Л.Н. Гумилев атындағы Еуразия ұлттық университетінің ХАБАРШЫСЫ.
ISSN: 2616-6844. eISSN: 2663-1318

ҚҰҚЫҚ СЕРИЯСЫ/ LAW SERIES/ СЕРИЯ ПРАВО

Қылмыстық құқық. Қылмыстық процесс / Criminal law. Criminal procedure/ Уголовное право. Уголовный процесс

МРНТИ 10.81.45. *https://doi.org/10.32523/2616-6844-2026-155-2-199-223*
Научная статья.

Особенности классификаций видов, типов и форм организованных преступных групп трансграничного характера в области конструкции и распространения маркеров массового воздействия в социальных сетях

Е.С. Шалхаров[1], А.Н. Нартай*[2], Г.М. Рысмагамбетова[3]

[1,2]Международный казахско-турецкий университет имени Х.А. Ясави. Туркестан, Казахстан
[3]Карагандинский национальный исследовательский университет им. академика Е.А. Букетова

(e-mail: [1]yernar_shalkharov@list.ru, [2]sarapshy.tk@mail.ru, [3]gulnaramusievna@bk.ru)

Аннотация. Данная статья посвящена исследованию особенностей классификации организованных преступных формирований трансграничного характера, действующих в цифровой среде и формирующих маркеры массового воздействия в социальных сетях. В работе выделены пять видов таких групп: сетевые координационные ядра, гибридные криминально идеологические объединения, квазилокальные медийные платформы, анонимные распределенные сообщества и временные мобилизационное кластеры. Определены три типа структур: централизованный, децентрализованный и смешанный. дополнительно раскрыты семь форм функциорования: информационные вбросы, вирусные флешмобы, координированные кампании травли, манипулятивные нарративы, фабрикация событий, использование ботовых сетей и скрытая реклама деструктивных идей. Цель исследования состоит в разработке целостной криминологической модели классификации указанных формирований и выявлении их влияния на общественную стабильность. Работа выполнена в русле национальной безопасности, оперативной деятельности, мониторинга и анализа цифровых следов, профайлинга угроз и теории организованной преступности. Методологическую основу составили когортный анализ и исследование корреляционной динамики распространения деструктивного контента.

Результаты показали устойчивую связь между активностью указанных структур и возникновением межэтнических, межнациональных, межрелигиозных конфликтов, призывов к беспорядкам, формированием негативных идеологий, делигитимацией власти, дестабилизацией институтов, радикализацией молодежи и ростом социальной напряженности. При этом

Поступила: 08.05.2026 Одобрена: 29.06.2026 Доступна онлайн: 30.06.2026

***автор для корреспонденции**

рассматривались элементы таких событий из исторической хронологии как «Жана Озен», «Маловодный», «Чилик», «Алишер Навои», «Архан Керген», «Жамыл Тасовский эпизод», «Кордай» и «Кантар». Исследование направлено на конструкцию прогнозирующего и профилактического инструмента. Научная значимость заключается в уточнении понятийного аппарата и расширении типологии организованных преступных групп в цифровой среде. Практическая ценность выражается в возможности использования предложенной классификации для прогнозирования угроз, разработки мер противодействия и совершенствования оперативно аналитической деятельности. Дополнительно установлены такие виды воздействия, как распространение панических настроений, подрыв доверия к правоохранительным органам, искажение исторической памяти, усиление миграционных конфликтов, экономическая дестабилизация, рост киберпреступности, формирование теневых сетей влияния, а также вовлечение несовершеннолетних в противоправную активность. Полученные выводы конкретизируют механизмы скрытого управления массовым поведением и могут быт применены при разработке превентивных стратегий государственного уровня и межведомственного взаимодействия структур.

Ключевые слова: трансграничная организованная преступность, социальные сети, маркеры массового воздействия, деструктивный контент, информационные операции, профайлинг угроз, национальная безопасность.

Введение

Данная статья обращается к проблеме, которая еще недавно казалась вторичной и повседневной, а теперь спокойно вмешивается в вопросы национальной безопасности. Речь идет о трансграничных организованных преступных формированиях, которые действуют не через классические каналы, а через социальные сети, создавая управляемые информационные события и формируя маркеры массового воздействия. Сам по себе феномен организованной преступности изучен достаточно глубоко, однако его цифровая трансформация и эволюция происходит быстрее, чем наука успевает зафиксировать устойчивые закономерности. В этом и возникает та самая проблемная зона, которая обычно игнорируется до первого серьезного кризиса. Актуальность темы обусловлена тем, что современные социальные сети перестали быть просто площадками для коммуникации. Они стали инструментами влияния, причем влияние это носит многослойный и часто скрытый характер. Организованные группы используют цифровую среду для конструирования событий, которые воспринимаются обществом как спонтанные. В реальности за ними стоит расчет, координация и вполне конкретные интересы. При этом в научной литературе отсутствует единая классификация таких формирований, их типов и форм функционирования. Исследования либо сосредоточены на киберпреступности в узком смысле, либо на информационных войнах, но связка с теорией организованной преступности остается фрагментарной. Объектом исследования выступают общественные отношения, возникающие в процессе

функционирования трансграничных организованных преступных групп в цифровой среде. Предметом являются закономерности их классификации, а также механизмы формирования и распространения маркеров массового воздействия в социальных сетях. Цель исследования заключается в разработке комплексной криминологической модели, позволяющей системно описать виды, типы и формы таких групп т выявить их влияние на общественные процессы. Для достижения поставленной цели сформулированы задачи, которые логично вытекают одна из другой, хотя на практике их выполнение напоминает разбор сложной схемы с постоянно меняющимися элементами. Во-первых, необходимо определить признаки трансграничности и организованности в условиях цифровой среды. Во-вторых, требуется выделить устойчивые виды и типы преступных формирований. Если эти закономерности выявить и систематизировать, становится возможным не только описание, но и прогнозирование угроз. Научная и практическая значимость работы определяется тем, что она предлагает попытку объединить несколько направлений исследований, которые до этого существовали параллельно. Речь идет о теории организованной преступности, исследованиях цифровых коммуникаций и практике обеспечения национальной безопасности. Такое объединение позволяет по-другому взглянуть на привычные категории и, возможно, пересобрать их под новые реалии. Практическая ценность заключается в возможности применения полученных результатов в оперативной деятельности, в разработке аналитических инструментов и в формировании превентивных мер. Обзор литературы показывает, что зарубежные исследования активно развиваются в направлении изучения цифровых угроз, однако часто рассматривают их через призму кибербезопасности или политической коммуникации. Традиционные исследования организованной преступности в основе своей в большинстве данных источников фокусируются на её экономических и насильственных проявлениях, игнорируя информационную составляющую. Хотя работы по дезинформации и манипуляциям в соцсетях описывают механизмы распространения контента, они редко учитывают организованный и трансграничный характер этих явлений, где даже существует ряд исследований, анализирующие децентрализованные сетевые структуры, но они не всегда объясняют наличие скрытых центров управления. Он также важно отметить, что оно не претендует на окончательное решение всех вопросов, что было бы слишком самонадеянно, но стремится задать рамку, в которой дальнейшие исследования смогут двигаться более осмысленно. В итоге введение подводит к основной части исследования, где предложенная классификации будет раскрыта более детально, а также будет показано, каким образом теоретические положения могут быть применены на практике. Без этого вся конструкция осталась бы просто еще одной красивой схемой, которые так любят в академической среде, но редко используют в реальной работе.

Материалы и методы исследования

Методология настоящего исследования выстроена с учетом междисциплинарного характера изучаемой проблемы и ориентирована на воспроизводимость полученных результатов в условиях различных исследовательских сред. В центре внимания находится исследовательский вопрос, который формулируется следующим образом: обладают ли трансграничные организованные преступные формирования, функционирующие

в цифровой среде социальных сетей, устойчивыми признаками, позволяющими их классифицировать по видам, типом и формам воздействия, и возможно ли на основе этих признаков прогнозировать их деструктивную активность. Указанный вопрос обусловлен необходимостью преодоления фрагментарности существующих подходов и перехода к системному анализу.

Гипотеза исследования заключается в том, что трансграничные организованные преступные группы, не находящиеся на территории Казахстана, действующие в социальных сетях, формируют повторяющиеся поведенческие паттерны, которые поддаются выявлению посредством комплексного анализа цифровых следов, и могут быть классифицированы по структурным и функциональным критериям. Дополнительно, предполагается. что корреляция между их активностью и социальными последствиями носит не случайный, а закономерный характер, что позволяет использовать выявленные зависимости в целях профилактики и оперативного реагирования.

Объектом исследования выступают процессы функционирования организованных преступных формирований в трансграничной цифровой среде. Предмет исследования включает совокупность методов, механизмов и инструментов, применяемых такими формированиями для создания и распространения маркеров массового воздействия в социальных сетях. В качестве эмпирической базы использованы массивы данных, включающие новостные сводки за период с 2018 по 2025 годы, выборки контента из популярных социальных платформ, а также обобщенные статические данные уголовной правовой статистики и специальных учетов. Количественно материал исследования охватывает более двухсот тысяч единиц цифрового контента, включая текстовые сообщения, визуальные элементы и метаданные распространения. Качественный анализ проводился на репрезентативной выборке, сформированной с учетом временных, тематических и географических параметров.

Ход исследования был структурирован в несколько этапов, каждый из которых выполнял самостоятельную аналитическую функцию. но в совокупности обеспечивал достижение поставленной цели.

На первом этапе осуществлялся сбор и предварительная очистка данных. Удалялись дублирующиеся записи, а также контент, не имеющий признаков целенаправленного воздействия.

На втором этапе проводилась разметка данных с выделением ключевых признаков, включая источники распространения, скорость реп лекции, эмоциональную окраску и наличие координационных сигналов.

На третьем этапе применялись аналитические методы, направленные на выявление закономерностей и формирование классификационных моделей.

Заключительный этап включал интерпретацию результатов, их сопоставление с теоретическими положениями и формирование выводов.

Ключевым методом, примененным в исследовании, выступает спектральный анализ, адаптированный к задачам криминологического изучения цифровых структур. В классическом понимании спектральный анализ используется для выявления частотах характеристик сигналов, однако в данном исследовании он применен для выявления повторяющихся паттернов активности в информационных потоках.

Временные мобилизационные кластеры проявляются в виде кратковременных, но интенсивных всплесков, совпадающих с определенными событиями.

Когортный анализ использовался для изучения динамики формирования и развития указанных групп. В рамках данного метода формировались когорты пользователей и информационных потоков, объединенных по признаку времени возникновения и тематической направленности. Наблюдение за их поведением в динамике позволило выявить три типа структур.

Централизованный тип характеризуется наличием четко выраженного ядра, которое инициирует и координирует активность.

Децентрализованный тип представлен множеством относительно автономных элементов, взаимодействующих без явного центра.

Смешанный тип сочетает признаки первых двух, включая наличие скрытых центров координации при сохранении внешней децентрализованной.

Метод корреляционной динамики применялся для установления взаимосвязей между активностью исследуемых групп и социальными последствиями их деятельности. В качестве переменных использовались показатели интенсивности распространения контента, частота упоминаний, определенных тем, а также данные о социальных событиях, зафиксированных в новостных сводках и статических источниках. Расчет коэффициентов корреляции позволил установить устойчивые связи между активностью групп и формированием семи форм функционирования. Информационные вбросы проявляются в резком увеличении объема однотипного контента. Вирусные флешмобы характеризуются экспоненциальным ростом вовлеченности. Координированные кампании травли выявляются через синхронность негативных сообщений. Манипулятивные нарративы формируются через устойчивое повторение определенных смысловых конструкций. Фабрикация событий определяется через несоответствие между информационным шумом и фактическими данными. Использование ботовых сетей фиксируется через аномалии в поведении аккаунтов. Скрытая реклама деструктивных идей проявляется в большинстве своем гипотетическим в интеграции таких идей в более нейтральный и казалось бы безобидный контент.

• Деструктивные идеи могут незаметно проникать в общественное сознание, будучи вплетенными в безобидный, на первый взгляд, контент социальных сетей в инстаграм, тик ток и других ..

• Внедрение таких вредоносных деструктивных идей в нейтральные материалы является один из способов их скрытого продвижения, то есть лоббирования самой деструктивной идеи.

• Маскировка деструктивных идей под видом обычного контента это как правило распространенная тактика их распространения среди подавляющих масс общественности.

Дополнительным методом выступил правовой эксперимент, которые в юридических науках используется редко, но тем не менее, направлен на оценку эффективности существующих правовых механизмов противодействия рассматриваемым явлениям ну или феноменам. В рамках эксперимента моделировались ситуации распространения деструктивного контента с последующей оценкой реакции правоприменительных органов. Это позволило выявить временные задержки, пробелы в регулировании и недостатки в координации между различными субъектами.

• Для проверки действенности существующих законов и мер борьбы с подобными явлениями был проведен правовой эксперимент. В ходе него имитировались случаи

распространения вредоносного контента, и анализировалась реакция соответствующих государственных органов. Это существенно помогло обнаружить задержки в реагировании, законодательные нормы и проблемы во взаимодействии между различными участниками процесса.

• Эффективность правовых инструментов, предназначенных для борьбы с исследуемыми проблемами, была протестирована посредством так называемого, применённого исследовательской группой правового эксперимента, в пределах которого были предприняты конструкции различного рода сценариев, где предположительно и гипотетически может распространяться деструктивный контент.

Рассматривая и анализируя огромные блоки литературных данных отчесевтенных источников, а также источников стран ближнего и дальнего зарубежья можно было увидеть чисто классические методлики научного изучения, в котором применялись методики дедукции, индукции, аьстрагирования, синтеза, моделирования и других.

Результаты наших исследования маркеров исследования показали, что предложенная методологическая конструкция позволяет не только описывать, но и объяснять механизмы функционирования трансграничных организованных преступных формирований. Выявленные виды, типы и формы демонстрируют устойчивость и воспроизводимость в различных условиях. При сопоставлении с существующими исследованиями установлено, что многие из выявленных закономерностей ранее фиксировались фрагментарно, однако их системное объединение отсутствовало.

• Исследование продемонстрировало что разработанный методологический подход позволяет не просто описать, но и объяснить, как действуют транснациональные организованные преступные группы. Обнаруженные разновидности, категории и формы их деятельности оказались устойчивыми и повторяющимися в разных обстоятельствах. Сравнительный анализ с предыдущими работами показал, что многие из выявленных закономерностей уже были замечены, но не были систематизированы.

Она открывает перспективы для дальнейших исследований и создает основу для разработки прикладных инструментов, направленных на выявление и нейтрализацию угроз в цифровой среде.

Формирование выборки и критерии отбора данных. Для обеспечения репрезентативности исследования была сформирована многоуровневая выборка цифрового контента, опубликованного в социальных сетях Instagram, TikTok, Facebook, Telegram и X (ранее Twitter). Период сбора данных охватывал временной интервал с января 2018 года по декабрь 2025 года, что позволило проанализировать как краткосрочные информационные кампании, так и долгосрочные тенденции распространения маркеров массового воздействия. В исследование включались сообщения, содержащие признаки координированного информационного воздействия, деструктивных нарративов, искусственного повышения вовлеченности, распространения панических настроений, межэтнической, межрелигиозной либо социально конфликтной риторики, а также признаки деятельности организованных сетевых структур. Критериями включения являлись открытый доступ к публикациям, наличие текстового, визуального или мультимедийного контента, возможность идентификации временных характеристик публикации, а также наличие показателей вовлеченности пользователей. Из выборки исключались дублирующиеся сообщения, рекламный контент коммерческого характера, публикации с недостаточным объемом данных для анализа, автоматические системные

уведомления, а также материалы, не содержащие признаков целенаправленного информационного воздействия. Общий массив исследованных данных составил 200 000 единиц контента, из которых 55 000 сообщений были получены из Instagram, 50 000 из TikTok, 35 000 из Facebook, 30 000 из Telegram и 30 000 из X. Для минимизации систематической ошибки использовалась стратифицированная выборка, при которой данные распределялись по платформам, временным периодам, тематическим категориям и географическим признакам. Внутри каждой страты применялся механизм случайного отбора сообщений, что обеспечило статистическую сбалансированность выборки и повысило достоверность полученных результатов. Использованный подход позволил сформировать репрезентативную эмпирическую базу для выявления закономерностей функционирования трансграничных организованных преступных формирований в цифровой среде.

Проверка надежности и воспроизводимости результатов. Для обеспечения достоверности, надежности и воспроизводимости полученных результатов в исследовании была реализована многоступенчатая процедура контроля качества данных и верификации аналитических выводов. Особое внимание уделялось минимизации субъективного влияния при классификации цифрового контента и интерпретации выявленных маркеров массового воздействия. На первом этапе проводилась независимая проверка корректности кодирования материалов. Для этого из общего массива данных случайным образом была отобрана контрольная подвыборка, составляющая 15 % исследуемого контента. Отобранные материалы подвергались повторному кодированию двумя независимыми экспертами, обладающими опытом в области криминологии, анализа социальных сетей и информационной безопасности. Согласованность результатов оценивалась посредством расчета коэффициента Cohen's Kappa, который составил 0,82. Полученное значение свидетельствует о высокой степени согласованности экспертных оценок и подтверждает надежность используемой классификационной модели. На втором этапе осуществлялась процедура повторной проверки выборки. Дополнительно 10 % ранее проанализированных материалов подвергались повторному исследованию спустя тридцать календарных дней после первоначального анализа. Результаты показали уровень совпадения классификационных решений на уровне 88,6 %, что свидетельствует об устойчивости выявленных закономерностей и отсутствии существенных временных колебаний в интерпретации данных. На заключительном этапе проводилась экспертная валидация результатов. К оценке были привлечены специалисты в области криминологии, национальной безопасности, цифровой криминалистики и анализа информационных угроз. Экспертам предоставлялись обобщенные классификационные модели, перечни выделенных признаков и результаты корреляционного анализа. По итогам экспертной оценки более 85 % предложенных классификационных решений были признаны обоснованными и пригодными для практического использования в деятельности аналитических и правоохранительных подразделений. Проведенные процедуры подтверждают высокий уровень надежности, воспроизводимости и научной состоятельности полученных результатов исследования.

Результаты и обсуждение

Обсуждение результатов исследования требует сопоставления полученных данных с уже существующими научными подходами, сформированными в зарубежной и

частично отечественной литературе. При этом важно учитывать, что значительная часть исследований в данной области развивается фрагментарно, без формирования единой теоретической конструкции, что и обусловило необходимость предложенной классификации.

Согласно казахстанским исследованиям в области цифровой криминологии и анализа информационных угроз, проведенным в рамках межуниверситетских программ изучения киберрисков, установлено, что современные организованные структуры все чаще переходят от жесткой иерархии к гибким сетевым моделям [1]. При этом особое внимание уделяется так называемым координационным центрам, которые формируют ключевые информационные сигналы [2]. Эти выводы прямо коррелируют с выделенным в настоящем исследовании видом сетевых координационных ядер. Их основная характеристик заключается не столько в численности, сколько в способности задавать повестку и управлять ритмом распространения информации. В отличие от классических преступных структур, такие ядра могут существовать в латентном состоянии, активизируясь только в определенные периоды [3].

В соответствие с исследованиями Поздняковой, проводимые в университетах, специализирующихся на анализе социальных сетей и цифрового поведения, показывают, что наиболее устойчивыми оказываются гибридные структуры, сочетающие криминальные и идеологические элементы [4]. В частности, ученые отмечают, что финансовые интересы таких групп тесно переплетаются с распространением определенных нарративов. Это подтверждает выделение гибридных криминально идеологических объединений как самостоятельного вида. Профессор Муминов также отметил, что их отличительная черта состоит в том, что они не ограничиваются получением прибыли, а стремятся к долгосрочному влиянию на общественное сознание, формируя устойчивые установки и модели поведения [5].

Другие исследования проведенные Абдуллахом М.[6] акцентируют внимание на феномене квазилегальных медийный платформ как одних из самых распространенных [7]. При этом в данных исследованиях замечается очень много контента анонимного характера [8,9].

Исследования из разных стран показывают, что временные группы, возникающие в ответ на конкретные события, быстро распадаются после достижения цели. Их краткое существование затрудняет изучение, но именно они часто провоцируют резкий рост социальной напряженности. Именно наше исследование выявило, что эти группы формируются на базе существующих связей, но активируются специфическими факторами, такими как дезинформация или резонансные события.

Что касается структур то централизованный тип, несмотря на цифровизацию, остается эффективным для управления и координации как показывают американские исследования. Такие структуры имеют чёткое руководство, где их легче обнаружить из-за более заметных цифровых следов и распознавать конкретные маркеры воздействия на определенные группы человек. Децентрализованные же структуры по данным европейских исследований являются более устойчивы к внешним угрозам и могут функционировать даже при потере части участников хотя их координация менее эффективна, но тем не менее компенсируется массовостью и гибкостью. Смешанный тип, сочетающий черты обоих, наиболее труден для выявления и анализа. Анализ форм функционирования показывает, что информационные вбросы являются

базовым инструментом воздействия. Они представляют собой целенаправленное распространение информации, часто не соответствующей действительности, с целью формирования определенного восприятии. Согласно зарубежным исследованиям, такие вбросы часто используются как стартовый механизм для запуска более сложных процессов [16].

Вирусные флешмобы, как форма воздействия, характеризуются высокой скоростью распространения и вовлечения. Исследования показывают, что их эффективность обусловлена использованием эмоциональных триггеров и простых для воспроизведения действий. При этом инициаторы таких флешмобов часто остаются в тени, что затрудняет их идентификацию [17].

Координированные кампании травли представляют собой более агрессивную форму воздействия. Они направлены на дискредитацию конкретных лиц или групп и сопровождаются массовым распространением негативного контента [18]. В зарубежных исследованиях отмечается, что такие кампании часто организуются с использованием ботовых сетей и координационных центров [19].

Манипулятивные нарративы формируются через систематическое повторение определенных смысловых конструкций. Их цель заключается в постепенном изменении восприятия реальности [20]. Фабрикация событий, в свою очередь, предполагает создание информационных поводов, которые в действительности не имеют под собой реальной основы [21].

Использование ботовых сетей является ключевым инструментом масштабирования воздействия. Исследования показывают, что современные боты способны имитировать поведение реальных пользователей, что значительно усложняет их выявление [22]. Скрытое продвижение, вредоносных идей, происходит, когда эти идеи незаметно вплетаются в обычный или развлекательный контент. Такой подход ослабляет способность аудитории критически оценивать информацию.

Для обнаружения подобных схем в интернете предлагается анализировать цифровые следы. Это включает в себя изучение IP-адресов времени активности моделей поведения пользователей и их сетевых связей.

Первоочередная задача это группирование и перегруппирование IP-адресов для выявления необычно высокой активности в определенных местах. Особое внимание следует уделять использованию прокси-серверов и VPN так как это может свидетельствовать о попытках скрыть истинное местоположение что также является одним из знаков.

Анализ цифровых следов также требует сопоставления времени активности. Одновременные публикации, повторение одного и того же контента или совпадение временных интервалов могут указывать на скоординированные действия.

Теоретическое обоснование авторской классификации. Предложенная авторская классификация опирается на современные зарубежные концепции исследования сетевой преступности, цифровых угроз и организованных информационных воздействий. В основе модели лежат положения теории criminal networks, согласно которым преступные структуры все чаще функционируют в форме гибких сетей, объединяющих участников через цифровые коммуникационные каналы. Выделенные в исследовании сетевые координационные ядра являются развитием концепции criminal network hubs, описывающей узлы управления, через которые осуществляется координация

участников, распределение задач и формирование информационной повестки. Гибридные криминально-идеологические объединения соотносятся с исследованиями social influence operations, рассматривающими сочетание информационного воздействия, психологических механизмов влияния и организационных структур, преследующих как политические, так и экономические цели. Категория квазилегальных медийных платформ соответствует современным представлениям о легитимизированных каналах распространения дезинформации и манипулятивных нарративов. Анонимные распределенные сообщества и временные мобилизационные кластеры концептуально близки к феномену coordinated inauthentic behaviour, используемому для описания скрыто координируемой активности множества аккаунтов, создающих иллюзию естественной общественной реакции. Дополнительно предложенная классификация коррелирует с подходами, используемыми в информационных операциях НАТО, где особое внимание уделяется выявлению сетевых центров влияния, координационных механизмов и моделей распространения деструктивного контента. Результаты исследования также согласуются с аналитическими подходами Europol и UNODC, согласно которым современные трансграничные преступные сети активно используют цифровые платформы для управления информационными потоками, мобилизации аудитории и формирования устойчивых моделей воздействия на общественное сознание. Таким образом, разработанная классификация не противоречит существующим международным научным подходам, а расширяет их применительно к задачам криминологического анализа и обеспечения национальной безопасности.

В целом, проведенное обсуждение подтверждает, что транснациональные организованные преступные группы в цифровом пространстве имеют сложную, но поддающуюся анализу структуру. Их эффективное противодействие возможно только при условии системного подхода, объединяющего научные и практические методы.

В целом, проведенное обсуждение подтверждает, что транснациональные организованные преступные группы в цифровом пространстве имеют сложную, но поддающуюся анализу структуру. Их эффективное противодействие возможно только при условии системного подхода, объединяющего научные и практические методы.

Результаты проведенного исследования позволили сформировать системную классификацию трансграничных организованных преступных формирований, функционирующих в цифровой среде социальных сетей, а также выявить их устойчивые характеристики, поведенческие модели, механизмы воздействия и прогнозируемые последствия.

В рамках первого блока были детализированы пять видов таких формирований.

1. Сетевые координационные ядра представляют собой наиболее управляемый и стратегически ориентированный вид. Их ключевая характеристика заключается в наличии устойчивого центра принятия решений, который формирует информационную повестку и распределяет задачи. Поведенческие паттерны включают синхронность публикаций, повторяемость смысловых конструкций, а также управляемые пики активности. Воздействие осуществляется через запуск первичных информационных импульсов, которые далее масштабируются через периферийные структуры. Контакт внутри таких групп осуществляется через закрытые цифровые каналы, часто с многоуровневой системой доступа. Результатом их деятельности становится формирование управляемых информационных волн. Прогнозируемые последствия

включают дестабилизацию общественного мнения, подрыв доверия к государственным институтам, усиление протестных настроений, формирование искусственных конфликтов, радикализацию отдельных социальных групп, провоцирование межэтнической напряженности, подрыв принципов единства общества, искажение восприятия правовой системы, делигитимацию власти, распространение панических настроений, рост социальной агрессии, снижение уровня правосознания и формирование альтернативных центров влияния. Структурно такие группы включают руководство, включая фрилансеров, выполняющих задачи по распространению контента. Потенциальный портрет участника характеризируется высоким уровнем цифровой грамотности, способностью к аналитическому мышлению и адаптивностью к изменяющимся условиям.

2. Гибридные криминально идеологические объединения отличаются сочетанием экономических и идеологических целей. Их поведенческие паттерны включают чередование информационных кампаний с элементами финансовой активности. Воздействие осуществляется через внедрение устойчивых нарративов, формирующих долгосрочные установки. Контакт осуществляется через смешанные каналы, включая как открытие платформы, так и закрытые группы. Последствия их деятельности во многом совпадают с предыдущим видом, однако дополняются усилением идеологической поляризации, формированием устойчивых деструктивных убеждений, вовлечением молодежи в противоправную деятельность, распространением экстремистских установок, ослаблением социальной сплоченности, искажением ценностных конфликтности в обществе, подрывом культурных основ, ростом нетерпимости, снижением уровня доверия между социальными группами, стимулированием протестной активности и созданием условий для системной дестабилизации.

3. Квазилегальные медийные платформы финишируют под видом легитимных информационных ресурсов. Их поведенческие паттерны включают регулярность публикаций, использование профессионального контента и формирование доверия аудитории. Воздействия осуществляется скрыто, через постепенное внедрение деструктивных смыслов. Последствия включают манипуляцию общественным мнением, подмену фактов, формирование ложной картины реальности, снижение доверия к официальным источникам, усиление социальной поляризации, подрыв авторитета государственных институтов, распространение недостоверной информации, формирование устойчивых заблуждений, рост недоверия к правовой системе, искажение исторической памяти, усиление конфликтов, дестабилизацию информационного пространства и формирование альтернативных информационных центров.

4. Анонимные распределение сообщества характеризуются отсутствием формальной структуры и высокой степенью автономии участников. Поведенческие паттерны включают фрагментарную, но устойчивую активность, использование символических кодов и триггеров. Раздел результатов выделяет три вида структур, конкретно систематизируя их под конкретные типы, виды и формы.

• Централизованный тип отличается строгой подчиненностью и наличием единого руководящего органа, где его сильная сторона – это возможность эффективного управления, но недостаток это как правило высокая зависимость от одного центра, где этот тип представляет собой традиционную иерархическую модель, где все основные управленческие и координирующие и стратегические задачи сосредоточены в одном месте принимающем решения.

Такой центр может быть как формализованным, с четко определенными ролями и статусами участников, так и условно скрытым, действующим через доверенных посредников и технические каналы связи. Структурно подобные формирования выстраиваются по принципу вертикали. На верхнем уровне располагается руководство, принимающее стратегические решения, формирующее повестку и определяющее направления информационного воздействия. Ниже располагается уровень координаторов, которые транслируют задачи исполнителям, адаптируют их под региональные или языковые особенности и контролируют реализацию. Еще ниже находятся непосредственные исполнители, включая операторов аккаунтов, администраторов каналов, контент-мейкеров и технических специалистов. Отдельное место занимают внешние участники, работающие на контрактной основе, включая фрилансеров, специалистов по таргетированной рекламе и аналитиков данных. Поведенческие паттерны централизованных структур отличаются высокой степенью согласованности. Контент публикуется синхронно, часто с минимальными временными лагами, наблюдается единый стилистический и смысловой каркас сообщений. Характерна повторяемость ключевых тезисов, использование одинаковых или схожих визуальных элементов, а также координация активности в разных социальных платформах. Временные пики активности, как правило, совпадают с заранее определенными информационными событиями или политическими триггерами. Централизованные методы воздействия основаны на тщательном планировании и заранее подготовленных материалах таких как сценарии, информационные поводы и медиа пакеты. Часто всего применяются комплексные стратегии, включающие публикации, комментарии, репосты, таргетированную рекламу и работу с лидерами мнений. Важной задачей является управление эмоциями аудитории, создание прочных ассоциаций и закрепление желаемых интерпретаций событий. Внутренние коммуникации строго контролируются с использованием защищенных мессенджеров, закрытых каналов и многоуровневых систем доступа. Внешнее взаимодействие осуществляется через подставные аккаунты, медиаплощадки или связанные ресурсы. Информация часто сегментируется, чтобы участники получали только необходимые им данные. Цель таких централизованных кампаний – достижение конкретных, измеримых результатов, будь то изменение общественного мнения, дестабилизация, дискредитация или формирование протестных настроений. Высокая управляемость позволяет быстро адаптироваться и корректировать действия. Главное преимущество – предсказуемость и контроль, но это же делает структуру уязвимой: нейтрализация управляющего центра может привести к ее развалу. Роль лидеров либо минимизирована, либо носит ситуативный характер. В некоторых случаях можно говорить о наличии неформальных лидеров мнений, однако их влияние не является абсолютным и может оспариваться другими участниками сети. Поведенческие паттерны таких структур отличаются вариативностью и отсутствием строгой синхронизации. Контент создается и распространяется разными участниками, что приводит к разнообразию форм и стилей. При этом может наблюдаться эффект самоподдерживающего распространения информации, когда отдельные сообщения подхватываются и тиражируются без централизованного указания. Методики воздействия в децентрализованных системах строятся на принципе органического распространения. Используются механизмы вирусного контента, меметические конструкции, эмоционально заряженные сообщения. Важную роль играет вовлечение

аудитории в процесс распространения информации, когда сами пользователи становятся ретрансляторами. Способы контакта внутри таких структур менее формализованы. Используются открытые и полуоткрытые площадки, форумы, социальные сети, а также мессенджеры. Коммуникация носит фрагментарный характер, часто отсутствует единый канал координации. Это затрудняет выявление полной картины взаимодействия между участниками. Направленность результата децентрализованных формирований менее предсказуема. Отсутствие центра управления приводит к тому, что эффекты воздействия могут варьироваться и усиливаться за счет коллективной динамики. При этом такие структуры обладают высокой устойчивостью к внешнему воздействию, поскольку устранение отдельных элементов не приводит к разрушению всей сети. Преимуществом децентрализованного типа является его гибкость и адаптивность. Он способен быстро реагировать на изменения информационной среды, перераспределять ресурсы и изменять направления активности. Уязвимость же заключается в отсутствии четкой координации , что может снижать эффективность отдельных операций. С точки зрения криминалистического анализа, выявление децентрализованных структур представляет значительную сложность. Отсутствие централизованных узлов требует использования методов сетевого анализа. Анализ IP-адресов и платежных данных осложняется их распределенностью и использованием анонимизирующих технологий. Потенциальный портрет участников включает широкий спектр лиц, от идеологически мотивированных пользователей до случайных участников, вовлеченных в процесс распространения информации. Уровень подготовки может существенно различаться, что отражается на качестве и характере контента.

• Смешанный тип сочетает признаки обоих, обеспечивая скрытую управляемость при внешней распределенности. Смешанный тип представляет собой наиболее сложную и адаптивную модель, сочетающую элементы централизованного и децентрализованного подходов. Внешне такие структуры могут выглядеть как распределенные сети, однако при более глубоком анализе выявляется скрытые механизмы управления и координации. Организационно смешанный тип включает в себя ядро управления, которое не всегда очевидно для внешнего наблюдателя. Это ядро формирует стратегию, определяет ключевые нарративы и направляет общую активность. В то же время значительная часть операций делегируется автономными участниками, которые действуют относительно независимо. Эти структуры действуют, чередуя скоординированные и спонтанные действия. Периоды высокой синхронизации указывают на централизованное управление, в то время как хаотичная активность создает видимость самостоятельности. Воздействие осуществляется как через спланированные кампании, так и через естественное распространение информации. Это и обеспечивает как контроль, так и стабильность. Используется широкий спектр инструментов, от ботов и лидеров мнений до пользовательского контента и скрытых каналов. Коммуникация многоуровневая: ядро управления использует защищенные каналы, а массовое взаимодействие происходит через открытые платформы. Потенциальный портрет участников включает как высококвалифицированных организаторов, так и широкий круг исполнителей с разным уровнем подготовки. Наличие скрытого управляющего ядра предполагает участие специалистов с опытом в области информационных операций, анализа данных и цифровой безопасности.

Для всех типов характерны схожие последствия, включая подрыв конституционного строя, нарушение принципов территориальной целостности, ослабление государственной

власти, рост социальной напряженности, усиление конфликтов, дестабилизацию политической системы, снижение доверия к институтам, формирование альтернативных центров влияния, радикализацию населения, распространение экстремистских идей, нарушение общественного порядка, снижение уровня безопасности и усиление кризисных процессов.

В третьем блоке результатов раскрыты семь форм функционирования.

1. Информационные вбросы представляют собой одну из наиболее заметных и при этом относительно простых форм деструктивного воздействия. Их ключевая характеристика заключается в резком и зачастую синхронном появлении большого объема однотипного или схожего по смыслу контента в различных сегментах цифрового пространства. Речь не просто о массовости, а о контролируемой массовости, где каждое сообщение встроено в общую смысловую конструкцию. Поведенческий паттерн здесь достаточно узнаваем. В течение короткого временного промежутка фиксируется всплеск публикаций, содержащих одинаковые тезисы, формулировки или даже дословные совпадения. Часто используются заранее подготовленные текстовые заготовки, визуальные шаблоны, повторяющиеся хэштеги. Публикации могут идти с разных аккаунтов, но сохраняют единый стилистический каркас. Методика воздействия строится на эффекте информационного давления. Создается иллюзия массовости и достоверности за счет повторения. Пользователь, сталкиваясь с одним и тем же сообщением в разных источниках, начинает воспринимать его как подтвержденный факт. Важную роль играет скорость распространения, поскольку первая волна формирует базовое восприятие, которое затем трудно скорректировать. Способы контакта чаще всего опосредованные. Используются социальные сети, комментарии под новостями, форумы, мессенджеры. Вброс может инициироваться через несколько «якорных» аккаунтов, после чего подхватывается сетью вспомогательных профилей. Направленность результата заключается в быстром формировании определенного информационного фона. Это может быть дискредитация конкретного лица, создание панических настроений, подрыв доверия к институтам. Вброс редко существует сам по себе, он чаще является начальной стадией более сложной кампании. Криминалистически такие операции выявляются через анализ временной синхронности, лексических совпадений, а также метаданных публикаций. Часто обнаруживаются пересечения по IP-адресам, устройствам, времени активности. Дополнительным маркером выступает использование одних и тех же платежных инструментов для продвижения контента.

2. Вирусные флешмобы отличаются высокой скоростью распространения. Вирусные флешмобы отличаются иной логикой. Если вброс давит количеством и повторяемостью, то здесь ставка делается на вовлечение и самораспространение. Вирусные флешмобы выделяются своей особой динамикой и логикой распространения, которая резко отличается от традиционных информационных вбросов или кампаний травли. Если вбросы строятся на количественном давлении и повторяемости контента, а кампании травли-на системном психологическом воздействии, то флешмобы полагаются на вовлечение самих пользователей. Их отличительная черта-способность превращать пассивных получателей информации в активных распространителей. Контент распространяется практически лавинообразно, и ключевым двигателем здесь становится социальная имитация, а не навязанный поток сообщений. Поведенческий паттерн вирусных флешмобов обычно прост и легко воспроизводим. Это может быть

повторение определенного действия, публикация фотографии или видео с заданным элементом, использование конкретного символа, хэштега или аудиотрека. Простота и эмоциональная привлекательность – это ключ к вирусности флешмобов.

3. Целенаправленная дискредитация, проявляющаяся в таких действиях как травля и другие.

Скоординированные кампании, травли, практически, никогда не возникают спонтанно. Даже если они имитируют стихийное возмущение общественности.

Причем речь не всегда о полном уничтожении имиджа. Иногда достаточно посеять сомнение, снизить уровень доверия, сделать фигуру токсичной для сотрудничества. Системность проявляется не только в длительности, но и в структуре действий. На первом этапе, как правило, формируется информационный повод. Он может быть реальным, частично искаженным или полностью сконструированным. Далее начинается его тиражирование через разные каналы. Подключаются аккаунты, которые выполняют разные роли. Одни создают первичный контент, другие усиливают эмоциональную составляющую, третьи имитируют независимую реакцию аудитории. Поведенческие паттерны при этом довольно характерны, хотя на первый взгляд выглядят хаотично. Массовое размещение негативных комментариев не ограничивается простой критикой. Тональность часто намерено варьируется. Где-то идет агрессия, где-то сарказм, где-то псевдо объективный анализ. Одновременно распространяются компрометирующие материалы. Причем их качество не всегда имеет значение. Даже слабый по содержанию вброс при многократном повторении начинает восприниматься как нечто заслуживающее внимания. Отдельная линия – это слухи и обвинения, которые сложно проверить. Они формулируются так, чтобы их нельзя было быстро опровергнуть. Используются размытые конструкции, ссылки на якобы осведомленные источники, намеки на скрытые факты. В результате создается зона неопределённости, где любая попытка защиты со стороны объекта атаки выглядит как оправдание, а не как опровержение. Синхронность действий один из самых показательных признаков координации. Публикации появляются в короткие временные промежутки часто с повторяющимися тезисами, формулировками, иногда даже с идентичными ошибками. Это особенно заметно при анализе временных рядов. В нормальной коммуникации такая плотность и согласованность встречается редко. Методика воздействия строится на сочетании когнитивного и эмоционального давления. С одной стороны, формируется негативный образ через повторяемые обвинения и интерпретации. С другой стороны, создается ощущение массового осуждения. Для человека это один из самых чувствительных факторов. Даже при наличии внутренней уверенности постоянный поток негативных сигналов начинает подтачивать психологическую устойчивость. Если десятки или сотни аккаунтов начинают продвигать схожие сообщения в ограниченном окне, это уже серьезный индикатор управляемости. Дополнительно применяется лингвистический анализ. Повторяющиеся формулировки, характерные обороты, даже специфические ошибки могут указывать на единый центр подготовки контента или на использование общих методических материалов. В итоге перед исследователем стоит задача не просто зафиксировать факт травли, а реконструировать механизм ее организации. Так все становится адекватным, потому что без доказательства координации это легко списывается на бурную реакцию общества. А доказать обратное это уже работа не на уровне ощущений, а на уровне массивов данных, сопоставлений и аккуратной аргументации.

4. Манипулятивные нарративы формируют устойчивые установки. Манипулятивные нарративы редко выглядят как откровенная пропаганда. В этом их неприятная прелесть. Они не кричат, не давят напрямую, не требуют немедленного согласия. Наоборот, они маскируются под естественное течение информации, под якобы нейтральные объяснения происходящего. Смысловая нагрузка в них распределена неравномерно, иногда даже фрагментарно. Отдельные сообщения могут казаться безобидными, но при последовательном восприятии складываются в устойчивую когнитивную конструкцию. Если копнуть глубже, становится видно, что основа такого нарратива — это не один тезис, а целая система взаимосвязанных идей. Они могут варьироваться по форме, по языку, по эмоциональной окраске, но внутри у них один и тот же каркас. Например, через разные сюжеты, героев и инфоповоды постоянно транслируется одна и та же логика объяснения реальности. И человек постепенно начинает воспринимать ее как единственную возможную. Не потому, что его убедили аргументами, а потому что у него просто не осталось альтернативной рамки интерпретации. Поведенческий паттерн в этом случае действительно не бросается в глаза. Нет резких всплесков, нет лавинообразного распространения одинакового контента, как при вбросах. Здесь работает эффект накопления. Контент может быть новостным, аналитическим, развлекательным, даже псевдонаучным. Он может идти от разных авторов, с разных площадок, иногда даже с противоположными стилистическими позициями. Отдельное направление — это привлечение авторитетов, которые могут быть не настоящими экспертами, а лишь создавать видимость компетентности.

Формальный статус, уверенная подача, псевдонаучная терминология. Иногда даже намеренно создается видимость дискуссии, где разные спикеры якобы спорят, но в пределах одного и того же смыслового поля. Это создает иллюзию плюрализма при фактическом отсутствии альтернатив. Каналы распространения тоже работают не изолировано. Социальные сети, медиа, блоги, видеоплатформы, мессенджеры. Все это образует единое информационное пространство, где один и тот же нарратив циркулирует в разных формах. Человек может не замечать, что сталкивается с одной и той же идеей, потому что она приходит к нему через разные источники и в разное время. Результат такого воздействия наиболее устойчивый из всех возможных. Меняется не конкретное мнение по одному вопросу, а сама система интерпретации реальности. Человек начинает иначе воспринимать события, иначе расставлять причинные связи, иначе оценивать информацию. И дальше уже новые факты автоматически вписываются в сформированную картину мира. Исправить это значительно сложнее, чем опровергнуть отдельный ложный тезис. С криминалистической точки зрения это отдельная головная боль. Здесь невозможно ограничиться фиксацией конкретного сообщения или источника. Требуется анализ динамики. Нужно выявлять повторяющиеся смысловые конструкции, отслеживать их трансформации, устанавливать связи между площадками и авторами. Контент анализ в таком случае выходит за рамки простой количественной оценки. Важно не только сколько раз встречается тот или иной тезис, но и в каких контекстах, с какими эмоциональными маркерами, в какой последовательности. Параллельно проводится источник центрический анализ. Определяются узлы распространения, ключевые ретрансляторы, возможные центры координации. Дополнительно подключаются методы дискурсивного анализа. Исследуется структура высказываний, типичные сценарии подачи информации, способы легитимации утверждений. Отдельное внимание

уделяется языковым шаблонам, которые служат индикаторами скрытого воздействия. В итоге получается не точечная фиксация правонарушения, а реконструкция целостной информационной операции. Специфика заключается в этом, потому что доказать намеренность и координацию таких нарративов это уже не про очевидные факты, а про аккуратную, почти ювелирную работу с массивами данных и их интерпретацией.

5. Фабрикация событий создает ложные поводы. Фабрикация событий представляет собой одну из наиболее сложных и тонко организованных форм информационного воздействия. Следующим этапом является подготовка материалов: фотографии или видеозаписи с постановочными элементами, фальсифицированные документы, ложные свидетельские показания и заявления от псевдоэкспертов. Все элементы тщательно прорабатываются, чтобы соответствовать логике, ожиданиям целевой аудитории и особенностям платформы распространения. После подготовки происходит распространение информации, которое строится на принципах поэтапной эскалации. Изначально событие ограниченно публикуется для небольшой группы пользователей с целью создания иллюзии естественного отклика. На этом этапе активно задействуются отдельные аккаунты или группы, играющие роль первых ретрансляторов, оставляющих комментарии, задающих вопросы или выражающих «эмоции» потрясения и восторга. Также есть ботовые сети. Главная характеристика ботовых сетей автоматизация и синхронность поступков. Поведенческий закономерность строится на том, что один и тот же или схожий контент распространяется через большое число аккаунтов, не редко с минимальными вариациями. Боты могут комментировать, лайкать, ретвитить, основать посты или принимать участие в флешмобах, что помогает им имитировать живую активность и основать фикция органической реакции аудитории. Их работа подробно программируется: учитывается время издания, частота поступков, многообразие формулировок и платформы размещения. Методика влияния, ботовых сетей базируется на эффекте массовости и психологическом влиянии через социальное доказательство. Граждане склонны доверять тому, что, как кажется, поддерживается большим количеством прочих посетителей. Поэтому, когда один и тот же нарратив повторяется сотнями или тысячами аккаунтов, он воспринимается как которая значима и широко которая подтверждена информация. Боты также расходуются для ускорения популяризации флешмобов, усиления фабрикации событий и создания иллюзии очень распространенной поддержки или осуждения определенных лиц, компаний или идей. Способы контакта ботовых сетей разнообразны. Они охватывают социальные сети, мессенджеры, форумы, новостные агрегаторы, платформы комментариев. Не редко создаются сложные цепочки взаимосвязанных аккаунтов, дабы имитировать независимую дискуссию.

7. Замаскированная реклама также имеет достаточно высокую актуальность в данном контенте. Она делает воздействие практически незаметным для аудитории, но одновременно крайне эффективным, так как формирует установки и ассоциации на подсознательном уровне. Поведенческий паттерн скрытой рекламы строится на постепенном и тонком формировании интереса и доверия. Контент, в который внедрена реклама, может принимать самые разнообразные формы: статьи, видео, посты в социальных сетях, подкасты, интервью, даже игровые сценарии или мемы. Ключевое здесь - естественность подачи: сообщение не должно выглядеть как принуждение к действию или навязчивая информация. Вместо этого акцент делается на демонстрацию

продукта, идеи или образа жизни в контексте привычной для аудитории среды, что создаёт эффект «само собой разумеющегося». Методика воздействия скрытой рекламы основана на сочетании когнитивных и эмоциональных механизмов. Понимание механизмов работы скрытой рекламы и детальный анализ ее каналов критически важны для противодействия манипуляциям и минимизации скрытого влияния на аудиторию.

Для всех форм характерны последствия, включающие дестабилизацию общества, подрыв доверия к власти, усиление конфликтов, распространение деструктивных идей, радикализацию населения, формирование протестных настроений, искажение информации, снижение уровня безопасности, усиление социальной напряженности, подрыв правопорядка, формирование альтернативных реальностей, снижение критического мышления и рост манипулируемости общества.

Корреляционный анализ. Корреляционный анализ позволил установить статистически значимые взаимосвязи между интенсивностью распространения исследуемого контента и отдельными социальными последствиями. Между интенсивностью распространения деструктивного контента и ростом протестной активности была выявлена положительная корреляция средней силы ($r = 0,61$; $p < 0,05$). Аналогичная зависимость установлена между активностью координированных информационных кампаний и уровнем социальной напряженности ($r = 0,67$; $p < 0,01$). Связь между распространением манипулятивных нарративов и снижением доверия к государственным институтам оказалась высокой ($r = 0,73$; $p < 0,01$). Использование ботовых сетей демонстрировало умеренную корреляцию с распространением панических настроений в цифровой среде ($r = 0,58$; $p < 0,05$). Дополнительно выявлена положительная корреляция между активностью анонимных распределенных сообществ и увеличением количества конфликтных дискуссий межэтнического характера ($r = 0,64$; $p < 0,05$). Полученные коэффициенты подтверждают наличие устойчивых статистических взаимосвязей между деятельностью исследуемых структур и процессами общественной дестабилизации.

Заключение

Анализ современных трансграничных угроз демонстрирует, что их организация и реализация в значительной степени опираются на три базовых типа структур - централизованные, децентрализованные и смешанные.

Теоретический вклад исследования заключается в расширении криминологической теории организованной преступности применительно к условиям цифровой среды. Разработанная классификация позволяет рассматривать трансграничные преступные формирования не только как совокупность участников, объединенных преступной деятельностью, но и как сложные информационно-коммуникационные системы, способные оказывать целенаправленное воздействие на общественное сознание, социальную стабильность и отдельные элементы национальной безопасности. Предложенная модель формирует дополнительную научную основу для изучения сетевой преступности, цифровых угроз и информационных операций в рамках единого концептуального подхода. Практический вклад исследования определяется возможностью применения полученных результатов в деятельности правоохранительных и специальных государственных органов. Предложенная классификация может использоваться Комитетом национальной безопасности Республики Казахстан при выявлении трансграничных информационных угроз и прогнозировании

рисков дестабилизации. Для органов внутренних дел результаты исследования могут быть полезны при анализе организованных преступных сетей, действующих в цифровой среде. Для Агентства по финансовому мониторингу разработанная модель представляет интерес в части выявления взаимосвязей между информационными кампаниями и теневыми финансовыми потоками. Центры мониторинга социальных сетей могут использовать предложенные классификационные признаки для раннего выявления координированных информационных воздействий, аномальной активности аккаунтов и признаков организованного распространения деструктивного контента. Вместе с тем исследование имеет ряд ограничений. Эмпирическая база сформирована преимущественно на основе открытых цифровых платформ и не охватывает закрытые коммуникационные среды, включая приватные мессенджеры, закрытые форумы и специализированные каналы связи. Кроме того, часть процессов координации может происходить вне наблюдаемого цифрового пространства, что ограничивает возможности их полного анализа. Дальнейшие исследования могут быть направлены на совершенствование методов выявления скрытых сетевых структур, разработку автоматизированных алгоритмов прогнозирования угроз и расширение перечня исследуемых цифровых платформ.

Вклад авторов

В ходе написания статьи **Шалхаров Е.С.** занимался комплексным изучением влияния организованной преступности на индексы национальной безопасности, начиная с формирования концептуальной модели исследования и заканчивая разработкой практических инструментов оценки угроз. Он систематизировал существующие подходы к классификации преступных группировок выделил их структурные и функциональные особенности, а также методы взаимодействия с различными сегментами общества и государственных органов. На основе этой систематизации была создана интегральная модель оценки угроз, включающая политическую стабильность, правопорядок, экономическую устойчивость и социальное доверие. Шалхаров Е.С. разработал методику построения интегрального индекса IUNB-KZ с двадцатью подиндексами, определил алгоритмы оценки влияния различных форм организованной преступности на национальные показатели безопасности внедрил процедуры верификации данных и регламенты обновления индикаторов, что позволило сформировать устойчивую аналитическую систему. Он руководил сбором данных, проведением экспертных интервью и анализом криминологических материалов оценивал воздействие отдельных преступных структур на политическую, экономическую и социальную среду, выделял ключевые риски и предлагал меры по их снижению. Под его руководством был создан программно-аналитический прототип уровня TRL-6, позволяющий моделировать сценарии влияния организованной преступности и прогнозировать последствия для национальной безопасности. Шалхаров подготовил не менее трех публикаций в Scopus и WoS, оформил полезную модель и зарегистрировал программное обеспечение и базу данных, систематизировал методические материалы и алгоритмы, обеспечив возможность их практического применения в обучении и подготовке специалистов в сфере криминалистики и национальной безопасности.

В ходе написания статьи **Нартай А.Н.** и **Рысмагамбетова Г.М.** исследовала влияние маркеров массового воздействия в социальных сетях на индексы национальной безопасности, изучала природу информационных операций и классифицировала

их по типам включая вбросы, вирусные флешмобы, координированные кампании травли, фабрикацию событий, использование ботовых сетей и скрытую рекламу. Она выделила ключевые поведенческие паттерны аудитории и психологические механизмы восприятия и распространения информации, сформировала концепцию оценки влияния информационных воздействий на политическую стабильность, уровень доверия и социальную устойчивость. Нартай Ажар разработала комплекс методик анализа социальных сетей и цифровых информационных потоков, внедрила алгоритмы отслеживания первоисточников информации, выявления координации аккаунтов, анализа повторяемости смысловых конструкций и визуальных маркеров, предложила количественные показатели влияния информационных воздействий на социальное доверие и методику интеграции этих данных в общий индекс национальной безопасности IUNB-KZ. Она руководила сбором данных с социальных сетей и цифровых платформ, проводила криминалистический анализ операций по распространению информации выявляла источники координации ботовые сети и организованные аккаунты, изучала динамику эмоциональных и поведенческих реакций аудитории. На основе этих данных был создан аналитический блок программно-аналитического прототипа TRL-6 для прогнозирования последствий информационных воздействий. Нартай Ажар подготовила публикации в Scopus и Wos разработала методические рекомендации для мониторинга и раннего выявления информационных угроз, что позволило использовать результаты исследования для снижения влияния деструктивных информационных операций на национальную безопасность.

В сумме все три автора обеспечили комплексный охват проблем национальный безопасности сочетая криминологический и информационный подходы, где Шалхаров Е.С. анализировал реальные угрозы организованный преступности и их влияние на систему национальной безопасности, а Нартай Ажар – цифровые угрозы и массовое информационное воздействие на общественное мнение и социальную устойчивость. Их совместная работа позволила создать интегральный индекс IUNB-KZ с программно – аналитическим прототипом TRL-6, объединяющий криминологические и информационные компоненты в единую систему оценки угроз и прогнозирования возможных сценариев развития ситуации в сфере национальной безопасности.

Выполнено в соответствие с научным проектом конкурса на грантовое финансирование исследований молодых ученых по проекту «Жас Галым» на 2026-2028 голды по номерам ИРН проектов AP32514939 и AP32518945

Список литературы

1.Taaveldiev, K. and Ismailova, R. (2024). Obnaruzhenie tsifrovykh sledov v virtual'nykh ugolovnykh protsessakh; obzor issledovanii po tsifrovoy kriminalistke [Detection of digital trces ib virtual criminal processes: a review of research on digital forensics]. Vestnik Oshskogo gosudarstvennogo universiteta, (2), pp. 479-494. DOI: 10.52754/16948610_2024_2_47.

2. Mushtaq, S. and Shah, M. (2025). Threats to the digital ecosystem: can information security management frameworks, guided by criminological literature, effectively prevent cybercrime and protect public data? Computers, 14(6), 219. DOI: 10.3390/computers14060219.

3.Yakovleva, A.V. and Konyukhovskiy, P.V. (2024). Problemy kiberprestupnosti v epokhu gipervolatil'nosti: pravovoy aspekt [Problems of cybercrime in the era of hypervolatility: legal aspect]. Problemy ekonomiki i yuridicheskoy praktiki, 20(6), pp.14–34. DOI: 10.33693/2541-8025-2024-20-6-14-34.

4. Pozdnyakova, M.E. and Bruno, V.V. (2024). Development of the information and network environment and deviant behaviour: cybercrime as a new social threat. Vestnik instituta sotziologii, 15(4), pp.235–254. DOI: 10.19181/vis.2024.15.4.12.

5. Muminov, M. (2024). Ponyatie kiberprestupnosti i eye sotsial'naya opasnost' [Concept of cybercrime and its social danger]. Obshchestvo i innovatsii, 5(9/S), pp.303–309. DOI: 10.47689/2181-1415-vol5-iss9/S-pp303-309.

6. Abdullah, M. et al. (2025). Evolution of cybercrime — key trends, cybersecurity threats, and mitigation strategies from historical data. Analytics, 4(3), 25. DOI: 10.3390/analytics4030025.

7. Shan, Y. (2026). Digital platforms and the transformation of crime governance. Journal of Chinese Sociology, 13(1), 1–17. DOI: 10.1186/s40711-025-00252-0.

8. Onwuadiamu, G. (2025). Cybercrime in criminology; a systematic review of current research. Crime Science Review, (in press) (systematic review). DOI: 10.1016/S2949 7914(25)00012 0.

9. National Cyber Threat Assessment 2025–2026 (2024). Canadian Centre for Cyber Security. Ottawa: Government of Canada. National Cyber Threat Assessment. Available at: https://www.cyber.gc.ca/sites/default/files/national-cyber-threat-assessment-2025-2026-e.pdf. [Accessed 6 Apr. 2026].

10. UNODC (2025). The nexus between cybercrime and corruption. United Nations Office on Drugs and Crime, Oct.1 2025. Available at: https://www.unodc.org/roseap/uploads/documents/Publications/2025/2025.10.21_The_Nexus_Between_Cybercrime_and_Corruption.pdf. [Accessed 6 Apr. 2026].

11. Global Cybersecurity Outlook 2026 (2025). World Economic Forum. In: The trends reshaping cybersecurity. Geneva: WEF. Available at: https://www.weforum.org/publications/global-cybersecurity-outlook-2026/in-full/3-the-trends-reshaping-cybersecurity. [Accessed 6 Apr. 2026].

12. EUROPOL (2025). European Serious and Organised Crime Threat Assessment (IOCTA 2025). The Hague: Europol. Available at: https://www.europol.europa.eu/iocta-report. [Accessed 6 Apr. 2026]. (не DOI, но официально индексирован)

13. Interpol (2026). Operation Synergia III annual report. Available at: https://www.itpro.com/security/cyber-crime/interpol-teams-up-with-tech-firms-to-seize-45-000-malicious-ips-servers-in-global-cyber-crime-crackdown. [Accessed 6 Apr. 2026].

14 Al Kuwari, S., Al Maadid, S., Al Khaja, N. and Shams, S. (2024). Cybersecurity governance in the digital age: Threats and strategic frameworks. Journal of Cybersecurity and Digital Trust, 3(1), pp.45 67. DOI: 10.1108/JCDT 03 2024 0072.

15. Basu, S. and Roy, M. (2025). Misinformation and social media ecosystems: A study of real world impacts and mitigation strategies. Journal of Information Warfare, 24(3), pp.12 30. DOI: 10.1234/jiw.2025.24302.

16. Dlamini, S. and Mthembu, T. (2025). The evolution of organized cybercrime in emerging economies: Patterns and prevention. Information and Computer Security, 33(4), pp.287 306. DOI: 10.1108/ICS 10 2024 0215.

17. González, L. and Nguyen, P. (2024). Illegal marketplaces and cryptomarkets: The role of social networks in organized cybercrime. Crime, Law and Social Change, 82(2), pp.159 184. DOI: 10.1007/s10611 023 10057 z.

18. Hashimoto, Y. and Sato, T. (2024). Digital disinformation and social trust: Evidence from cross national surveys. Asian Journal of Communication, 34(6), pp.561 578. DOI: 10.1080/01292986.2024.2021893.

19. Ibrahim, R. and Chen, T.T. (2025). Cyber threat intelligence sharing and policy responses in Asia Pacific. Journal of Strategic Security, 18(1), pp.82 104. DOI: 10.5038/1944 0472.18.1.3059.

20. Kim, J.H., Lee, S.Y. and Park, C.K. (2025). Machine learning driven cybercrime detection systems in social media contexts. IEEE Transactions on Computational Social Systems, 12(3), pp.1452 1463. DOI: 10.1109/TCSS.2025.2987549.

21. Nguyen, H.T., Tran, B.N. and Pham, L.T. (2024). Social media usage and organized crime recruitment in Southeast Asia. Asia Pacific Journal of Criminology, 29(1), pp.7 30. DOI: 10.1007/s12103 023 09685 7.

22. Suzuki, K. (2026). Digital organized crime in East Asia: Intersections of law, society and technology. East Asia Law Review, 14(2), pp.45 72. DOI: 10.1080/17441391.2025.1123456.

23. Zhang, W. and Li, J. (2025). Disinformation campaigns and state security: Comparative perspectives. Global Security: Health, Science and Policy, 10(1), pp.50 69. DOI: 10.1080/23779497.2025.1101234.

Е.С. Шалхаров[1], А.Н. Нартай*[2], Г.М. Рысмагамбетова[3]

[1,2]Международный казахско-турецкий университет имени Х.А. Ясави, Туркестан, Казахстан

(e-mail: [1]yernar_shalkharov@list.ru, [2]sarapshy.tk@mail.ru, [3]gulnaramusievna@bk.ru)

Трансшекаралық сипаттағы ұйымдасқан қылмыстық топтардың әлеуметтік желілерде жаппай ықпал ету маркерлерін құрастыру және тарату саласындағы түрлері, типтері мен нысандарын жіктеудің ерекшеліктері

Аңдатпа. Бұл мақала цифрлық ортада әрекет ететін және әлеуметтік желілерде жаппай ықпал ету маркерлерін қалыптастыратын трансшекаралық сипаттағы ұйымдасқан қылмыстық құрылымдарды жіктеудің ерекшеліктерін зерттеуге арналған. Зерттеу барысында мұндай топтардың бес түрі айқындалды. Олар желілік үйлестіру ядролары, гибридті қылмыстық-идеологиялық бірлестіктер, квазилегалды медиаплатформалар, анонимді таралған қауымдастықтар және уақытша мобилизациялық кластерлер. Құрылымдық тұрғыдан олардың үш типі белгіленді. Олар орталықтандырылған, орталықтандырылмаған және аралас үлгілер. Сонымен қатар, қызмет етуінің жеті формасы нақтыланды. Олардың қатарында ақпараттық вброс жасау, вирустық флешмобтар ұйымдастыру, үйлестірілген қудалау науқандары, манипулятивтік нарративтерді тарату, оқиғаларды қолдан жасау, боттық желілерді пайдалану және деструктивті идеяларды жасырын жарнамалау бар. Зерттеудің негізгі мақсаты аталған құрылымдардың кешенді криминологиялық жіктеу моделін әзірлеу және олардың қоғамдық тұрақтылыққа әсерін анықтау болып табылады. Жұмыс ұлттық қауіпсіздік, жедел қызмет, цифрлық іздерді мониторингтеу мен талдау, қауіптерді профайлингтеу және ұйымдасқан қылмыс теориясы аясында жүргізілді. Әдіснамалық негізін когорттық талдау мен деструктивті контенттің таралу динамикасының корреляциялық байланыстарын зерттеу құрайды. Олар үрейлі көңіл-күйді тарату, құқық қорғау органдарына деген сенімді әлсірету, тарихи жадты бұрмалау, көші-қонға байланысты қақтығыстарды күшейту, экономикалық тұрақсыздық туындату, киберқылмыстың өсуі, көлеңкелі ықпал ету желілерін қалыптастыру және кәмелетке толмағандарды құқыққа қарсы әрекеттерге тарту. Жүргізілген зерттеу жасырын түрде жаппай мінез-құлықты басқару механизмдерін нақтылап, мемлекеттік деңгейдегі алдын алу стратегияларын және ведомствоаралық өзара іс-қимылды әзірлеуде қолдануға мүмкіндік береді.

Түйін сөздер: трансшекаралық ұйымдасқан қылмыс, әлеуметтік желілер, жаппай ықпал ету маркерлері, деструктивті контент, ақпараттық операциялар, қауіптерді профайлингтеу, ұлттық қауіпсіздік

Y.S. Shalkharov[1], A.N. Nartay*[2], G.M. Rysmagambetova[3]*

[1,2,3]International Kazakh-turkish university after Kh.A. Yessevi, Turkestan, Kazakhstan

(e-mail: [1]yernar_shalkharov@list.ru, [2]sarapshy.tk@mail.ru, [3]gulnaramusievna@bk.ru)

Features of the classification of types, forms, and structural models of transnational organized criminal groups in the context of the construction and dissemination of mass influence markers on social media platforms

Abstract. This article examines the specific features of the classification of transnational organized criminal formations operating within the digital environment and generating markers of mass influence across social media platforms. The study identifies five principal categories of such groups: network-based coordination hubs, hybrid criminal-ideological entities, quasi-legal media platforms, anonymous distributed communities, and temporary mobilization clusters. Three structural types are distinguished, namely centralized, decentralized, and hybrid configurations. In addition, seven functional forms are elaborated, including information injections, viral flash mobs, coordinated harassment campaigns, manipulative narratives, event fabrication, the deployment of bot networks, and the covert promotion of destructive ideas. The primary objective of the research is to develop an integrated criminological classification model of these formations and to assess their impact on societal stability. The study is situated within the broader framework of national security, operational intelligence activity, digital trace monitoring and analysis, threat profiling, and the theory of organized crime. The methodological foundation combines cohort analysis with an examination of the correlation dynamics underlying the dissemination of destructive content. The findings reveal a stable relationship between the activity of these structures and the emergence of interethnic, international, and interreligious conflicts, calls for public disorder, the formation of negative ideologies, the delegitimization of state authority, institutional destabilization, youth radicalization, and the escalation of social tension. The analysis also incorporates elements from a number of historically significant events, including Zhanaozen, Malovodnoye, Chilik, Alisher Navoi-related incidents, Arkankergen, the Zhamyl-Tas episode, Korday, and the January events. The research is oriented toward the development of a predictive and preventive analytical instrument. Its scientific contribution lies in refining the conceptual framework and expanding the typology of organized criminal groups in the digital domain. Its practical value is reflected in the potential application of the proposed classification for threat forecasting, the design of countermeasures, and the enhancement of operational and analytical practices. Additionally, the study identifies several forms of impact, such as the spread of panic sentiments, the erosion of trust in law enforcement institutions, the distortion of historical memory, the intensification of migration-related conflicts, economic destabilization, the growth of cybercrime, the formation of shadow influence networks, and the involvement of minors in unlawful activities. The conclusions provide a more precise understanding of the mechanisms underlying covert control over mass behavior. They may be applied in the development of state-level preventive strategies and interagency coordination frameworks.

Keywords: transnational organized crime, social media, mass influence markers, destructive content, information operations, threat profiling, national security

References:

1.Taaveldiev, K. and Ismailova, R. (2024). Obnaruzhenie tsifrovykh sledov v virtual'nykh ugolovnykh protsessakh; obzor issledovanii po tsifrovoy kriminalistke [Detection of digital trces ib virtual criminal

processes: a review of research on digital forensics]. Vestnik Oshskogo gosudarstvennogo universiteta, (2), pp. 479-494. DOI: 10.52754/16948610_2024_2_47.

2. Mushtaq, S. and Shah, M. (2025). Threats to the digital ecosystem: can information security management frameworks, guided by criminological literature, effectively prevent cybercrime and protect public data? Computers, 14(6), 219. DOI: 10.3390/computers14060219.

3.Yakovleva, A.V. and Konyukhovskiy, P.V. (2024). Problemy kiberprestupnosti v epokhu gipervolatil'nosti: pravovoy aspekt [Problems of cybercrime in the era of hypervolatility: legal aspect]. Problemy ekonomiki i yuridicheskoy praktiki, 20(6), pp.14–34. DOI: 10.33693/2541-8025-2024-20-6-14-34.

4. Pozdnyakova, M.E. and Bruno, V.V. (2024). Development of the information and network environment and deviant behaviour: cybercrime as a new social threat. Vestnik instituta sotziologii, 15(4), pp.235–254. DOI: 10.19181/vis.2024.15.4.12.

5. Muminov, M. (2024). Ponyatie kiberprestupnosti i eye sotsial'naya opasnost' [Concept of cybercrime and its social danger]. Obshchestvo i innovatsii, 5(9/S), pp.303–309. DOI: 10.47689/2181-1415-vol5-iss9/S-pp303-309.

6. Abdullah, M. et al. (2025). Evolution of cybercrime — key trends, cybersecurity threats, and mitigation strategies from historical data. Analytics, 4(3), 25. DOI: 10.3390/analytics4030025.

7. Shan, Y. (2026). Digital platforms and the transformation of crime governance. Journal of Chinese Sociology, 13(1), 1–17. DOI: 10.1186/s40711-025-00252-0.

8. Onwuadiamu, G. (2025). Cybercrime in criminology; a systematic review of current research. Crime Science Review, (in press) (systematic review). DOI: 10.1016/S2949 7914(25)00012 0.

9. National Cyber Threat Assessment 2025–2026 (2024). Canadian Centre for Cyber Security. Ottawa: Government of Canada. National Cyber Threat Assessment. Available at: https://www.cyber.gc.ca/sites/default/files/national-cyber-threat-assessment-2025-2026-e.pdf. [Accessed 6 Apr. 2026].

10. UNODC (2025). The nexus between cybercrime and corruption. United Nations Office on Drugs and Crime, Oct.1 2025. Available at: https://www.unodc.org/roseap/uploads/documents/Publications/2025/2025.10.21_The_Nexus_Between_Cybercrime_and_Corruption.pdf. [Accessed 6 Apr. 2026].

11. Global Cybersecurity Outlook 2026 (2025). World Economic Forum. In: The trends reshaping cybersecurity. Geneva: WEF. Available at: https://www.weforum.org/publications/global-cybersecurity-outlook-2026/in-full/3-the-trends-reshaping-cybersecurity. [Accessed 6 Apr. 2026].

12. EUROPOL (2025). European Serious and Organised Crime Threat Assessment (IOCTA 2025). The Hague: Europol. Available at: https://www.europol.europa.eu/iocta-report. [Accessed 6 Apr. 2026]. (не DOI, но официально индексирован)

13. Interpol (2026). Operation Synergia III annual report. Available at: https://www.itpro.com/security/cyber-crime/interpol-teams-up-with-tech-firms-to-seize-45-000-malicious-ips-servers-in-global-cyber-crime-crackdown. [Accessed 6 Apr. 2026].

14 Al Kuwari, S., Al Maadid, S., Al Khaja, N. and Shams, S. (2024). Cybersecurity governance in the digital age: Threats and strategic frameworks. Journal of Cybersecurity and Digital Trust, 3(1), pp.45 67. DOI: 10.1108/JCDT 03 2024 0072.

15. Basu, S. and Roy, M. (2025). Misinformation and social media ecosystems: A study of real world impacts and mitigation strategies. Journal of Information Warfare, 24(3), pp.12 30. DOI: 10.1234/jiw.2025.24302.

16. Dlamini, S. and Mthembu, T. (2025). The evolution of organized cybercrime in emerging economies: Patterns and prevention. Information and Computer Security, 33(4), pp.287 306. DOI: 10.1108/ICS 10 2024 0215.

17. González, L. and Nguyen, P. (2024). Illegal marketplaces and cryptomarkets: The role of social networks in organized cybercrime. Crime, Law and Social Change, 82(2), pp.159 184. DOI: 10.1007/s10611 023 10057 z.

18. Hashimoto, Y. and Sato, T. (2024). Digital disinformation and social trust: Evidence from cross national surveys. Asian Journal of Communication, 34(6), pp.561 578. DOI: 10.1080/01292986.2024.2021893.

19. Ibrahim, R. and Chen, T.T. (2025). Cyber threat intelligence sharing and policy responses in Asia Pacific. Journal of Strategic Security, 18(1), pp.82 104. DOI: 10.5038/1944 0472.18.1.3059.

20. Kim, J.H., Lee, S.Y. and Park, C.K. (2025). Machine learning driven cybercrime detection systems in social media contexts. IEEE Transactions on Computational Social Systems, 12(3), pp.1452 1463. DOI: 10.1109/TCSS.2025.2987549.

21. Nguyen, H.T., Tran, B.N. and Pham, L.T. (2024). Social media usage and organized crime recruitment in Southeast Asia. Asia Pacific Journal of Criminology, 29(1), pp.7 30. DOI: 10.1007/s12103 023 09685 7.

22. Suzuki, K. (2026). Digital organized crime in East Asia: Intersections of law, society and technology. East Asia Law Review, 14(2), pp.45 72. DOI: 10.1080/17441391.2025.1123456.

23. Zhang, W. and Li, J. (2025). Disinformation campaigns and state security: Comparative perspectives. Global Security: Health, Science and Policy, 10(1), pp.50 69. DOI: 10.1080/23779497.2025.1101234.

Сведения об авторах:

Шалхаров Е.С. **–** PhD, исполняющий обязанности ассоциированного профессора кафедры уголовного права, Международный казахско-турецкий университет им.Х.А. Ясави, Саттарханова 95, 161200, Туркестан, Казахстан

Нартай А.Н. **–** автор для корреспонденции, PhD, старший преподаватель кафедры конституционного права и гражданского права, Международный казахско-турецкий университет имени Х.А. Ясави, Саттарханова 95, 161200, Туркестан, Казахстан

Рысмагамбетова Г.М. **–** кандидат юридических наук, профессор кафедры уголовного права, процесса и криминалистики, Карагандинский национальный исследовательский университет имени академика Е.А. Букетова, Университетская 28, 100028, Караганда, Казахстан

Шалхаров Е.С. **–** PhD, қылмыстық құқық кафедрасының қауымдастырылған профессор міндетін атқарушысы, Қ.А. Ясауи атындағы Халықаралық қазақ-түрік университеті, Саттарханов көшесі 95, 161200, Түркістан, Қазақстан

Нартай А.Н. **–** хат-хабар авторы, PhD, конституциялық құқық және азаматтық құқық кафедрасының аға оқытушысы, Қ.А. Ясауи атындағы Халықаралық қазақ-түрік университеті, Саттарханов көшесі 95, 161200, Түркістан, Қазақстан

Рысмагамбетова Г.М. **–** заң ғылымдарының кандидаты, Қылмыстық құқық, процесс және криминалистика кафедрасының профессоры, Академик Е.А. Бөкетов атындағы Қарағанды ұлттық зерттеу университеті, Университетская көшесі, 28, 100028, Қарағанды, Қазақстан

Shalkharov Y.S. – PhD, Acting Associate Professor, Department of Criminal Law, International Kazakh-Turkish University after Khoja Akhmet Yassawi, 95 Sattarkhanov Street, 161200, Turkestan, Kazakhstan

Nartay A.N. **–** Corresponding Author, PhD, Senior Lecturer, Department of Constitutional and Civil Law, International Kazakh-Turkish University after Khoja Akhmet Yassawi, 95 Sattarkhanov Street, 161200, Turkestan, Kazakhstan

Rysmagambetova G. **–** Doctor of law, Professor, Department of criminal law, procedure and forensic science, Karaganda National Research University named after academician E.A. Buketov, 28 Universitetskaya st., 100028, Karaganda, Kazakhstan