуальных характеристик способна оказаться жертвой киберпреступления⁶.

Ключевые уровни индивидуальной виктимологической профилактики можно представить в следующей классификации:

1. Доинцидентный уровень (разработка моделей раннего противодействия киберпреступности) заключается во внедрении значительного числа стандартов и шаблонов, снижающих виктимность в цифровом пространстве и не допускающих ее реализации. Они формируются на индивидуально-поведенческом (путем воспитательных или образовательных мероприятий, сертификации персонала, повышения квалификации, предустановки на устройства комплекса обучающих и защитных программ) или нормативном уровне в виде национальных стандартов информационной безопасности, которых на сегодня насчитывается уже более десятка. Среди них можно выделить:

а) безопасное использование гаджетов и персонального компьютера (установка лицензионного программного обеспечения, антивирусная защита; проверка сторонних подключений, очистка средств отслеживания, блокировка удаленных соединений и др.);

б) безопасный серфинг в виртуальном пространстве (использование двухфакторной аутентификации и сложных ключей генерации, практика обязательного разлогинивания на чужих ПК, использование настроек приватности в виде отказа от передачи телеметрии, избыточных данных, рекламных идентификаторов и др.);

в) навыки защиты от вредоносных программ (отказ от установки неизвестных программ и приложений, отказ от передачи собственных устройств третьим лицам, автообновление браузера, использование системных решений в области безопасности и др.);

г) безопасная эксплуатация сетей Wi-Fi (запрет на передачу конфиденциальных данных и платежной информации через публичный доступ, использование специальных браузерных расширений, усиливающих безопасность, деактивация функций «подключение к Wi-Fi автоматически» и др.);

д) безопасная активность в социальных сетях (проверка подлинности профилей, периодическая смена паролей, осторожность при установке дополнений и приложений для социальной сети др.);

⁶ Жмуров Д. В. Индивидуальная виктимологическая профилактика киберпреступности // Сибирский юридический вестник. 2023. № 1. С. 52—59.



е) безопасное использование электронной почты (избегание неизвестной корреспонденции и ссылок, верификация и проверка отправителей сомнительных писем, использование почтовых антивирусов, использование ЭПЦ для важной переписки, активное использование спам-фильтрации и др.);

ж) безопасная игровая деятельность онлайн (использование антигриферских плагинов для резервного копирования игрового мира, скрин-фиксация коммуникаций и др.);

и) безопасное осуществление онлайн-покупок (хранение ограниченной суммы денег на счету, отключение автозаполнения платежных форм в браузере, проверка наличия разнообразных чек-боксов, периодическое ознакомление с выписками по кредитной карте на наличие несанкционированных транзакций)⁷.

2. Инцидентный уровень (разработка стандартов учета виктимного поведения) предполагает концентрацию внимания на выявлении, фиксации, подсчете и статистическом отображении группы виктимизированных лиц в Интернете.

3. Постинцидентный уровень (разработка стандартов реагирования на кибервиктимизацию) относится к преодолению ближайших и отдаленных последствий киберпреступности. К нему относятся: организация работы по приему заявлений о киберпреступлениях; формирование институтов поддержки жертв киберпреступлений — создание структур, призванных оказывать содействие виктимизированным лицам (консультационная, правовая, психологическая помощь); обучение сценариям реагирования.

Разработка системы эффективной защиты жертвы киберпреступлений не может отвечать практико-ориентированности без таких важных звеньевых элементов, как виктимное профилирование и прогноз.

Виктимное профилирование должно разработать наиболее четкий и полный профиль жертвы в киберпространстве на основе классификационных типологий с определением индивидуальных особенностей психолого-поведенческого свойства.

Виктимологический прогноз должен основываться на критериях обусловленности, распространенности и эпидемичности⁸.

Обусловленность строится на дифференциальном подходе — выявлении зависимости кибервиктимных тенденций от гендерных, возрастных, поведенческих, личностных условий или причин. Как статистический показатель распространенность определяет интенсивность кибервиктимных актов и число лиц, потерпевших от них. Эпидемичность в данном вопросе оценивает способность актов кибервиктимизации причинять вред в плане социального и физического здоровья, негативно воздействовать на популяцию.

Методы, применяемые в индивидуальной профилактике кибержертв, имеют важное значение и могут варьироваться в зависимости от характеристик потенциальной жертвы. К ним можно отнести:

— консультирование — индивидуальные беседы с психологами, педагогами или специалистами по информационной безопасности;

⁷ Жмуров Д. В. Индивидуальная виктимологическая профилактика киберпреступности.

⁸ Жмуров Д. В. Кибервиктимизация. Исследовательская матрица.

- обучение на примерах — разбор конкретных случаев кибермошенничества, имитация фишинговых атак в контролируемой среде;
- психологическая поддержка — оказание помощи лицам, уже ставшим жертвами, с целью предотвращения повторной виктимизации;
- настройка технических средств защиты — помощь в установке и правильной конфигурации антивирусов, систем двухфакторной аутентификации и родительского контроля;
- медико-социальное сопровождение для лиц с психоневрологическими расстройствами или когнитивными нарушениями.

Индивидуальная виктимологическая профилактика в условиях киберугроз становится необходимым элементом национальной политики в сфере безопасности. Она позволяет не только снижать риск виктимизации конкретных лиц, но и формировать культуру цифровой самозащиты, опирающуюся на осознанность, компетентность и психологическую готовность, что делает ее стратегическим инструментом в борьбе с современной, все более сложной и персонализированной киберпреступностью.

В зарубежной криминологической и виктимологической практике особое внимание уделяется снижению уровня виктимности посредством комплексных мер, включающих правовое просвещение, технические инструменты защиты и институциональные гарантии.

В Великобритании функции по защите населения от киберугроз возложены на Национальный центр кибербезопасности (NCSC)⁹, действующий при разведывательном агентстве GCHQ. Центр активно взаимодействует с бизнесом, образовательными учреждениями и гражданским обществом. Одним из ключевых направлений работы является программа Cyber Aware, ориентированная на формирование цифровой грамотности населения. В рамках инициативы распространяются рекомендации по настройке учетных записей, использованию двухфакторной аутентификации, защите данных. Дополнительно функционирует сервис Suspicious Email Reporting Service (SERS), позволяющий оперативно реагировать на фишинговые атаки и обучать население их распознаванию.

Германия делает акцент на формировании цифровой ответственности и превенции виктимизации на ранних этапах социализации. Проект Klicksafe, реализуемый при поддержке Европейской комиссии, предоставляет платформу для обучения школьников, учителей и родителей основам цифровой безопасности¹⁰; активно развиваются направления поведенческой аналитики и индивидуальной оценки киберрисков, что позволяет предсказывать вероятность виктимизации определенных категорий пользователей и адаптировать меры защиты.

Сингапур демонстрирует пример системного стратегического подхода к снижению киберрисков. Государственное агентство Cyber Security Agency of Singapore

⁹ National Cyber Security Centre. Cyber Aware // URL: <https://www.ncsc.gov.uk/cyberaware> (дата обращения: 20.03.2025).

¹⁰ U.S. Department of Homeland Security. Stop.Think.Connect. Campaign // URL: <https://www.dhs.gov/stopthinkconnect> (дата обращения: 22.03.2025).



(CSA)¹¹ разработало национальную стратегию кибербезопасности, в которую включен отдельный блок, посвященный защите населения. Программа Go Safe Online охватывает не только обучающие кампании, но и разработку пользовательских приложений для мониторинга подозрительных действий в сети, а также поддерживает «кибердобровольчество» — инициативу вовлечения молодежи в просветительскую деятельность.

Изучение зарубежного опыта защиты потенциальных жертв киберпреступлений позволяет выделить ряд эффективных подходов:

- превенция через образование и цифровую грамотность;
- широкое межведомственное и общественно-государственное сотрудничество;
- индивидуализация профилактики с учетом уязвимости пользователя;
- активное вовлечение частного сектора и гражданских инициатив.

Анализируется значение виктимологической профилактики преступлений в условиях цифровизации общества. Исследуется трансформация виктимного поведения в цифровом пространстве, обусловленная как ростом цифровых угроз, так и изменением структуры коммуникаций. Рассматриваются ключевые группы риска, механизмы воздействия на потенциальных жертв со стороны преступников, а также типовые модели виктимизации.

В России активно развиваются проекты и программы, направленные на виктимологическую профилактику в цифровом пространстве. Такие инициативы реализуются на государственном, региональном и общественном уровнях. В ряде регионов реализуются пилотные проекты, направленные на виктимологическую профилактику, например:

- программа «Цифровой иммунитет» для школьников и студентов;
- интерактивный портал МВД России по кибербезопасности;
- инициативы по цифровому просвещению от «Сбербанка», «Яндекса», Лаборатории Касперского и др.

Особое внимание в системе виктимологической профилактики уделяется просветительским и образовательным проектам. Так, в рамках национального проекта «Цифровая экономика» реализуется программа повышения цифровой грамотности, направленная на формирование устойчивого защитного поведения в сети. Аналогичную цель преследует инициатива «Цифровой диктант», ориентированная на диагностику и развитие навыков безопасного поведения у широкого круга пользователей.

В последние годы активно развиваются федеральные, региональные и частные инициативы, направленные на формирование культуры безопасного поведения в цифровой среде и снижение виктимности различных социальных групп, они включают как образовательные, так и информационно-просветительские компоненты и реализуются при сотрудничестве государственных структур, IT-компаний и образовательных учреждений.

Цифровизация различных сфер общественной жизни привела к трансформации традиционных форм преступности и появлению новых угроз. Одновременно с этим изменяется и профиль потенциальной жертвы. Виктимологическая

¹¹ Cyber Security Agency of Singapore. Go Safe Online // URL: <https://www.csa.gov.sg/gosafeonline> (дата обращения: 12.03.2025).

профилактика приобретает особую актуальность в условиях стремительного роста количества киберпреступлений и повышения уязвимости граждан в цифровой среде.

Киберпреступность порождает особую форму виктимности, требующую специализированных подходов к защите. Виктимологическая профилактика в цифровом пространстве должна сочетать правовые, образовательные и психологические меры, а также учитывать специфику уязвимых групп. Только системное внедрение моделей цифровой самозащиты и широкая виктимологическая просветительская работа способны эффективно снизить уровень виктимизации и укрепить личную и общественную безопасность в киберпространстве.

БИБЛИОГРАФИЯ

1. Жмуров Д. В. Индивидуальная виктимологическая профилактика киберпреступности // Сибирский юридический вестник. — 2023. — № 1. — С. 52—59.
2. Жмуров Д. В. Кибервиктимизация. Исследовательская матрица // Пролог: журнал о праве. — 2021. — № 3. — С. 109—121.
3. Назаров Д. В. Киберповедение личности: между безопасностью и риском // Социальная психология и общество. — 2021. — № 3. — С. 59—64.
4. Соколова И. А. Виктимологический анализ интернет-преступлений: поведенческий аспект // Криминология: научные труды. — 2022. — № 2. — С. 42—47.
5. Соловьев Д. П. Киберугрозы и уголовная ответственность // Вестник Московского университета. — Серия 11 : Право. — 2021. — № 6. — С. 72—78.
6. Яковлев А. Ф. Преступления в киберпространстве: правовые аспекты // Уголовное право. — 2022. — № 5. — С. 34—38.
7. Cyber Security Agency of Singapore. Go Safe Online // URL: <https://www.csa.gov.sg/gosafeonline> (дата обращения: 12.03.2025).
8. National Cyber Security Centre. Cyber Aware // URL: <https://www.ncsc.gov.uk/cyberaware> (дата обращения: 20.03.2025).
9. U.S. Department of Homeland Security. Stop.Think.Connect. Campaign // URL: <https://www.dhs.gov/stopthinkconnect> (дата обращения: 22.03.2025).





**Ольга Алексеевна
КУЗНЕЦОВА,**

главный научный сотрудник,
заведующий кафедрой уголовного
права, уголовного процесса
и криминалистики
Юридического института
Российского университета
дружбы народов
имени Патриса Лумумбы,
доктор юридических наук, доцент
kuznetsova-ola@rudn.ru
117198, Россия, г. Москва,
ул. Миклухо-Маклая, д. 6



**Мурад Мамедович
МАДЖУМАЕВ,**

ведущий научный сотрудник,
старший преподаватель кафедры
уголовного права, уголовного
процесса и криминалистики
Юридического института
Российского университета
дружбы народов имени
Патриса Лумумбы,
кандидат юридических наук
madzhumayev-mm@rudn.ru
117198, Россия, г. Москва,
ул. Миклухо-Маклая, д. 6

Защита частной жизни в виртуальной реальности: ответственность за использование дипфейк-контента в метавселенной¹

Аннотация. Метавселенная, представляющая собой иммерсивную и постоянную виртуальную среду, в сочетании с неправомерным использованием технологий искусственного интеллекта для создания гиперреалистичных синтетических медиаматериалов (фото, видео, аудио), образует новую категорию угроз для общественных отношений в сфере обеспечения неприкосновенности частной жизни.

Действующие нормативно-правовые механизмы, предназначенные в основном для регулирования взаимодействия в физической реальности и более ранних итерациях цифровой среды, недостаточно адаптированы для эффективного противодействия вызовам, возникающим в связи с созданием, использованием и распространением так называемых дипфейков (deepfakes). Именно применение этих технологий для формирования виртуальных аватаров (образов) людей в метавселенной представляет собой особенно сложную задачу. Представлен возможный механизм установления юридической ответственности, основанный на формальном признании комплекса «виртуальные права личности». Этот комплекс включает в себя право на аутентичность и контроль над собственным аватаром, право на подтверждение авторства и защиту от незаконного присвоения виртуальной личности, а также право на обеспечение целостности виртуальной среды субъекта. Предлагаемый подход также предусматривает необходимость разграничения юридической ответственности между субъектами, непосредственно создающими синтетические медиаматериалы с использованием машинного обучения, теми, кто осуществляет их последующее использование и распространение, и провайдером платформ метавселенной, обеспечивающими инфраструктуру для такого взаимодействия.

Ключевые слова: метавселенная, метапреступление, виртуальная реальность, дополненная реальность, виртуальный аватар, автономность виртуальной личности, цифровой двойник, машинное обучение, дипфейк, частная жизнь

DOI: 10.17803/2311-5998.2025.129.5.244-253

© Кузнецова О. А.,
Маджумаев М. М., 2025

¹ Исследование выполнено за счет гранта Российского научного фонда № 25-28-01478, <https://rscf.ru/project/25-28-01478/>.

Olga A. KUZNETSOVA,

*Chief Researcher, Head of the Department
of Criminal Law, Criminal Procedure, and Criminalistics
of the Law Institute of the Patrice Lumumba Russian
University of Peoples' Friendship,
Dr. Sci. (Law), Associate Professor
kuznetsova-ola@rudn.ru
6, ul. Miklukho-Maklaya, Moscow, Russia, 117198*

Murad M. MAJUMAEV,

*Leading Researcher, Senior Lecturer at the Department
of Criminal Law, Criminal Procedure and Criminalistics
of the Patrice Lumumba Russian University of Peoples' Friendship,
Cand. Sci. (Law)
madzhumaev-mm@rudn.ru
6, ul. Miklukho-Maklaya, Moscow, Russia, 117198*

Protection of Privacy in Virtual Reality: Liability for the Use of Deepfake Content in the Metaverse

Abstract. *The metaverse, as an immersive and persistent virtual environment, forms a new category of threat to public relations regarding privacy, when combined with the misuse of artificial intelligence technologies to create hyper-realistic synthetic media (photo, video, audio).*

Existing legal frameworks, predominantly designed to regulate interaction in physical reality and earlier iterations of the digital environment, are not sufficiently adapted to effectively counteract the challenges posed by the creation, use and dissemination of so-called deepfakes. The application of these technologies to the formation of virtual avatars (images) of people in the metaverse presents a particularly complex regulatory challenge.

Presented is a possible mechanism for establishing legal liability based on the formal recognition of a set of "virtual personality rights". This complex includes the right to authenticity and control over one's own avatar, the right to confirm authorship and protection from misappropriation of virtual identity, as well as the right to ensure the integrity of the subject's virtual environment. The proposed approach also envisages the need to distinguish the legal responsibility between the actors who directly create synthetic media materials using machine learning, those who carry out their subsequent use and distribution, and the providers of metaverse platforms that deliver the infrastructure for such interaction.

Keywords: *metaverse, metacrime, virtual reality, augmented reality, virtual avatar, autonomy of virtual personality, digital twin, machine learning, deepfake, privacy*



Современные тенденции развития общественных отношений сопряжены со стремительным распространением передовых вычислительных систем и цифровых (виртуальных) инфраструктур, способных в беспрецедентных масштабах перестроить существующие социально-экономические процессы. На фоне столь ускоренной научно-технической эволюции юриспруденция не может занимать позицию дисциплинарного изоляционизма. Необходима динамичная реконструкция устоявшихся нормативных рамок в целях обеспечения эффективного усвоения и практического применения инновационных достижений технических наук. Упущение таких интеграционных мер может представлять серьезную опасность: право окажется в непоправимом отрыве от складывающихся реалий и технологических парадигм, на которых строится взаимодействие внутри общества. Аналогичным образом сама траектория развития научно-технических инноваций требует соответствующего правового регулирования.

Показательным в этом отношении является метавселенная, представляющая собой формирующуюся систему взаимосвязанных виртуальных пространств, которая способна переосмыслить формы социального взаимодействия. Статистические показатели указывают на солидный оборот глобального рынка метавселенной, который в 2023 г. оценивался в 94,1 млрд долларов США при ежемесячной активной пользовательской базе в 400 млн человек, а к 2032 г. должен вырасти до 2 346,2 млрд долларов США².

В то же время результаты проведенного исследования свидетельствуют о росте количества дипфейк-контента: в первом триместре 2025 г. в Российской Федерации был выявлен 61 такой уникальный контент и 2 300 копий, что на 65 % больше, чем за весь 2024 г., и в 2,6 раза больше, чем в 2023 г.³ Все это лишний раз подтверждает необходимость тщательного изучения возможных форм социальных отношений в этих иммерсивных цифровых реальностях, в особенности с учетом использования изображений людей в метавселенной.

Метавселенная является гипотетической, следующей стадией развития сети Интернет, так называемой Web 3.0 или пространственной паутиной, которая характеризуется слиянием физической и цифровой реальностей, обеспечивая плавные переходы и взаимодействие между различными виртуальными пространствами⁴. Она представляет собой постоянную взаимосвязанную сеть общих трехмерных виртуальных пространств⁵. В этих пространствах пользователи, обычно представляемые фотографиями или другими графическими изображениями (аватарами), используемыми в учетной записи для их персонализации, могут синхронно взаимодействовать с окружающей средой, друг с другом

² Pangarkar T. Metaverse Statistics 2025 by New Technology in Virtual Space // Market.us Scoop. 2025. URL: <https://scoop.market.us/metaverse-statistics/> (дата обращения: 28.03.2025).

³ Wave of deepfake fraud: how technology is changing the threat landscape // Global Fact-Checking Network (GFCN). 2025. URL: <https://globalfactchecking.com/wave-of-deepfake-fraud-how-technology-is-changing-the-threat-landscape/> (дата обращения: 09.04.2025).

⁴ Kiaer J. Conversing in the Metaverse: The Embodied Future of Online Communication. Great Britain : Bloomsbury Publishing Plc, 2024. P. 6—12.

⁵ Kiaer J. Op. cit. P. 6.

и программными агентами в режиме полного погружения⁶. Эти аватары служат цифровыми суррогатами, позволяя пользователям выражать свою индивидуальность, взаимодействовать с другими пользователями и ориентироваться в виртуальном мире. Уровень детализации и настройки аватаров на различных платформах метавселенной может варьироваться от стилизованных изображений до фотореалистичных.

Постоянство (устойчивость) метавселенной означает, что виртуальное пространство и цифровые активы в нем существуют непрерывно, независимо от того, активны (присутствуют) ли в нем отдельные пользователи⁷. В отличие от многих «традиционных» виртуальных пространств, таких как онлайн-игры или симуляторы, которые часто основаны на сессиях и прекращают свое существование (функционирование), как только пользователь отключается от сети, здесь «жизнь» продолжается и развивается независимо от присутствия или отсутствия (бездействия) отдельного пользователя.

Синхронность, с другой стороны, предполагает взаимодействие в реальном времени и совместный пользовательский опыт в метавселенной⁸.

Воплощенное цифровое присутствие является другой определяющей характеристикой метавселенной, относящейся к представлению пользователей через аватары в виртуальной среде, обеспечивая ощущение «присутствия». Чувство воплощенного присутствия усиливают такие технологии, как виртуальная реальность (VR), дополненная реальность (AR), смешанная реальность (MR), расширенная реальность (XR) и тактильные эффекты (haptics), которые обеспечивают визуальный, слуховой и тактильный опыт, способствующий ощущению «реального» пребывания в цифровом пространстве⁹. Так, гарнитуры VR позволяют полностью погрузить пользователя в виртуальную среду, при AR накладываются цифровые элементы на реальный мир, а MR объединяет обе реальности, позволяя взаимодействовать между виртуальными и физическими объектами.

По мере расширения деятельности индивидов в таких виртуальных пространствах формируется качественно новая форма криминальной активности, которую можно обозначить как метапреступление. Под ним следует понимать «любое преступление, объективная сторона которого частично или полностью совершается в виртуальной среде метавселенной»¹⁰.

Открывая новые перспективы, этот технологический рубеж одновременно порождает и новые правовые вызовы, прежде всего связанные с защитой частной жизни.

⁶ *Mystakidis S.* Metaverse // Encyclopedia. 2022. Vol. 2. № 1. P. 491—493.

⁷ *Mystakidis S.* Op. cit. P. 486.

⁸ *Mystakidis S.* Op. cit. P. 488—489.

⁹ *Murala D. K., Panda S. K.* The role of immersive reality (AR/VR/MR/XR) in metaverse. In *Metaverse and Immersive Technologies* (eds. A. Chandrashekhkar, S. H. Saheb, S. K. Panda, S. Balamurugan and S.-L. Peng). 2023. P. 159—189 ; *Pacchierotti C.* et al. Guest Editorial Haptics in the Metaverse: Haptic Feedback for Virtual, Augmented, Mixed, and eXtended Realities // *IEEE Transactions on Haptics*. 2024. Vol. 17. № 2. P. 122—128.

¹⁰ *Seo S., Seok B., Lee C.* Digital forensic investigation framework for the metaverse // *Journal of Supercomputing*. 2023. Vol. 79. № 9. P. 9467—9468.



Обеспечение полного погружения (ощущения присутствия) является ключевой особенностью технологии виртуальной реальности и предполагает сбор, обработку и использование личной или семейной информации о пользователе. В основном эти данные требуются для создания реалистичной виртуальной среды, отслеживания взаимодействия с пользователем и персонализации опыта. Диапазон данных, собираемых в виртуальных средах, широк и многогранен и охватывает различные категории.

Собираются метаданные о пользователях, включая их профили, данные об использовании и аналитику, которые применяются для улучшения приложений с помощью A/B-тестирования и рекомендаций VR-контента¹¹. Эта категория также может включать социально-демографическую информацию, предпочтения пользователей, интересы, время, проведенное в «среде», и паттерны взаимодействия, которые потенциально могут быть использованы для целевого развития и рекламы¹². Даже IP-адреса могут собираться для целей модерации, например, для введения запретов на их основе¹³.

Помимо этого, осуществляется сбор физиологических данных о пользователях, причем виртуальные платформы и приложения потенциально могут собирать такие физические параметры, как рост и вес, для отслеживания физической формы¹⁴. Биометрические данные, в частности взгляд (изображение радужной оболочки глаза человека) и реакция лица, могут использоваться для организации рекламы и определения восприятия пользователями новых функций¹⁵.

При этом существует потенциальный риск использования таких данных, составляющих частную жизнь человека, без его согласия для регистрации аватара в метавселенной. В частности, распространены технологии, основанные на алгоритмах искусственного интеллекта (машинного обучения) для создания дипфейк-контента с использованием генеративных состязательных сетей (GAN) и диффузионных моделей. Они представляют собой возможность создания высокореалистичных искусственных (синтетических) цифровых материалов, способных модифицировать визуальный и аудиоконтент, что размывает границы между реальностью и «фабрикацией»¹⁶.

¹¹ *Abhinaya S. B. et al. "What are they gonna do with my data?": Privacy Expectations, Concerns, and Behaviors in Virtual Reality // Proceedings on Privacy Enhancing Technologies. 2025. № 1. P. 62.*

¹² *Chakraborty D. et al. Use of metaverse in socializing: Application of the big five personality traits framework // Psychology & Marketing. 2023. Vol. 40. P. 10.*

¹³ *Chawki M., Basu S., Choi K. S. Redefining boundaries in the Metaverse: navigating the challenges of virtual harm and user safety // Laws. 2024. Vol. 13. № 3. P. 33.*

¹⁴ *Lee J., Yoon H. K., Kim D. Design of Metaverse-Based Physical Fitness Service for the Enhancement of Exercise Capability for Youth // Mobile Information Systems. 2023. № 1. P. 7272781.*

¹⁵ *Manna R., Singh A., Apte M. Demystifying metaverse data from user-technology interaction // Applied Marketing Analytics. 2024. Vol. 9. № 4. P. 357—374.*

¹⁶ *Van der Sloot B. Regulating the synthetic society: Generative AI, legal questions, and societal challenges. Great Britain : Bloomsbury Publishing Plc, 2024. P. 45—46.*

Генеративные состязательные сети используют систему из двух нейронных сетей: генератора, который должен создавать искусственный (поддельный) контент, и дискриминатора, который пытается отличить настоящий контент от сгенерированного¹⁷. В ходе последовательного состязательного процесса генератор совершенствуется в создании синтетического контента, который может достаточно убедительно ввести в заблуждение дискриминатор, в результате чего получаются достаточно реалистичные подделки¹⁸. То есть генеративные состязательные сети используются для создания реалистичных фото-, видеоматериалов с заменой лица, голоса, в которых сходство одного человека плавно накладывается на фигуру (голос) другого, сохраняя убедительную мимику и движения.

Диффузионные модели работают путем преобразования простых распределений данных, таких как гауссовский шум, в сложные данные, которые выглядят очень похожими на реальные изображения или видео¹⁹. Используя технологию диффузии, пользователи могут манипулировать существующим медиаконтентом, например, частично изменять черты лица или полностью заменять лица людей, либо создавать совершенно новый образ несуществующих людей или объектов на основе текстовых описаний, как синтез сценариев, в которых люди говорят или делают то, чего они на самом деле никогда не говорили и не делали²⁰.

Использование глубокого обучения для создания поддельных биометрических данных (информации, характеризующей физиологические и биологические особенности человека) представляет собой повышенную общественную опасность и нарушает неприкосновенность частной жизни. В метавселенной после получения биометрических данных пользователя его аватар, цифровые активы, социальные связи и цифровая (метавиртуальная) жизнь будут скомпрометированы самым деструктивным образом, чем в современной сети Интернет (киберсреде), поскольку большинство биометрических данных невозможно сбросить.

Действующие правовые механизмы (за исключением тех, которые направлены на регулирование цифровой (кибер) среды, отличающейся от метасреды, метавселенной), предназначенные в первую очередь для регулирования общественных отношений, возникающих в реальном (физическом) мире, не способны в полной мере противостоять уникальным вызовам, возникающим в результате дипфейков в иммерсивных виртуальных средах.

На сегодняшний день уже не раз предпринимались попытки уголовно-правового регулирования отдельных общественных отношений, возникающих в связи с совершением преступлений с использованием дипфейк-контента. В Государственную Думу внесена инициатива о введении уголовной ответственности за использование дипфейк-контента при совершении преступлений, предусмотренных ст. 128¹, 158, 159, 159⁶, 165 УК РФ, с использованием изображения или голоса (в том числе поддельного или искусственно созданного) потерпевшего или иного лица, а также с использованием биометрических персональных данных

¹⁷ Van der Sloot B. Op. cit. P. 45.

¹⁸ Van der Sloot B. Op. cit. P. 45.

¹⁹ Croitoru F. A. et al. Diffusion models in vision: A survey // IEEE Transactions on Pattern Analysis and Machine Intelligence. 2023. Vol. 45. № 9. P. 10851.

²⁰ Croitoru F. A. et al. Op. cit. P. 10851.



потерпевшего или иного лица²¹. Другой законодательной инициативой была предпринята попытка отнести использование технологий искусственного интеллекта при совершении преступления в целом к обстоятельствам, отягчающим наказание в связи с их повышенной общественной опасностью²².

Отсутствие нормативного обеспечения в метавселенной может создать условия, в которых злоумышленники смогут воспользоваться этими пробелами, что в итоге приведет к недостаточной защите интересов цифровой идентичности от противоправных действий и затруднит их уголовное преследование за ущерб, причиненный в результате использования дипфейков. Поэтому необходим принципиально новый комплексный подход к правовому регулированию метавселенной. Этот подход должен основываться на признании возникающих прав, характерных для виртуальной среды, и установлении обязанностей, которые должны быть надлежащим образом выверены в рамках разнообразных экосистем метавселенной.

В этой связи представляется целесообразным предложить идею признания целостности и автономности виртуальной личности, т.е. признания, что цифровое представление человека в метавселенной, включая выбранный им аватар и связанные с ним биометрические и поведенческие данные, является продолжением его личности в реальной (физической) действительности. Здесь признается важность виртуального присутствия человека, все более погружающегося в цифровой мир, для его самовыражения и взаимодействия с другими членами общества²³. При этом для обеспечения защиты такой виртуальной идентичности необходимо реализовать ряд основных (мета)прав.

Во-первых, это право на аутентичность и контроль аватара²⁴, которое подразумевает исключительную прерогативу индивида определять форму и характеристики своего основного виртуального образа в метавселенной. Это право является основополагающим для развития чувства собственности и контроля над своим виртуальным «я». Несанкционированное создание или размещение практически аналогичного аватара, особенно если он используется в контексте, который может быть обоснованно воспринят как представление человека или его мнения, будет являться нарушением этого права. Технологии дипфейк значительно повышают угрозу этому праву, позволяя неправомерно имитировать аватар человека путем манипулирования биометрическими и поведенческими данными, на основе которых формируются движения, мимика и голосовые сигналы аватара.

²¹ Законопроект № 718538-8 «О внесении изменений в Уголовный кодекс Российской Федерации (в части установления уголовной ответственности за совершение преступлений с использованием технологий подмены личности)» // URL: https://sozd.duma.gov.ru/bill/718538-8#bh_histras (дата обращения: 11.04.2025).

²² Законопроект № 885494-8. В архиве. «О внесении изменения в статью 63 Уголовного кодекса Российской Федерации» // URL: <https://sozd.duma.gov.ru/bill/885494-8> (дата обращения: 11.04.2025).

²³ Беззодова С. А., Микляева А. В. Цифровые трансформации психологии человека : учебное пособие / под ред. А. В. Микляевой. СПб. : Издательство РГПУ имени А. И. Герцена, 2023. С. 5.

²⁴ Cheong B. C. Avatars in the metaverse: potential legal issues and remedies // *International Cybersecurity Law Review*. 2022. Vol. 3. № 2. P. 467—494.

Это право вписывается в общую тенденцию признания важности виртуальной идентичности как фундаментального компонента человеческого существования в цифровую эпоху. В то же время пользователи должны иметь возможность управлять и контролировать свои виртуальные образы. Появление технологий искусственного манипулирования медиаконтентом напрямую обуславливает необходимость правовой защиты от несанкционированного использования своего виртуального образа.

Следующее право — на утверждение авторства и предотвращение незаконного присвоения виртуальной личности²⁵ — предполагает, что любые виртуальные действия, заявления или выступления, приписываемые аватару человека, действительно являются его собственными. Создание и распространение поддельного контента, который ложно приписывает действия или высказывания аватару, тем самым искажая намерения или поведение человека в метавселенной, должно рассматриваться как нарушение этого права. Таким образом, признается возможность значительного репутационного ущерба и психических страданий, которые могут быть вызваны такими цифровыми искажениями.

Кроме того, следует признать, что право на целостность виртуальной среды²⁶, окружающей человека, определяет его заинтересованность в том, чтобы это пространство было свободно от вредоносного поддельного контента, который непосредственно направлен на его аватар или выдает себя за него, представляя собой преследование, клевету или причинение иного вреда. Иммерсивный характер среды виртуальной реальности может значительно усилить последствия таких нарушений по сравнению с «традиционными» онлайн-платформами. Это право подчеркивает необходимость создания безопасной и надежной виртуальной среды, в которой люди могут взаимодействовать, не опасаясь криминального подражания или целенаправленного преследования. Проактивные меры по предотвращению создания и распространения таких вредоносных имитаций крайне важны, поскольку их последствия в иммерсивных средах могут быть весьма серьезными.

Ответственность за потенциальные посягательства на частную жизнь в метавселенной должна быть дифференцирована в отношении тех, кто создал и (или) использовал дипфейк-контент, или вовлеченных в процесс субъектов:

Вменяемые физические лица (авторы дипфейк-контента), намеренно создающие синтетический материал с использованием глубокого обучения с целью причинения вреда третьим лицам в метавселенной, должны нести ответственность на общих условиях. Эта ответственность должна распространяться как на создание, так и на первоначальное распространение такого материала.

Вменяемые физические лица, которые сознательно распространяют вредоносный дипфейк-контент, созданный другими в метавселенной, также должны нести ответственность. Степень ответственности может варьироваться в зависимости от их участия в совершении преступления.

Также можно рассмотреть вопрос об ответственности провайдеров платформ метавселенной за непринятие необходимых мер для предотвращения создания и

²⁵ Cheong B. C. Op. cit. P. 477—478.

²⁶ Cheong B. C. Op. cit. P. 475—477.



распространения вредоносного дипфейк-контента на своих платформах. К таким мерам могут относиться разработка и внедрение технологий для обнаружения дипфейк-контента, создание четких руководящих принципов сообщества, запрещающих создание, использование и распространение дипфейк-контента, а также предоставление пользователям механизмов для сообщения и получения компенсации за причиненный вред.

Принципы виртуальной аутентичности, алгоритмической подотчетности и распределенной ответственности образуют устойчивую основу для формирования нового подхода к решению вопросов, связанных с созданием, использованием и распространением фальшивого, поддельного контента в метавселенной.

При таком подходе, когда устанавливаются четкие права, связанные с целостностью и автономией виртуальной личности, на провайдеров платформ возлагается ответственность за проактивное обнаружение, аутентификацию и модерацию контента, а также устанавливается ответственность для участников оборота дипфейк-контента в зависимости от их намерений и действий (бездействия), представляет собой комплексную стратегию для построения доверия и аутентичности в виртуальной среде метавселенной.

Невозможно переоценить важность технологической совместимости и стандартизированной аутентификации, поскольку эти меры имеют решающее значение для практической реализации и обеспечения соблюдения любых правовых рамок. Наконец, постоянная потребность в междисциплинарных исследованиях и разработке адаптивных правовых механизмов обеспечит эффективное регулирование быстро развивающейся технологической среды метавселенной.

Принятие такого многоуровневого и принципиального подхода позволит реализовать видение метавселенной как пространства доверия, подлинности и ответственного виртуального взаимодействия.

БИБЛИОГРАФИЯ

1. *Безгодова С. А., Микляева А. В.* Цифровые трансформации психологии человека : учебное пособие / под ред. А. В. Микляевой. — СПб. : Издательство РГПУ имени А. И. Герцена, 2023.
2. *Abhinaya S. B. et al.* "What are they gonna do with my data?": Privacy Expectations, Concerns, and Behaviors in Virtual Reality // *Proceedings on Privacy Enhancing Technologies*. — 2025. — № 1.
3. *Chakraborty D. et al.* Use of metaverse in socializing: Application of the big five personality traits framework // *Psychology & Marketing*. — 2023. — Vol. 40.
4. *Chawki M., Basu S., Choi K. S.* Redefining boundaries in the Metaverse: navigating the challenges of virtual harm and user safety // *Laws*. — 2024. — Vol. 13. — № 3.
5. *Cheong B. C.* Avatars in the metaverse: potential legal issues and remedies // *International Cybersecurity Law Review*. — 2022. — Vol. 3. — № 2. — P. 467—494.
6. *Croitoru F. A. et al.* Diffusion models in vision: A survey // *IEEE Transactions on Pattern Analysis and Machine Intelligence*. — 2023. — Vol. 45. — № 9.

7. *Kiaer J.* Conversing in the Metaverse: The Embodied Future of Online Communication. — Great Britain : Bloomsbury Publishing Plc, 2024. — P. 6—12.
8. *Lee J., Yoon H. K., Kim D.* Design of Metaverse-Based Physical Fitness Service for the Enhancement of Exercise Capability for Youth // *Mobile Information Systems*. — 2023. — № 1.
9. *Manna R., Singh A., Apte M.* Demystifying metaverse data from user-technology interaction // *Applied Marketing Analytics*. — 2024. — Vol. 9. — № 4. — P. 357—374.
10. *Murala D. K., Panda S. K.* The role of immersive reality (AR/VR/MR/XR) in metaverse. In *Metaverse and Immersive Technologies* (eds. A. Chandrashekhar, S. H. Saheb, S. K. Panda, S. Balamurugan and S.-L. Peng). — 2023. — P. 159—189.
11. *Mystakidis S.* Metaverse // *Encyclopedia*. — 2022. — Vol. 2. — № 1. — P. 491—493.
12. *Pacchierotti C.* et al. Guest Editorial Haptics in the Metaverse: Haptic Feedback for Virtual, Augmented, Mixed, and eXtended Realities // *IEEE Transactions on Haptics*. — 2024. — Vol. 17. — № 2. — P. 122—128.
13. *Pangarkar T.* Metaverse Statistics 2025 By New Technology in Virtual Space // *Market.us Scoop*. — 2025. — URL: <https://scoop.market.us/metaverse-statistics/> (дата обращения: 28.03.2025).
14. *Seo S., Seok B., Lee C.* Digital forensic investigation framework for the metaverse // *Journal of Supercomputing*. — 2023. — Vol. 79. — № 9. — P. 9467—9468.
15. *Van der Sloot B.* Regulating the synthetic society: Generative AI, legal questions, and societal challenges. — Great Britain : Bloomsbury Publishing Plc, 2024. — P. 45—46.
16. Wave of deepfake fraud: how technology is changing the threat landscape // *Global Fact-Checking Network (GFCN)*. — 2025. — URL: <https://globalfactchecking.com/wave-of-deepfake-fraud-how-technology-is-changing-the-threat-landscape/> (дата обращения: 09.04.2025).

ПРАВО В ИСТОРИЧЕСКОМ ПРЕЛОМЛЕНИИ

Из периодики прошлого

А. Эстрин¹

К вопросу о принципах построения системы уголовной репрессии в пролетарском государстве² (Извлечение)

В развитии советского уголовного права можно отметить четыре этапа, рубежами которых являются 1919, 1922, 1924 гг. В течение первого этапа, 1917—1919 гг., все уголовно-правовые нормы, в сущности, сводились к одной: «Пролетарский суд применяет к подсудимому ту или иную меру, руководствуясь исключительно своим революционным правосознанием». Только в 1919 г., сперва (частично) в программе ВКП(б), затем в Руководящих началах по уголовному праву РСФСР от 12 декабря 1919 г., были сформулированы принципиальные положения, положенные в основу дальнейшего построения уголовной репрессии в Советском государстве, в том числе и основное положение: «Наказание не есть возмездие за “вину”, не есть искупление “вины”, а является “оборонительной мерой”».

Второй этап, 1920—1922 гг., можно назвать периодом оформления революционного правосознания, ибо через несколько месяцев после издания Руководящих начал, на III Всероссийском съезде деятелей советской юстиции (июнь 1920 г.) ставится уже вопрос об издании Уголовного кодекса; к 1920 г. и относится начало работы по составлению проекта Уголовного кодекса в НКЮ, а в 1921 г. эта работа оживляется и делается более интенсивной благодаря переходу к нэпу. Уголовный кодекс РСФСР вводится в действие с 01.06.1922, за ним следуют вскоре и уголовные кодексы других советских республик. Применение УК в 1922—1924 гг. является проверкой на практике этого первого опыта советского законодательства в области кодификации уголовного права; практическая проверка прежде всего привлекает внимание советской общественности к вопросам «карательной политики», а в дальнейшем, конечно, порождает и проверку теоретическую, причем оказывается, что УК 1922 г. теоретически не вполне выдержан, ибо в советской юридической мысли «еще имеется и живет очень много неясных, старых,

¹ Эстрин Александр Яковлевич (1889—1938), ученый, государственный деятель, заместитель Московского губернского прокурора (1922—1926), директор Научно-исследовательского института уголовной и исправительно-трудовой политики Народного комиссариата юстиции РСФСР (1932—1933). В 1938 г. приговорен СК Верховного суда СССР к высшей мере наказания, расстрелян. В 1956 г. посмертно реабилитирован за отсутствием состава преступления.

² Эстрин А. Я. К вопросу о принципах построения системы уголовной репрессии в пролетарском государстве // Революция права. 1927. № 1. С. 74—98.

Статья представляет собой доклад, зачитанный на публичном заседании секции права в мае 1926 г.

традиционных, явно не наших воззрений»³, которые и проникли в редакцию УК 1922 г. На очередь ставится задача теоретически «свести концы с концами», построить марксистски выдержанную систему уголовной репрессии. К разрешению этой задачи советское законодательство подходит в 1924 г., когда на повестку сессии ЦИК СССР ставится вопрос об издании предусмотренных союзной Конституцией Основных начал уголовного законодательства Союза ССР и союзных республик. Изданные 31 октября 1924 г., эти Основные начала, выбросившие из советского уголовного права самое понятие наказания, действительно означают большой прогресс по сравнению с УК 1922 г. На основании Основных начал в союзных республиках приступают к переработке республиканских уголовных кодексов. Таким образом, начавшийся с 1924 г. и продолжающийся по сие время этап в развитии советского уголовного права можно охарактеризовать как период переработки уголовного законодательства как в направлении дальнейшего урегулирования карательной политики в соответствии с потребностями жизни, так и в направлении достижения марксистской выдержанности, с устранением всех некритически воспринятых прежде пережитков буржуазных взглядов и теорий. В процессе этой переработки сессия ВЦИК в октябре 1925 г. пришла к выводу о необходимости внести некоторые поправки и в сам текст Основных начал, и вопрос об этом обсуждался на апрельской сессии ЦИК СССР.

Не следует, однако, думать, что даже по важнейшим вопросам уголовного законодательства у нас в настоящее время уже достигнута полная ясность. Взять хотя бы вопрос о «революционном правосознании». Статья 9 УК 1922 г. указывала, что «назначение наказания производится судебными органами по их социалистическому правосознанию с соблюдением руководящих начал и статей настоящего Кодекса»; в Основных началах ни одна статья о необходимости для суда руководствоваться своим революционным или социалистическим правосознанием не упоминает. Между тем ст. 45 принятого ВЦИК проекта УК снова повторяет: «При назначении осужденному судебноп-исправительной меры суд руководствуется <...> в) своим социалистическим правосознанием».

Еще в 1922 г. на III сессии ВЦИК IX созыва, при обсуждении проекта УК было отмечено (в выступлении тов. Бройдо⁴), что «если мы прежде говорили: закона нет, пусть данный судья руководствуется социалистическим правосознанием, то здесь мы говорим: социалистическое правосознание оформлено в виде кодекса, который извольте исполнять». В самом деле, что такое правосознание? Обычно в буржуазной литературе под этим словом понимается правовое сознание; П. И. Стучка выдвинул утверждение, что наше «классовое правосознание есть классовое сознание (т.е. сознание классового интереса)»⁵. В первом случае необходимым элементом правосознания является юридический фетишизм, при котором отношения между людьми рассматриваются через «юридические очки»



³ Доклад тов. Крыленко на 2-й сессии ВЦИК XII созыва (стеногр. отчет, с. 335).

⁴ См.: Бюллетень сессии. 1922. № 4. С. 10.

⁵ См.: Стучка П. И. Заметки о классовой теории права // Советское право. 1922. № 3. С. 15.

(выражение Энгельса). Стихийно вырабатываемая пролетариатом идеология, конечно, не свободна и от такого правосознания, слишком долго навязывавшегося буржуазией пролетариату (ср.: Ленин. Что делать, гл. II), и потому тов. Стучка был безусловно прав, когда в цитированной статье говорил: «Правосознание с полным основанием можно назвать главным элементом исторических предрасудков в нас».

Во втором случае пролетарий, по Энгельсу, рассматривает «вещи в их действительности, без юридических очков»; оценивая с этой точки зрения взаимоотношения людей, он подходит к ним не юридически, а политически. Любопытно, что о революционном правосознании не вспомнили ни при составлении Гражданского кодекса, ни при составлении Гражданского процессуального кодекса. В последнем правосознание прямо заменено политическим подходом: «За недостатком узаконений и распоряжений для решения какого-либо дела, суд решает его, руководствуясь общими началами советского законодательства и общей политикой рабоче-крестьянского правительства» (ст. 4 ГПК). Основная «юридическая идея» есть «идея эквивалента», по правильному замечанию тов. Пашуканиса. Может быть, именно потому, что гражданское право — даже у нас — есть идея эквивалента, развитая в 435 статьях, никому и не пришла в голову желательность включения в ГК специальной статьи о правосознании, т.е. о «юридической идее». Но не с уголовным правом. Идея эквивалента в уголовно-правовой области выражена в идее «справедливого возмездия». Попытка покончить с этой идеей была сделана у нас еще в 1919 г., когда были изданы Руководящие начала, о принципиальной позиции которых по вопросу о «вине» и «возмездии» сказано в начале статьи. И вот: «гони природу», то бишь юридический фетишизм, «в дверь, она влетит в окно». УК 1922 г. в теории остался на точке зрения Руководящих начал, на практике же ему от идеи справедливого возмездия полностью отгородиться не удалось. Отсюда и ст. 9 УК о правосознании и п. 4 ст. 413 УПК об отмене приговора в случае явной несправедливости такового.

Вот именно, скажут нам. Вы хотели создать «сухую воду» — создать уголовное право без справедливости? Но право должно содержать юридическую идею точно так же, как кофе должен содержать кофеин. Вы были непоследовательны именно потому, что ваша последовательность зарезала бы наше право. Оставайтесь же непоследовательны.

В тему нашей статьи не входит разработка вопроса, возможно ли существование права без юридической идеи. Мы ограничиваемся поэтому только тем, что на вопрос отвечаем вопросом: какая юридическая идея сообщает правовой характер Конституции СССР или РСФСР, конституции, всё содержание которой составляет развитие идеи совсем другого, не юридического порядка — идеи диктатуры пролетариата? Констатируя, что уголовное право теснейшим образом соприкасается с государственным правом, мы готовы, однако, признать, что в нашем уголовном праве есть юридическая идея, но не идея справедливого возмездия, а идея революционной законности.

Мыслимы два, и только два, принципиальных критерия для применения к осужденному меры уголовной репрессии: либо критерий целесообразности, либо критерий справедливости. Для марксиста, борющегося с юридическим фетишизмом, единственно приемлем первый, совершенно неприемлем второй. Но применяемые властью в борьбе с преступностью меры целесообразности, т.е. меры социальной

защиты, могут быть ничем юридически не ограничены и могут быть ограничены. В эпоху военного коммунизма единственным руководящим для судов началом была директива сообразоваться с революционным правосознанием; она же была и единственным ограничением усмотрения, единственной — пусть скудной — гарантией для граждан, ибо приговоры судов подлежали отмене в случае их несоответствия с нею. Она только и делала наше уголовное право правом; понятно, почему кое-кто из нас и сейчас не мыслит Уголовного кодекса без статьи о революционном правосознании.

В эпоху нэпа, при революционной законности, гарантией для граждан от произвольного применения к ним мер социальной защиты является Уголовный кодекс. Это не ново, и это не является особенностью советского уголовного права: уже буржуазные юристы говорили, что уголовный закон является *Magna Charta* (Великой хартией вольностей) для преступника и при том обеспечивает последнего потому, что в основу уголовного законодательства положен принцип: *Nullum crimen, nulla poena sine lege poenale* (ни преступления, ни наказания без уголовного закона), т.е.: преступное преступно, лишь когда об этом сказано в уголовном законе, и наказание может быть назначено лишь предусмотренное уголовным законом. Дав, однако, преступлению определение неформальное (преступление — деяние, воспрещенное законом под страхом наказания), а определение по существу (преступление — общественно опасное для пролетарского государства деяние, хотя бы и не предусмотренное законом), мы урезали гарантию наполювину; все же вторая часть формулы буржуазных криминалистов имеет полную силу и с точки зрения нашего уголовного права. Да и первая часть этой формулы не является абсолютно для советского права неприемлемой.

Конечно, материальное определение преступления не может быть в советском праве заменено формальным определением. Наказуемое деяние могло бы становиться просто в силу закона, как формально воспрещенное. Но если мы термин «наказуемое деяние» отбрасываем и вместо него ставим термин «деяние, влекущее за собой меры соц. защиты», то ясно, что защищаться приходится только от того, что опасно. Коррелятом наказания является «вина» — коррелятом меры соц. защиты является опасность. Отсюда вытекают два вывода: деяние, являющееся для нас социально опасным, может влечь за собой меры соц. защиты, даже если оно не предусмотрено в УК; с другой стороны, деяние, в данном своем виде вовсе не являющееся социально опасным, может не влечь за собой применение мер соц. защиты, даже если деяния того же состава и предусмотрены в УК вследствие заключающейся в них обычно социальной опасности...

Первый вывод сделан в не допускающей никаких сомнений форме еще в 1922 г., когда при составлении УК в него была включена ст. 10 об аналогии. Ко второму выводу наше законодательство очень робко подошло только в 1925 г., когда была сформулирована ст. 4а УПК. Статья эта, однако, очевидно, не считалась необходимой принадлежностью советского уголовного права, ибо она включена была не в УК, а только в УПК. В настоящее время в руководящих органах советской юстиции ст. 4а УПК встречает сильную оппозицию, и ее предлагают упразднить как приводящую на практике к прекращению уголовных дел по

усмотрению того или иного суда и тем идущую вразрез с принципом революционной законности⁶.

Между тем ст. 4а УПК является таким же теоретически законным выводом из положения, что преступлением признается у нас всякое общественно опасное деяние, как и ст. 10 УК об аналогии. И все же только лица, склонные к *Begriffsjurisprudenz* (юриспруденции, сводящей все к юридической логике), могли бы возражать против необходимости обсудить, насколько политически целесообразно придание этому теоретически корректному выводу юридической силы. На практике ст. 10 УК в настоящее время большого применения не имеет. Если бы наши суды чаще пользовались ею, то, несомненно, против этой ст. 10 УК поднялась бы такая же оппозиция, как против ст. 4а УПК. Во всяком случае вопрос о соответствии и этой статьи задаче укрепления революционной законности стал бы тогда дискуссионным.

Лично мы считаем, что исключение ст. 4а из нашего законодательства (с нашей точки зрения, ее нужно сохранить) возможно лишь при одновременном изменении некоторых других его постановлений. В настоящее время и Основные начала и — еще более определенно — принятый ВЦИК в октябре 1925 г. новый УК признали невозможным сохранить старый подход к покушению и приготовлению, при котором уголовной репрессии подлежало лишь первое, но не второе. Теоретически эта новая постановка вопроса является, безусловно, шагом вперед, хотя новой ее можно назвать, лишь игнорируя тот факт, что принципиальное разграничение приготовления от покушения стало проводиться буржуазными юристами лишь с начала XIX века, и что в одном из буржуазных государств — Дании — это разграничение не вошло даже в Уголовный кодекс, составленный в середине XIX века. Как бы то ни было, буржуазные криминалисты потерпели полное фиаско при разрешении задачи, как отграничить приготовление от покушения⁷. Кроме этого обстоятельства, решающим для нашего законодательства соображением было то, что приготовление к преступлению может быть опасным, — конечно, потенциально опасным — но ведь, в сущности, этим свойством потенциальности отличается всякая опасность, ибо реализация опасности, когда уже наступил тот вред, которым она угрожала, есть в определенном смысле ликвидация опасности; во всяком случае приготовление может свидетельствовать о явной социальной опасности того, кто готовится к преступлению.

Итак, приготовление к преступлению теоретически есть уже преступление. Это зафиксировано в ст. 19 нового УК РСФСР. Но всегда ли нужно и целесообразно предавать суду и применять уголовную репрессию за приготовление к преступлению? Здесь необходима сугубая сдержанность и осторожность. Тов. Самурский, представитель Дагестанской ССР, говорил на последней сессии ВЦИК: «Возьмите представляемую мною республику, где еще существует кровная месть. Кровники постоянно держат наготове кинжалы или винтовки. И если мы применим к ним

⁶ «Мы ее выкинем», — сказал тов. Крыленко на 2-й сессии ВЦИК XII созыва (стеногр. отчет, с. 338). Так обстояло дело в момент, когда настоящая статья писалась (весною 1926 г.). К моменту же напечатания ее спор по поводу ст. 4а разрешился тем, что ее не только не «выкинули», но — в несколько измененном виде — перенесли из УПК в УК.

⁷ См. нашу статью «Деяние» в «Энциклопедии государства и права».

этот пункт, мы должны будем всех наказывать, потому что почти 2/8 населения на наших окраинах являются кровниками»⁸. С другой стороны, по вполне понятным соображениям уголовной политики, добровольно оставленное покушение или приготовление не подлежит уголовному преследованию, если в нем не заключается иного преступления (ст. 19, ч. 2 нового УК). Ну, а если суд при разборе дела лица, привлеченного за приготовление к преступлению, приходит к выводу, что даже и без вмешательства власти «преступник» едва ли в дальнейшем приступил бы к активному осуществлению своего намерения? Хотя это приготовление в данный момент вовсе не является «добровольно оставленным», и потому суд обязан на основании ч. 1, ст. 19 вынести обвинительный приговор, но разве в таком случае целесообразна уголовная репрессия? Абстрактно рассуждая, приготовление к общественно опасному действию можно признать, как таковое, уже общественно опасным действием. Но данное конкретное приготовление может оказаться все же совершенно безобидным, не стоящим внимания суда действием. Без права суда отказываться от преследования абстрактно преступного (т.е. формально преступного) действия по мотивам его конкретной безобидности, маловажности, т.е. без права суда на применение ст. 4а УПК, которая именно об этом и говорит, практика суда рискует оказаться непрактичной, рискует привести суд в противоречие с бытом. Похерить ст. 4а можно только при одновременном ограничении понятия уголовно преследуемого приготовления.

Необходимо помнить, что и уголовная репрессия нуждается в режиме экономии. Раньше наш УК признавал наказуемыми все случаи покушения, начиная от покушения на тяжчайшее преступление и кончая покушением на нарушение порядка, предусмотренным главой VIII УК. Теперь это же распространяется и на все вообще подготовительные к преступлению действия. Буржуазные кодексы обычно признают случаи покушения на более легкие преступления ненаказуемыми вовсе. Уголовный кодекс при этом несколько теряет в стройности, ибо не все положения Общей части в нем оказываются одинаково применимыми ко всем главам Особенной части, как это обстоит у нас.

Но нам вовсе не нужна та стройность, которая сводится к жесткой прямолинейности. Стройность, необходимая для советского права, должна быть результатом принципиальной выдержанности в духе марксизма, и именно потому она не может исключать гибкости.

Мы сказали, что основное положение советского уголовного права заключается в том, что критерием для применения уголовной репрессии берется не справедливость, а целесообразность этой репрессии в качестве меры обороны. Нетрудно показать, что до сих пор некоторые очень серьезные вопросы разрешены у нас с этой точки зрения чрезвычайно невыдержанно.

⁸ Стеногр. отчет 2-й сессии XII созыва (с. 391).

**Вячеслав Николаевич
ВОРОНИН,**
доцент кафедры
уголовного права
Университета имени
О.Е. Кутафина (МГЮА),
кандидат юридических
наук, доцент

Подлинный анекдот «Петр Великий не прощает при смертной своей болезни убийц»¹

Якоб фон Штелин (нем. Jacob von Stäehlin, 9 мая 1709 г., Мемминген — 6 июля 1785 г., Санкт-Петербург) — немецкий ученый, гравер, картограф и мемуарист, большую часть жизни проработавший в России. Он был видным деятелем Петербургской академии наук и одним из первых историографов русского искусства.

В 1735 г. Штелин был приглашен в Санкт-Петербургскую академию наук, где занимался различными проектами, включая организацию фейерверков, иллюминаций и медалей. Он также преподавал красноречие и поэзию, а позже стал наставником и библиотекарем наследника престола Петра Федоровича (будущего императора Петра III). Штелин принимал участие в создании первого официального атласа Российской империи и возглавлял художественный департамент Академии наук, способствуя развитию гравирования и изобразительного искусства в России.

«Подлинные анекдоты о Петре Великом» — это сборник кратких эпизодов из жизни императора Петра I, собранных Штелиным на основе воспоминаний его современников. Книга была впервые издана на немецком языке в 1785 г. в Лейпциге, а затем переведена на русский язык и опубликована в Москве². Штелин стремился сохранить от забвения достопамятные анекдоты о Петре Великом, записывая рассказы от 52 человек, включая князя И. Ю. Трубецкого и канцлера А. П. Бестужева.

Эти истории, изложенные легким слогом, представляют уникальный взгляд на личность и деяния Петра I, отражая его характер, привычки и отношения с окружающими, являются отражением эпохи.

Царь Петр I, на 25 году от рождения своего, был опасно болен горячкою; когда уже не оставалось надежды к его выздоровлению и всем двором печаль овладела, в церквах же денно и нощно приносились за царя молитвы, то по древнему обыкновению явился судья преступников, чтоб спросить, не дать ли свободу девятерым разбойникам и убийцам, приговоренным к смерти, дабы они молили Бога о здравии царском. Как скоро Петр I сие услышал, то приказал судью позвать пред себя и повелел ему прочесть лист сих, к смерти приговоренных, и их



¹ См.: Подлинные анекдоты о Петре Великом, слышанные из уст знаменитых особ в Москве и Санкт-Петербурге, извлеченные из забвения Яковом фон Штелиным. Ныне же вновь переведенные с немецкого на русский язык; с прибавлением многих других на русском языке не изданных анекдотов; с присовокуплением гравированных фигур. Часть первая. М., 1787.

Подготовлено с использованием интернет-ресурсов.

² URL: https://kp.rusneb.ru/item/material/podlinnye-anekdoty-o-petre-velikom-ch1?utm_source=chatgpt.com.

преступления. Потом сказал его величество прерывающимся голосом к уголовному судье: «Разве ты думаешь, что я прощением сих недостойных злодеев и нарушением правосудия сделаю доброе дело и побужду небо к продлению моей жизни? Или что Бог примет молитву сих богоотступных мошенников и убийц? Пойди сей час и вели заутренняго утра исполнить приговор над девятью преступниками. Я паче надеюсь, что Бог таковым моим правосудием побужден будучи к милосердию, продлит жизнь мою и дарует мне здравие».

Приговор был на другой день исполнен, царю стало ежедневно становиться легче, и спустя малое время он совершенно выздоровел.

В анекдоте приводится изложение события, имевшего, предположительно, место в 1696 г., когда Петру I было 24 года.

Исторически известно, что 1696 г. был годом, решающим для Петра I, ознаменованным смертью его соправителя царя Ивана V и началом единоличного правления самого Петра, завершением второго Азовского похода, который он возглавлял, основанием регулярного российского флота.

В сохранившихся исторических источниках того периода нет достоверных сведений о тяжелой болезни Петра в этом году. Поэтому с исторической точки зрения факт болезни Петра вполне может быть литературным преувеличением либо некой легендой, возникшей позже и призванной подчеркнуть его образ праведного и справедливого правителя (в конце анекдота приводится пояснение, что «известно сие от Петра Миллера, железного заготовщика, который был в тот самый день при царском дворе в Москве»).

Что касается смертной казни, то на 1696 г. действовали нормы Соборного уложения 1649 г., а также многочисленные указные положения и военные регламенты, дополнявшие его. Смертная казнь активно применялась за тяжкие преступления, такие как убийство, разбой, государственная измена, насильственные преступления и иные тяжкие правонарушения.

Упомянутые в анекдоте «разбойники и убийцы» подпадали под нормы гл. XXI Соборного уложения (о разбое и убийстве), предписывающие обязательное применение смертной казни при тяжких обстоятельствах. Обычай освобождения преступников во время тяжелой болезни государя, упоминаемый в анекдоте, не был четко зафиксирован в нормативных актах того времени, однако эпизод мог отражать бытовавшие представления об акте милосердия монарха, способном склонить небесные силы на его сторону.

Вероятно, что согласно традиционным представлениям того времени, молитва освобожденных преступников могла восприниматься как акт религиозного посредничества, который принесет выздоровление правителю. Петр I, согласно анекдоту, ясно и категорично выбирает правосудие как высшую ценность и отказывается от «магической» логики помилования с целью собственного исцеления. Его слова («Я не могу нарушить закон даже при смертной своей болезни») подчеркивают





его приверженность принципам законности и неотвратимости наказания, которые он поставил выше личного благополучия и страха перед смертью.

Изложенный в анекдоте поступок вполне вписывается в исторический портрет царя-реформатора, отражает стремление Петра к отходу от средневековых суеверий и традиций в сторону более современных, ориентированных на закон норм. Последующая законотворческая деятельность Петра Великого в сфере уголовного права ознаменовалась кодификацией военно-уголовного законодательства³ — принятием в 1715 г. Артикула воинского, содержавшего 209 статей, из которых 74 предусматривали смертную казнь за различные преступления, включая измену, дезертирство, бунт и др.⁴

³ Рарог А. И. Наследие Петра Великого и современное военно-уголовное право России // Вестник Университета имени О.Е. Кутафина (МГЮА). 2024. № 4. С. 29—38.

⁴ Российское законодательство X—XX вв. : в 9 т. М. : Юридическая литература, 1986. Т. 4 : Законодательство периода становления абсолютизма / отв. ред. А. Г. Маньков.



ISSN 2311-5998



9 772311 599771 >