ҚАЗАҚСТАН РЕСПУБЛИКАСЫ ІШКІ ІСТЕР МИНИСТРЛІГІ
БАСҚАРУ АКАДЕМИЯСЫ

АКАДЕМИЯ УПРАВЛЕНИЯ
МИНИСТЕРСТВА ВНУТРЕННИХ ДЕЛ
РЕСПУБЛИКИ КАЗАХСТАН

ACADEMY OF MANAGEMENT OF THE MINISTRY OF INTERNAL
AFFAIRS OF THE REPUBLIC OF KAZAKHSTAN

«ЖАҺАНДЫҚ ТРАНСФОРМАЦИЯ ЖАҒДАЙЫНДАҒЫ ҚҰҚЫҚ: ЗАМАНАУИ СЫН-ҚАТЕРЛЕР МЕН ДАМУ ПЕРСПЕКТИВАЛАРЫ»

Халықаралық ғылыми-практикалық конференциясының

МАТЕРИАЛДАР ЖИНАҒЫ

(29 мамыр 2026 жыл)

СБОРНИК МАТЕРИАЛОВ

Международной научно-практической конференции

«ПРАВО В УСЛОВИЯХ ГЛОБАЛЬНОЙ ТРАНСФОРМАЦИИ: СОВРЕМЕННЫЕ ВЫЗОВЫ И ПЕРСПЕКТИВЫ РАЗВИТИЯ»

(29 мая 2026 года)

PROCEEDINGS OF MATERIALS

International Scientific and Practical Conference

«LAW IN THE CONTEXT OF GLOBAL TRANSFORMATION: MODERN CHALLENGES AND DEVELOPMENT PROSPECTS»

(29 May, 2026)

Астана қаласы

УДК 340.1
ББК 67.4
Д 46

Жалпы редакциясын басқарған:
ДИЛЬБАРХАНОВА Ж.Р.

Жаһандық трансформация жағдайындағы құқық: заманауи сын-қатерлер мен даму перспективалары атты Халықаралық ғылыми-тәжірибелік конференция материалдары **29 мамыр 2026 жыл** Астана: ҚР ІІМ Басқару академиясы, 2026. **–142 б**.

Д 46

ISBN 978-601-360-301-8

«Жаһандық трансформация жағдайындағы құқық: заманауи сын-қатерлер мен даму перспективалары» атты халықаралық ғылыми-практикалық конференция материалдарының жинағы жаһандық трансформациясы жағдайындағы – қоғам мен құқықтың даму мәселелеріне арналған. Сонымен қатар құқық саласын цифрландыру, заңнаманы жетілдіру, адам құқықтарын қорғау және құқықтық институттарды қазіргі заманғы сын-қатерлерге бейімдеу мәселелері қарастырылған. Бұл материалдар жинағы магистранттар, докоранттар, оқытушылар және тәжірибелі заңгерлер үшін қызығушылық тудырады.

Сборник материалов международной научно-практической конференции «Право в условиях глобальной трансформации: современные вызовы и перспективы развития» посвящён актуальным проблемам развития права в условиях глобальной трансформации общества. В нём рассматриваются вопросы цифровизации правовой сферы, совершенствования законодательства, защиты прав человека и адаптации правовых институтов к современным вызовам. Сборник материалов представляет интерес для магистрантов, докторантов, преподавателей и практикующих юристов.

The proceedings of the international scientific and practical conference «law in the context of global transformation: contemporary challenges and development prospects» are devoted to current issues in the development of law under the conditions of global societal transformation. The publication addresses the digitalization of the legal sphere, the improvement of legislation, the protection of human rights, and the adaptation of legal institutions to contemporary challenges. The proceedings are of interest to master’s students, doctoral candidates, academics, and practicing legal professionals.

УДК 340.1
ББК 67.4

Бұл жинаққа енгізілген материалдарға авторлар жауапты.
Authors are responsible for the content of their materials.

© Қазақстан Республикасы ІІМ Басқару академиясы, 2026



ДИЛЬБАРХАНОВА ЖАНАТ РАХИМЖАНОВНА
Қазақстан Республикасы ІІМ Басқару академиясының бастығы
заң ғылымдарының докторы, профессор
полиция полковнигі

ҚҰРМЕТТІ ӘРІПТЕСТЕР, ҚАДІРЛІ ҚОНАҚТАР, ЖАС ҒАЛЫМДАР!

Форум аясында жоспарланған «Жаһандық трансформация жағдайындағы құқық: заманауи сын-қатерлер мен даму перспективалары» халықаралық ғылыми-тәжірибелік конференцияға қош келдіңіздер!

Бүгінгі басқосу – кеше бастауын алған ауқымды шараның ғылыми жалғасы болып табылады.

Мемлекет басшысы Қасым-Жомарт Кемелұлы Тоқаев атап өткендей, заң үстемдігі мен құқықтық тәртіп – Әділетті Қазақстанның мызғымас тірегі. Бүгінде елімізде «Заң мен Тәртіп» қағидаты мемлекеттік саясаттың басты басымдықтарының біріне айналып отыр. Қоғамдағы тұрақтылық пен қауіпсіздікті қамтамасыз ету, азаматтардың құқықтарын қорғау және құқықтық мәдениетті нығайту – құқық қорғау жүйесі мен заң ғылымының ортақ міндеті. Ал оны нығайтатын – заман талабына бағдарланған заң ғылымы.

Сегодня мы обсуждаем развитие права в условиях глобальной трансформации современного общества. Стремительное развитие

цифровых технологий, изменение характера общественных отношений и трансформация традиционных правовых институтов формируют новые вызовы для правовой системы и правоприменительной практики.

В современных условиях обеспечение законности и правопорядка требует не только совершенствования механизмов государственного управления, но и глубокого научного осмысления происходящих процессов.

Многие правовые подходы сегодня нуждаются в адаптации к новым социальным и технологическим реалиям.

Особую актуальность приобретают вопросы цифровизации права, информационной безопасности, защиты прав и свобод граждан, а также повышения эффективности правоприменительной деятельности. Ответы на эти вызовы невозможны без тесного взаимодействия науки и практики.

Сегодня в этом зале собрались ученые, представители государственных органов, практикующие специалисты и молодые исследователи. Уверена, что объединение научного потенциала и практического опыта позволит выработать конструктивные предложения по совершенствованию законодательства и развитию современной правовой системы.

Особая роль в этом процессе принадлежит молодым ученым, которым предстоит формировать новые научные подходы и определять дальнейшее развитие отечественной юридической науки.

Желаю всем участникам содержательных дискуссий, конструктивного диалога и плодотворной работы.

О ПОИСКЕ НОВЫХ ПУТЕЙ ПРОТИВОДЕЙСТВИЯ ПРЕСТУПНОСТИ В СОВРЕМЕННЫХ УСЛОВИЯХ И ОБЕСПЕЧЕНИЯ ЗАКОНА И ПОРЯДКА В РЕСПУБЛИКЕ КАЗАХСТАН

АКИМЖАНОВ Талгат Курманович
Директор НИИ права, профессор Высшей школы права университета «Туран», доктор юридических наук, профессор, заслуженный работник МВД Республики Казахстан, почетный работник образования Республики Казахстан, полковник юстиции (в отставке)

В статье обоснована необходимость поиска новой модели противодействия преступности, поскольку действующая модель борьбы с преступностью не всегда успевает за количественными и качественными изменениями современной преступности. Автором на основе проведенного исследования, анализа работ ведущих ученых, правоприменительной практики, предложены примерные пути совершенствования противодействия преступности на современном этапе.

В статье внесен ряд конкретных предложений по дальнейшему совершенствованию уголовного законодательства Республики Казахстан.

Как известно, по мнению большинства криминологов, преступность, являясь негативным, социальным, изменчивым уголовно-правовым явлением, которая сопровождает человечество практически с момента его возникновения всегда нуждалась в особом и повышенном внимании со стороны общества.

Современная преступность развиваясь и видоизменяясь вместе с самим обществом, которое ее и порождает, представляет собой большую угрозу и опасность для самого общества, поскольку не только мешает его нормальному функционированию и существованию, но и опосредованно посягает на его национальную безопасность.

Проведенный анализ правоприменительной практики за 35-летний период суверенного развития Казахстана проблеме противодействия преступности уделяется со стороны государства достаточно внимания. Имеется правовая основа противодействия преступности, достаточно мобильная правоохранительная система, и самое главное – сформировано у большей части населения негативное отношение к криминальным проявлениям в обществе.

Процесс борьбы с преступностью всегда развивался на концептуальной основе.

Так, были приняты три Концепции правовой политики Республики Казахстан, которые утверждались указами Президента Республики Казахстан: - первая на период с 2002 по 2010 годы; [1]

-вторая на период с 2010 по 2020 годы; [2]

-третья на период с 2021 по 2030 годы. [3]

Вместе с тем, утверждать в настоящее время, что в реализации данной важной государственной функции все обстоит благополучно, к сожалению, не представляется возможным, так как об этом свидетельствует

правоприменительная практика, а также количественные и качественные показатели самой преступности.

По мнению известного ученого криминолога В.Н.Кудрявцева, в современном обществе наблюдается серьезное противоборство между преступностью и государством. [4, с. 29]

Причем чем совершеннее становятся формы и методы преступной деятельности, тем активнее должна быть деятельность правоохранительных органов и наоборот, когда криминальный мир в целях самосохранения и процветания вынужден приспосабливаться ко всем изменениям и усилениям со стороны правоохранительных органов, а иногда удачно используя возможности государственного аппарата в своих целях.

И любое снижение внимания к вопросам противодействия преступности может негативно сказаться не только на состоянии общественной безопасности и правопорядка, но и национальной безопасности всей страны.

Издержки в деятельности правоохранительных органов Республики Казахстан проявились в период январской трагедии 2022 года, когда мирные демонстрации граждан, недовольных социально-экономическим положением в стране под влиянием террористов и экстремистов превратились в массовые беспорядки сопровождаемые погромами, поджогами, убийствами как сотрудников правоохранительных органов и военнослужащих, так и мирных граждан.

Только активное участие войск ОДКБ, прибывших, благодаря высокому международному авторитету Президента РК К-Ж.К.Токаева в Республику Казахстан, смогло стабилизировать и нормализовать обстановку в Казахстане в кратчайшие сроки.

Как отметил Глава государства К-Ж.К.Токаев по итогам разбора произошедшей трагедии в январе 2022 года, нам не удалось разглядеть в Казахстане на более ранней стадии спящие экстремистские ячейки и эффективно им противодействовать, в результате чего и возникли нежелательные негативные социальные и экономические последствия.

О причинах возникновения январской трагедии 2022 года высказался на страницах газеты «Turkistan» 5 января 2026 года Президент РК Токаев К-Ж.К. где было отмечено, что зачинщики беспорядков под кураторством специалистов по «революциям» воспользовались решением Правительства повысить цены на топливо и спровоцировали выход людей на массовые демонстрации. Затем была спровоцирована паника среди граждан, госслужащих и, что удивительно, среди значительной части силовиков, которые стали покидать места несения службы, оставляя секретные документы, оружие, не выдержали экзамен на верность Отечеству и профессионализм ряд руководителей КНБ и МВД.

Особенно наглядно это проявилось в Алматы – главном направлении удара путчистов. Издевательства над военнослужащими и жителями города достигли крайней степени, погромы, поджоги, грабежи административных зданий, торговых центров, магазинов, банков требовали чрезвычайных мер. Сейчас, по истечении времени, некоторые недобросовестные и недалекие люди со

злорадством несут околесицу, сознательно обходя тему спасения государства от более масштабного гражданского хаоса с фатальными последствиями. [5]

Или другой пример, когда в результате бездействия сотрудников правоохранительных органов было совершено убийство молодой девушки в г. Шымкенте, которое стало резонансным и нашло отражение в выступлении Президента РК К-Ж.К.Токаева на прошедшем V заседании Национального курултая в Кызылорда 22 января 2026 года.

Так, Президентом было отмечено, что наше государство будет твердо защищать права и свободы, честь и достоинство всех граждан.

Жестокое убийство девушки по имени Нурай в Шымкенте вызвало широкий общественный резонанс по всей стране. Курултай получил в связи с этим происшествием более 130 обращений. Установлено, что подозреваемый преследовал Нурай и угрожал ей. В конечном счете, все закончилось ее гибелью.

В связи с этим Президентом РК Токаевым К-Ж.К. было дано поручение министру внутренних дел дать правовую оценку действиям департамента города Шымкента. Генеральному прокурору также надлежит взять на контроль это дело.

По информации МВД РК от занимаемых должностей были освобождены начальник ДП г. Шымкента, его заместитель по следствию и ряд руководящих кадров департамента полиции.

Или другой пример бездействия правоохранительных органов, связанный с резонансным смертельным ДТП, которое произошло в Алматы в ночь на 21 марта 2026 года на проспекте Аль-Фараби. Водитель электромобиля Zeekr 009, который по информации МВД РК находясь в нетрезвом состоянии на высокой скорости выехал на встречную полосу, спровоцировав лобовое столкновение с Mercedes-Benz. В результате аварии погибли три человека: 29-летний водитель Mercedes и двое пассажиров (девушки 20 и 22 лет).

Авария вызвала широкий общественный резонанс, дело находится на контроле, и из-за происшествия был уволен ряд руководителей полиции, включая заместителя начальника Департамента полиции (ДП) Алматы, курирующего дорожную безопасность, начальника управления административной полиции и начальника управления общественной безопасности.

Помимо увольнений, было возбуждено уголовное дело в отношении водителя одного из руководителей ДП (подозреваемого в бездействии).

В современной концепции противодействия преступности должна быть предложена идея, позволяющая повысить эффективность и качество правоприменительной деятельности правоохранительных органов в решении вопросов борьбы с преступностью в Казахстане на основе строжайшего соблюдения норм Конституции Республики Казахстан реализации положений Концепции правовой политики Республики Казахстан до 2030 года, утвержденной Указом Президента Республики Казахстан от 15 октября 2021 года № 674. [3]

Остановимся на некоторых проблемах в сфере противодействия преступности, которые нуждаются, на наш взгляд, в первоочередном исследовании и осмыслении.

Первое. **Назрела необходимость переосмысления отдельных положений сложившейся практики борьбы с преступностью и выработки новой концепции противодействия преступности.**

В первую очередь, необходима более детальная, с применением новых методов и технологий, диагностика самой преступности. Если сравнивать процесс противодействия преступности, которая является своего рода болезнью общества, порождающего эту преступность, то для ее лечения необходим правильный диагноз. В противном случае, как и в медицине, процесс «лечения» такой болезни как преступность не приведет к желательным результатам.

Как известно, благодаря исследованиям ученых-криминологов известно, что современная преступность развивается и видоизменяется вместе с самим обществом, которое ее и порождает и представляет собой большую угрозу и опасность для самого общества, поскольку не только мешает его нормальному функционированию и существованию, но и опосредованно посягает на его национальную безопасность.

По справедливому замечанию О.В.Дамаскина происхождение преступности связывается с периодом возникновения государства, права, социальным, имущественным и классовым расслоением человеческого общества. [6, с. 84].

Как справедливо отмечает один из ведущих ученых-криминологов советского и настоящего периодов Ю.М.Антонян, что преступность и меры борьбы с ней затрагивают практически все сферы бытия человека и общества. Преступление совершает человек, а поэтому именно он должен привлекать исследователя. Хотя человек и не рождается преступником, а становится им под влиянием общества, мы не освобождая его от ответственности, именно поэтому должны сделать все от нас зависящее, больше возможности, но они будут эффективными только в случае умелого и грамотного использования. [7, с. 3]

По мнению В.Е.Эминова социальный характер преступности определяется тем, что это первичный и, по всей видимости, ее важнейший признак, определяющий все остальные. Он определяет социальное происхождение преступности, ее зависимость от общества, которое его продуцирует и влияет на ее количественные и качественные характеристики [8, с. 30].

Среди многих причин отставания процесса противодействия преступности от развития самой преступности является постоянное ее изменение и развитие, приспособление к новым реалиям жизни, которые направлены на совершенствование форм и методов преступной деятельности, чтобы они были более эффективными, недосягаемыми до правоохранительных органов и приносили при этом большую прибыль, а также отсутствие или недостаточное прогностическое направление.

В современной концепции правопонимания должна быть предложена идея, позволяющая повысить эффективность и качество правоприменительной деятельности правоохранительных органов в решении вопросов противодействия преступности в Казахстане на основе строжайшего

соблюдения норм Конституции Республики Казахстан и в тесном контакте и опоре на гражданское общество и, на наш взгляд, большую роль в этом процессе следует отводить науке «Криминологии», изучающей преступность, причины преступности, личность преступника и предупреждение преступности и особенно вопросы криминологического прогнозирования.

О необходимости проведения гибкой, вместе с тем справедливой уголовной политики государства было закреплено в утвержденной Указом Президента Республики Казахстан от 15 октября 2021 года №674 «Концепции правовой политики Республики Казахстан до 2030 года», где было отмечено, что в процессе реализации правоприменительного процесса должны быть пересмотрены формы и методы противодействия преступности, включая и ее организованные формы, скорректировано уголовное и уголовно-процессуальное законодательство Республики Казахстан. [3]

Учитывая способность современной преступности, особенно ее организованных форм проявления, проникать во все отрасли жизнедеятельности общества и, особенно, в экономическую сферу, то нетрудно понять, что система противодействия преступности должна носить упреждающий характер, основанный на данных криминологического анализа и прогноза, и охватывать весь государственный механизм, скорректирована проводимая уголовная политика Республики Казахстан.

Для эффективного противодействия преступности необходим комплекс мероприятий, о чем ранее указывали известные ученые С.В.Бородиным [9, с.3] и В.Н.Кудрявцев[4] в своих фундаментальных работах посвященных изложению концептуальных вопросов противодействия преступности.

Наукам криминологии и уголовному праву предстоит исследовать уголовно-правовое законодательство и правоприменительную практику с тем, чтобы, в первую очередь, установить, а затем и разрешить имеющиеся проблемы в области уголовного права, морали, разумности и справедливости.

Реализация указанных положений уголовной политики Республики Казахстан, по нашему мнению , которое основано на мнении известных ученых в данной сфере, изучении правоприменительной практики как в Казахстане, так и странах дальнего и ближнего зарубежья, позволит улучшить положение такого важного приоритетного направления проводимой в стране правовой политики, как реализация уголовной политики в сфере противодействия современной преступности, позволяющая обеспечить стабильность в обществе, должный правопорядок и согласие, необходимые для поступательного развития экономики, права, политики и других институтов гражданского общества.

Второе. **В обязательном порядке при противодействии преступности следует внедрить прогнозирование процессов изменения преступности, а также мер по их предупреждению и недопущению**.

В результате недостаточного криминологического прогнозирования, в Республике Казахстан упущены начинающие проявления экстремистских течений в обществе.

В Казахстане за последние десятилетия возросли факты вовлечения наших граждан в запрещенную деятельность за пределами государства, а также

усилились попытки внедрения деятельности запрещенных организаций в Казахстан.

Например, если взять только один из видов преступности – преступления экстремистской и террористической направленности, то согласно официальным статистическим сведениям Комитета по правовой статистике и специальным учетам Генеральной прокуратуры Республики Казахстан, количество уголовных правонарушений экстремистской и террористической направленности, зарегистрированных в ЕРДР, принимая во внимание их высокую угрозу национальной безопасности, снова имеет тенденцию роста в последние годы.

Анализ результатов правоприменительной практики свидетельствует не только о распространении радикализма в обыденной жизни, но и его направленности на более высокие цели, в том числе захват власти и создание хаоса в стране через организацию насилия, погромов, убийств и др.

Как известно, благодаря исследованиям ученых-криминологов известно, что современная преступность развивается и видоизменяется вместе с самим обществом, которое ее и порождает и представляет собой большую угрозу и опасность для самого общества, поскольку не только мешает его нормальному функционированию и существованию, но и опосредованно посягает на его национальную безопасность.

В настоящее время в государствах дальнего и ближнего зарубежья сложились определенные системы прогнозирования преступности, особенно ее организованных форм проявления, а также выработки новых форм и методов воздействия и предотвращения их на более ранней стадии.

Однако, судя по результатам правоприменительной практики, мнению ведущих ученых, оптимальные пути прогнозирования преступности на более ранней стадии до сих пор не найдены, их поиски следует продолжить.

Третье. **Рассматривать преступность как одну из угроз национальной безопасности государства.**

Мировое сообщество осознало, что самой главной задачей для человечества в третьем тысячелетии является обеспечение национальной безопасности в отдельно взятом государстве и, в целом, на всем мировом пространстве.

Заслуживает внимания описанная известным ученым криминологом В.Н. Кудрявцевым в своей книге «Стратегия борьбы с преступностью» - стратегия безопасности. Цитируемый автор предлагает меры безопасности определять как предпринимаемые в целях защиты людей, промышленных, военных, научных и иных объектов от преступных посягательств неустановленных (неопределенных) лиц.[4, с. 202]

Как известно, понятие безопасности с позиции различных наук, как правило, трактуется неоднозначно. С позиций юридических наук безопасность рассматривается как система установления правовых гарантий защищенности личности и общества, обеспечения их нормальной жизнедеятельности, прав и свобод.

Законом Республики Казахстан от 6 января 2012 года «О национальной безопасности Республики Казахстан» к одним из источников угроз национальной безопасности, наряду с другими, отнесены снижение уровня

законности и правопорядка, в том числе рост преступности, включая организованные ее формы, сращивание государственных органов с криминальными структурами, террористическими и экстремистскими организациями, покровительство должностных лиц незаконному обороту капитала, коррупция, незаконный оборот оружия и наркотических средств, способствующих снижение степени защищенности национальных интересов. [10, с. 202]

То есть, у нас есть все правовые основания рассматривать преступность как один из главных источников угрозы национальной безопасности страны. А процесс борьбы с преступностью есть процесс обеспечения национальной безопасности Республики Казахстан.

Обеспечение национальной безопасности нашего государства является главной стратегической задачей, поскольку необеспечение национальной безопасности государства влечет потерю его суверенитета.

Четвертое. **Обеспечение научного сопровождения процесса борьбы с преступностью.**

Издержками нашей правоохранительной системы является то, что получаемая информация в целом о преступности, о ее количественных и качественных характеристиках в основном собирается и не подвергается глубокому анализу, то есть отсутствует обратная связь.

Недостаточное научное обеспечение практической деятельности правоохранительных органов привело к тому, что в деятельности последних, слабо представлена аналитическая работа, нет достаточно глубокого факторного анализа преступности и прогностического направления в борьбе с ней, не внедрены современные методы (методики) (математические, социологические и др.) анализа преступности.

По этой причине, правоохранительные органы не получают научных рекомендаций, реализация которых позволила бы значительно повысить эффективность правоприменительной деятельности и внедрить инновационные формы и методы работы.

Например, интересную мысль по этому поводу высказала известный советский – российский ученый криминолог А.И.Долгова на XI Российском Конгрессе уголовного права, 31 мая 2018 года в Москве в МГУ имени М.В.Ломоносова, что пагубно сказывается на противостоянии преступности и обеспечении национальной безопасности:

- сворачивание в России в новом веке криминологической, а также социально-правовой научно-исследовательской деятельности в государственных учреждениях;

- исключение криминологии из числа обязательных для преподавания будущим юристам дисциплин;

- нарастание числа учебников, учебных пособий и других публикаций авторов, не имеющих фундаментальной подготовки, навыков и опыта криминологических исследований, делающих акцент на общих, нередко узкосубъективных рассуждениях о преступности и миропорядке.

Ликвидация ранее существовавшего самого крупного в мире Всесоюзного института по изучению причин и разработке мер предупреждения преступности. В данном институте в комплексе разрабатывались вопросы наук криминального цикла (криминологические, уголовно-правовые, уголовно-процессуальные, уголовно-исполнительные, криминалистические и др.). Без воссоздания такого научно-исследовательского учреждения проблематично должное научное обеспечение не только борьбы с преступностью, но и более широкой деятельностью по обеспечению национальной безопасности. [11, с. 360]

Такое же предложение ранее высказывал и казахстанский ученый Е.О.Алауханов, что в Казахстане пока нет научно-исследовательской организации по вопросам изучения причин и условий, способствующих совершению преступлений. Хотя в России и в ряде зарубежных стран данные учреждения плодотворно действуют и дают положительные результаты. [12, с.72-73]

Например, в настоящее время в Российской Федерации в структуре МВД РФ успешно функционирует Всероссийский научно-исследовательский институт МВД РФ (бывший Всесоюзный научно-исследовательский институт МВД СССР), в котором автору статьи посчастливилось вместе с некоторыми коллегами из Казахстана обучаться в очной адъюнктуре (аспирантуре), в период бывшего СССР и увидеть какой вклад вносит данное учреждение в дело противодействия преступности.

Для разрешения проблемы научного обеспечения процесса противодействия преступности предлагается, по опыту бывшего СССР создать в Республике Казахстан Республиканский НИИ при Генеральной прокуратуре РК, а в структуре МВД РК создать на правах самостоятельного комитета или департамента Научно-исследовательский институт МВД РК, а в структуре областных департаментов полиции, а также департаментах полиции городов Астана, Алматы, Шымкент создать структурные подразделения НИИ МВД РК - криминологические центры, которые занимались бы изучением и анализом складывающейся криминальной ситуации, личности преступника и обеспечивали бы научное сопровождение процесса борьбы с преступностью на местах.

Результаты деятельности указанных научных подразделений послужат толчком во внедрении инноваций в вопросы изучения тенденций современной преступности, ее прогнозированию, а также борьбы с преступностью и, вместе с тем, будут обеспечивать развитие новых идей стратегии развития уголовной политики Республики Казахстан.

В противном случае, правоприменение без научного сопровождения процесса противодействия преступности может снизить его эффективность и намного отодвинуть продвижение в данном вопросе правоохранительной системы Республики Казахстан.

Пятое. **Необходимость расширения сферы противодействия преступности.** Поскольку общество и преступность всегда существовали вместе и тесно взаимосвязаны, то будет правильным рассматривать процесс борьбы с

преступностью не только как воздействие на преступность, как негативную составную общества, но и на само общество, которое и порождает эту преступность.

Так, Г.А.Аванесов отмечал, что преступность порождена условиями общественной жизни, но она и сама часть этих условий [13, с.18].

Наша правоохранительная система свое внимание сконцентрировала лишь на той части населения, которая совершает уголовные правонарушения (преступления, уголовные проступки. А основная часть представителей общества, законопослушных граждан, остается вне поля зрения. Например, если при численности населения Казахстана 20 миллионов человек ежегодно регистрируется примерно 270-350 тысяч преступлений, то доля совершенных преступлений, а также лиц их совершивших составляет всего 1,9 % от всего населения.

Если сравнить этот процесс с медициной, то врачей, как правило, интересует только больная часть населения, с различными диагнозами, а здоровую часть населения, которая в любую минуту может оказаться больной, они во внимание не берут. То же самое и наблюдается в сфере противодействия преступности.

Хотя особой границы, разделяющей законопослушное население и лиц совершивших или склонных к совершению преступлений в природе не существует. Любой законопослушный гражданин может оказаться на скамье подсудимых. И каждое лицо, отбывающее наказание в исправительном учреждении может стать законопослушным человеком и вернуться к нормальной жизни.

Данный процесс должен предполагать более широкие и масштабные мероприятия, реализация которых способствовала бы не только устранению конкретных причин и условий преступности, но и включали бы в себя воздействие и на здоровую, законопослушную часть общества, чтобы ее представители как можно меньше переходили в противоположный лагерь.

То есть при организации противодействия преступности в современных условиях следует упор делать на гражданское общество с участием которого, правоохранительные органы могли бы привлечь его на свою сторону и значительно повысить эффективность в своей работе.

Именно на это нацеливает Концепции по продвижению в обществе идеологии закона и порядка на 2025 – 2030 годы, утвержденная постановлением Правительства Республики Казахстан от 1 апреля 2025 года № 200, согласно п 5.4 которой предусмотрено повышение правовой культуры – комплексная задача, требующая объединения усилий государства, бизнеса, неправительственных организаций, образовательных учреждений, средств массовой информации и самих граждан. Здесь требуется действенная координация всех задействованных структур. [14]

Шестое. **Минимизация вовлечения граждан в сферу уголовной юстиции.**

Как нам представляется, задача государства состоит в том, чтобы, с одной стороны обеспечить неотвратимость наказания за совершенное преступление, а

с другой стороны сделать данное наказание наиболее справедливым и эффективным, максимально уменьшив социальные последствия, как для самого осужденного, так и для государства, в целом. При этом, не превращая осужденного в изгоя и вечного врага правосудия.

Кроме этого, увеличение индекса тюремного населения сказывается не только на имидже страны, но и имеет прямое отношение к национальной безопасности государства, так как способствует криминализации новых членов общества, проникновению субкультуры в общественные отношения и подрывает устои общества и общественной безопасности, а также разлагает мораль и нравственность законопослушных граждан.

Например, по данным Комитета уголовно-исполнительной системы МВД РК за период суверенного развития нашей страны, то есть с 1991 по 2026 годы через исправительные учреждения прошло свыше миллиона семисот тысяч человек.

В настоящее время положение вовлеченности населения в систему уголовной юстиции значительно изменилось в лучшую сторону.

Однако, тенденция роста численности «тюремного населения», а значит и роста вовлеченности граждан в сферу уголовной юстиции в Республике Казахстан, сохраняется.

Как нам представляется, одной из причин такого положения является состояние уголовного законодательства Республики Казахстан и в частности санкций, предусмотренных в статьях Особенной части УК Республики Казахстан, о которых более подробнее будет отмечено ниже.

Поэтому для реализации мер по минимизации вовлечения граждан в сферу уголовной юстиции, следует продолжить практику максимального исключения из санкций статей Особенной части УК РК такого вида наказания как лишение свободы, имеющего социальные, экономические и правовые негативные последств и замены его на альтернативные виды наказаний, не связанные с изоляцией от общества.

Седьмое. **Усиление профилактической направленности процесса борьбы с преступностью.** Как справедливо отмечают российские ученые П.В.Агапова, Г.Н.Антонов-Романовский, В.К. Артеменков, что вековая история развития преступности неразрывно связана с проблемой ее предупреждения. Если на первых порах человеческое общество не знало других средств ее преодоления, кроме самых жестоких расправ с преступниками, то по мере развития обшественных отношений, формирования юридических познаний сущности социальных процессов, их преломления в индивидуальном восприятии общество все чаще стало обращаться к реальным возможностям и средствам предупреждения как отдельных видов преступности, так и отдельных посягательств. [15, с.37]

В целях активизации принятого Закона Республики Казахстан 30 декабря 2025 года «О профилактике правонарушений»[16] было бы целесообразным, принять на правительственном уровне План мероприятий по реализации Закона РК «О профилактике правонарушений» с конкретными мероприятиями, которые

должны быть обеспечены организационно и финансово со стороны государства, как на республиканском, так и на местном уровне.

Следовало бы обязать все органы, указанные в Законе к неукоснительному исполнению всех его требований с истребованием ежегодных отчетов о его реализации.

Использовать возможности Законов РК «О профилактике правонарушений»[16] и «О национальной безопасности Республики Казахстан».[10, с. 50] для объединения усилий всех органов и общественности по формированию новой идеологии в обществе в сфере противодействия преступности. Разъяснить всему обществу, что противодействие преступности это задача всего общества, а не только правоохранительных органов.

Кроме этого, следовало бы создать специальные структурные подразделения, обеспечивающие организацию профилактической работы в стране. Ими могли бы стать специальный Комитет или департамент в структуре МВД РК, в департаментах полиции Астаны, Алматы, Шымкента, а также областных департаментов полиции.

Также было бы целесообразным в условиях повышения политической и гражданской активности граждан, предусмотреть создание во всех структурных единицах РК (Область, город, село, район) дворцов-домов демократии, где могли бы официально собираться группы людей, партии, объединения для выражения своих идей и взглядов, с участием руководителей регионов, а также правоохранительных органов для оперативного реагирования на вносимые предложения, под контролем санврачей и т.д.

Восьмое. **Меры по совершенствованию действующего уголовного законодательства РК.** На основании результатов одиннадцатилетней правоприменительной практики, с момента вступления в силу нового уголовного законодательства Республики Казахстан (1 января 2015 года) предлагаются следующие дополнения в действующее уголовное законодательство:

1.Продолжить работу по сокращению в уголовном законодательстве Республики Казахстан такого вида наказания как лишение свободы. Кроме этого предусмотреть в законодательном порядке некоторые ограничения на применение указанного вида наказания.

2.Расширить перечень оснований категоризации преступлений в ст. 11 УК РК, дополнив его другими видами наказаний (штраф, ограничение свободы и т.д).

3.Снизить предельные сроки лишения свободы, предусмотренные в ст. 46 УК РК 2014 установив наиболее оптимальные сроки наказания: за совершенные умышленные преступления не свыше 10 лет, за неосторожные преступления до 5 лет, по совокупности преступлений до 12 лет и по совокупности приговоров не более 15 лет лишения свободы.

4.Предусмотреть особый порядок назначения и исполнения наказаний, в отношении лиц, осужденных за экономические, должностные и коррупционные преступления.

5.Изменить порядок условно-досрочного освобождения, установленный в части 3 статьи 72 УК РК установив новые обязательные сроки отбытия наказания

при условно-досрочном освобождении от отбывания наказания : за преступления небольшой тяжести – до 1 года, средней тяжести до 2 лет, тяжкие – до 3 лет, особо тяжкие до 4 лет.

6.*Расширить применение института условного осуждения. (Статья 63 УК РК 2014 года Условное осуждение)*

С учетом вышеперечисленных обстоятельств можно констатировать, что предложенный подход к переосмыслению отдельных аспектов противодействия преступности будет способствовать решению многих задач, стоящих перед правоохранительными органами и повышению эффективности участия в данном процессе всего гражданского общества.

1.Указ Президента Республики Казахстан от 20 сентября 2002 года № 949 (Утратил силу Указом Президента Республики Казахстан от 17 июня 2011 года № 102)
2.Указ Президента Республики Казахстан от 24 августа 2009 года № 858 «О Концепции правовой политики Республики Казахстан на период с 2010 до 2020 года» (с изменениями и дополнениями от 16.01.2014 г.) // http:jnline.zakon.kz
3.Об утверждении Концепции правовой политики Республики Казахстан до 2030 года. Указ Президента Республики Казахстан от 15 октября 2021 года № 674
4.**Кудрявцев В.Н.** Стратегии борьбы с преступностью.-М.: Юристъ, 2003. -352 с.
5.Личность преступника и профилактика преступлений: монография /**Ю.М.Антонян, А.Е.Антонян, О.Р.Афанасьева** [и др]; под ред. **Ю.М.Антоняна.-** Москва: Проспект, 2017.- 224 с.
6.Криминология: учебник /отв. Ред. В.Е.Эминов.- Москва:Проспект, 2024.-368 с.
7.Газета «Turkistan», 5 января 2026 года, №1 (1638)
8.**Дамаскин О.В.** Криминологические аспекты противодействия преступности: научн.-прак. Пособие.- М.: Юрлитинформ, 2017. - 264 с.
9. Бородин С.В. Борьба с преступностью: теоретическая модель комплексной программы.- М.: Наука, 1990.- 272 с.
10.Правоохранительные органы: Сборник законодательных актов. – Алматы: Юрист, 2019. -256 с.
11.Обеспечение национальной безопасности – приоритетное направление уголовно-правовой, криминологической и уголовно-исполнительной политики: материалы XI Российского Конгресса уголовного права, посвященного памяти доктора юридических наук, профессора Владимира Сергеевича Комиссарова, состоявшегося 31 мая-1 июня 2018 года.-М.: Юрлитинформ, 2018. – 752 с.
12.**Алауханов Е.О.** Криминология. Учебник: Общая и Особенная части.- Алматы: Жеті жарғы, 2008. -664 с.
13.**Аванесов Г.А.** Преступность и социальные сословия. Криминологические рассуждения: монография, М, ЮНИТИ-ДАНА, 2010.- 72 с.
14. Об утверждении Концепции по продвижению в обществе идеологии закона и порядка на 2025 – 2030 годы. Постановление Правительства Республики Казахстан от 1 апреля 2025 года № 200
15.Теоретические основы предупреждения преступности на современном этапе развития российского общества: монография **/П.В.Агапов, Г.В.Антонов-Романовский, В.К.Артеменков** [и др.]; под общ. Ред. Р.В.Журбина; Академия Генеральной прокуратуры Российской Федерации.- Москва: Проспект, 2018. -656 с.
16. «О профилактике правонарушений». Закон Республики Казахстан от 30 декабря 2025 года № 245-VIII ЗРК.

ПРАВОВАЯ СИСТЕМА В ЭПОХУ ГЛОБАЛЬНОЙ ТРАНСФОРМАЦИИ: СОВРЕМЕННЫЕ УГРОЗЫ ЦИФРОВОЙ БЕЗОПАСНОСТИ И ПЕРСПЕКТИВЫ МЕЖДУНАРОДНОГО ПРАВОВОГО СОТРУДНИЧЕСТВА

АБЕНОВ Архат Асетович
Академия КНБ Республики Казахстан, г. Алматы

В статье рассматриваются современные угрозы цифровой безопасности в условиях глобальной трансформации правовой системы и развития цифровых технологий. Анализируются основные вызовы, связанные с распространением киберпреступности, защитой персональных данных, транснациональным характером цифровых угроз и необходимостью совершенствования механизмов правового регулирования в цифровой среде. Особое внимание уделяется вопросам международного правового сотрудничества в сфере противодействия киберугрозам, обмена информацией и формирования единых подходов к обеспечению цифровой безопасности. Рассматриваются современные тенденции развития международного цифрового права, а также перспективы адаптации национального законодательства Республики Казахстан к глобальным вызовам цифровой эпохи. По результатам исследования определены основные направления совершенствования правового регулирования и укрепления международного взаимодействия в сфере цифровой безопасности.

Современный этап развития мирового сообщества характеризуется стремительной цифровизацией практически всех сфер общественной жизни. Развитие информационно-коммуникационных технологий, глобальных цифровых платформ и систем обработки данных оказывает существенное влияние на экономические, политические и правовые процессы. В условиях глобальной трансформации цифровые технологии становятся неотъемлемой частью функционирования государственных институтов, включая сферу правоприменительной деятельности и обеспечения национальной безопасности.

Цифровизация оказывает значительное воздействие на развитие правовой системы, изменяя характер общественных отношений, механизмы государственного управления и способы правового регулирования. В современных условиях право сталкивается с необходимостью адаптации к новым цифровым реалиям, связанным с использованием искусственного интеллекта, электронного документооборота, цифровых платформ и автоматизированных систем принятия решений. В Республике Казахстан процесс цифровой трансформации является одним из приоритетных направлений государственной политики, направленной на модернизацию системы государственного управления и развитие цифрового государства.

Одновременно с развитием цифровых технологий возрастает количество угроз в сфере цифровой безопасности. Распространение киберпреступности, кибератак, незаконного доступа к информационным системам, утечки персональных данных и иных цифровых угроз создает серьезные риски как для отдельных граждан, так и для государственных институтов. Особенностью современных цифровых угроз является их транснациональный характер, поскольку большинство киберпреступлений выходит за пределы одной

юрисдикции и требует международного взаимодействия правоохранительных органов.

В условиях глобализации обеспечение цифровой безопасности становится невозможным без эффективного международного правового сотрудничества. Современные государства заинтересованы в формировании единых подходов к противодействию киберугрозам, совершенствовании механизмов обмена информацией и разработке международных стандартов цифрового права. Для Республики Казахстан вопросы международного сотрудничества в сфере цифровой безопасности приобретают особую актуальность в связи с необходимостью укрепления национальной системы информационной безопасности и адаптации законодательства к современным глобальным вызовам [1].

Целью настоящей статьи является исследование современных угроз цифровой безопасности, а также анализ перспектив международного правового сотрудничества в условиях глобальной трансформации правовой системы и развития цифровых технологий.

Современное развитие цифровых технологий оказывает существенное влияние на трансформацию правовой системы и механизмов государственного управления. Глобальная цифровизация приводит к изменению характера общественных отношений, способов взаимодействия государства и общества, а также форм реализации прав и обязанностей субъектов права. В условиях цифровой эпохи правовая система постепенно адаптируется к новым технологическим реалиям, связанным с использованием информационно-коммуникационных технологий, искусственного интеллекта и цифровых платформ.

Под цифровой трансформацией правовой системы понимается процесс внедрения цифровых технологий в сферу правового регулирования, правоприменительной деятельности и государственного управления. Данный процесс сопровождается изменением традиционных механизмов функционирования государственных институтов, модернизацией системы оказания государственных услуг и развитием электронного взаимодействия между государством, обществом и бизнесом.

Глобализация и развитие цифровой среды способствуют формированию новых правовых отношений, значительная часть которых осуществляется в виртуальном пространстве. Электронная коммерция, цифровые финансовые технологии, дистанционные формы взаимодействия и международный обмен информацией создают необходимость пересмотра традиционных подходов к правовому регулированию. В современных условиях государство сталкивается с задачей обеспечения эффективного контроля за цифровыми процессами при одновременном соблюдении прав и свобод человека.

Существенное влияние цифровые технологии оказывают на деятельность государственных и правоохранительных органов. Использование электронного документооборота, автоматизированных информационных систем и цифровых платформ позволяет повысить оперативность принятия решений, сократить административные процедуры и улучшить доступ граждан к государственным

услугам. В Республике Казахстан цифровизация государственного управления реализуется в рамках развития электронного правительства и внедрения современных цифровых сервисов.

Одним из наиболее значимых направлений цифровой трансформации является развитие электронного правосудия. Использование цифровых технологий в судебной системе позволяет обеспечить дистанционное рассмотрение дел, электронную подачу документов и автоматизацию отдельных юридических процедур. Это способствует повышению прозрачности судебной деятельности и расширению возможностей доступа граждан к правосудию.

Вместе с тем цифровая трансформация правовой системы сопровождается рядом сложностей и противоречий. Развитие цифровой среды создает новые формы правонарушений, усложняет механизмы определения юрисдикции и требует постоянного обновления нормативно-правовой базы. Кроме того, активное внедрение цифровых технологий усиливает зависимость государственных систем от уровня информационной безопасности и устойчивости цифровой инфраструктуры.

Развитие цифровых технологий наряду с расширением возможностей государственного управления и международного взаимодействия сопровождается ростом угроз в сфере цифровой безопасности. В условиях глобальной цифровизации информационные системы становятся одной из ключевых основ функционирования государства, экономики и общества, что делает их объектом повышенного внимания со стороны киберпреступников и иных деструктивных субъектов. Современные цифровые угрозы отличаются высокой степенью технологичности, транснациональным характером и способностью причинять значительный ущерб как отдельным гражданам, так и государственным институтам.

Одной из наиболее распространенных угроз является киберпреступность. В настоящее время преступления, совершаемые с использованием информационно-коммуникационных технологий, приобретают все более сложный и организованный характер. К числу наиболее распространенных форм киберпреступности относятся незаконный доступ к информационным системам, хищение персональных данных, цифровое мошенничество, распространение вредоносного программного обеспечения, кибершпионаж и атаки на государственные электронные ресурсы. Особую опасность представляют кибератаки на объекты критической инфраструктуры, поскольку их последствия способны затронуть безопасность государства и устойчивость функционирования стратегически важных систем.

Серьезной проблемой остается защита персональных данных. В условиях цифровизации государственные органы, финансовые организации и цифровые платформы осуществляют обработку значительных объемов информации о гражданах. Недостаточный уровень защиты цифровых систем создает риск утечки конфиденциальной информации, нарушения права на неприкосновенность частной жизни и незаконного использования персональных данных. В связи с этим вопросы обеспечения информационной безопасности и совершенствования механизмов защиты данных приобретают особое значение.

В современных условиях активно распространяются различные формы цифрового мошенничества. Использование фишинговых технологий, поддельных электронных сервисов, мошеннических интернет-платформ и методов социальной инженерии позволяет злоумышленникам получать доступ к банковским данным, электронным аккаунтам и иной конфиденциальной информации пользователей. Развитие цифровых финансовых технологий одновременно повышает уровень комфорта для граждан и создает новые риски финансовых преступлений в виртуальной среде.

Дополнительную угрозу представляет распространение вредоносного программного обеспечения и использование технологий искусственного интеллекта в противоправных целях. Современные цифровые инструменты позволяют автоматизировать кибератаки, создавать сложные механизмы обхода систем защиты и распространять дезинформацию в информационном пространстве. В результате цифровые угрозы затрагивают не только техническую сферу, но и оказывают влияние на общественную стабильность, политические процессы и международную безопасность.

Особенностью современных цифровых угроз является их транснациональный характер. Большинство киберпреступлений совершается с использованием международных цифровых сетей и затрагивает территории нескольких государств одновременно. Это существенно осложняет деятельность правоохранительных органов, поскольку национальные механизмы правового регулирования не всегда способны эффективно реагировать на преступления, совершаемые в глобальном цифровом пространстве. В связи с этим возрастает необходимость международного сотрудничества в сфере противодействия цифровым угрозам и разработки единых подходов к обеспечению цифровой безопасности.

Для Республики Казахстан обеспечение цифровой безопасности становится одним из приоритетных направлений государственной политики. Развитие цифрового государства, внедрение электронных сервисов и расширение цифровой инфраструктуры требуют постоянного совершенствования механизмов киберзащиты и адаптации законодательства к современным вызовам цифровой эпохи. В современных условиях эффективность системы цифровой безопасности во многом определяется способностью государства своевременно реагировать на новые угрозы и обеспечивать устойчивость функционирования национального информационного пространства [2].

В условиях глобализации и стремительного развития цифровых технологий международное правовое сотрудничество становится необходимым условием эффективного противодействия современным цифровым угрозам. Транснациональный характер киберпреступности, международный обмен информацией и глобальная взаимосвязанность цифровых систем требуют координации действий государств и формирования единых подходов к обеспечению цифровой безопасности.

Современные киберугрозы зачастую выходят за пределы юрисдикции одного государства, что существенно осложняет деятельность национальных правоохранительных органов. Преступления, совершаемые в цифровой среде,

могут одновременно затрагивать информационные системы нескольких стран, а лица, осуществляющие противоправную деятельность, нередко используют международные цифровые сети для сокрытия своей личности и местонахождения. В таких условиях борьба с киберпреступностью становится невозможной без международного взаимодействия, обмена оперативной информацией и проведения совместных расследований.

Одним из ключевых направлений международного сотрудничества является разработка международных правовых механизмов противодействия киберпреступности. В настоящее время многие государства и международные организации осуществляют работу по формированию единых стандартов цифровой безопасности, совершенствованию механизмов правового регулирования цифровой среды и унификации законодательства в сфере информационной безопасности. Международные соглашения и совместные программы позволяют государствам координировать деятельность правоохранительных органов и повышать эффективность противодействия цифровым угрозам.

Особое значение приобретает международный обмен информацией в сфере цифровой безопасности. Оперативное взаимодействие между государствами способствует своевременному выявлению киберугроз, предотвращению масштабных кибератак и установлению лиц, причастных к совершению цифровых преступлений. Современные условия требуют создания эффективных механизмов обмена данными, способных обеспечить баланс между обеспечением национальной безопасности и соблюдением международных стандартов защиты прав человека и конфиденциальной информации.

Важную роль в обеспечении международной цифровой безопасности играют международные организации. Их деятельность направлена на разработку рекомендаций, координацию международного сотрудничества, проведение исследований и формирование единых подходов к регулированию цифровой среды. Международные организации также способствуют развитию правовых механизмов защиты персональных данных, обеспечению устойчивости цифровой инфраструктуры и повышению уровня глобальной кибербезопасности [3].

Вместе с тем международное сотрудничество в сфере цифровой безопасности сталкивается с рядом проблем. Одной из основных сложностей является отсутствие единых международных подходов к регулированию цифрового пространства. Различия в национальном законодательстве, уровне технологического развития государств и подходах к обеспечению информационной безопасности затрудняют процесс унификации международного цифрового права. Кроме того, государства по-разному определяют пределы вмешательства в цифровую среду, вопросы цифрового суверенитета и механизмы контроля за трансграничным обменом информацией [4].

Для Республики Казахстан международное сотрудничество в сфере цифровой безопасности имеет стратегическое значение. В условиях активного развития цифровой инфраструктуры и интеграции в глобальное

информационное пространство государство заинтересовано в укреплении взаимодействия с зарубежными партнерами, совершенствовании национального законодательства и внедрении международных стандартов цифровой безопасности. Участие Казахстана в международных инициативах в области кибербезопасности способствует повышению устойчивости национальной правовой системы к современным цифровым угрозам.

В условиях глобальной цифровизации Республика Казахстан активно реализует политику развития цифрового государства и модернизации системы государственного управления. Цифровая трансформация рассматривается как один из ключевых факторов повышения эффективности государственных институтов, развития экономики и укрепления национальной безопасности. В последние годы в Казахстане осуществляется внедрение электронных государственных услуг, развитие цифровой инфраструктуры и совершенствование механизмов информационной безопасности.

Одним из приоритетных направлений государственной политики является развитие электронного правительства и цифровых сервисов. Использование современных информационно-коммуникационных технологий позволяет повысить доступность государственных услуг, сократить административные барьеры и обеспечить более эффективное взаимодействие государства и общества. Внедрение цифровых платформ способствует автоматизации государственных процессов и повышению прозрачности деятельности государственных органов.

Одновременно с развитием цифровой среды возрастает необходимость обеспечения национальной цифровой безопасности. В условиях активного внедрения информационных технологий государственные информационные системы становятся объектами потенциальных киберугроз, что требует постоянного совершенствования механизмов киберзащиты и укрепления устойчивости цифровой инфраструктуры. В Республике Казахстан принимаются меры по развитию системы информационной безопасности, совершенствованию законодательства в сфере информатизации и противодействию киберпреступности.

Особое внимание уделяется вопросам защиты персональных данных и обеспечения безопасности цифрового пространства. В современных условиях государство сталкивается с необходимостью регулирования процессов обработки и хранения информации, а также предотвращения незаконного использования цифровых данных. Развитие цифровых технологий требует постоянной адаптации национального законодательства к современным вызовам и международным стандартам цифровой безопасности.

Важным направлением государственной политики является противодействие киберпреступности. В Казахстане совершенствуются механизмы выявления и расследования цифровых преступлений, развивается взаимодействие между государственными органами и усиливается контроль за безопасностью информационных систем. Вместе с тем транснациональный характер современных цифровых угроз требует расширения международного

сотрудничества и укрепления взаимодействия с зарубежными государствами в сфере обмена информацией и совместного противодействия киберугрозам.

Для Республики Казахстан международное сотрудничество в сфере цифровой безопасности имеет особое значение в условиях интеграции в глобальное информационное пространство. Участие в международных инициативах и развитие партнерских отношений в области цифрового права позволяют государству внедрять современные механизмы защиты информации, совершенствовать национальную систему кибербезопасности и адаптировать законодательство к мировым тенденциям развития цифровой среды [5].

Перспективы развития правовой системы Казахстана во многом связаны с дальнейшим совершенствованием механизмов правового регулирования цифрового пространства, развитием цифровой грамотности населения и подготовкой квалифицированных специалистов в сфере цифрового права и информационной безопасности. В современных условиях обеспечение устойчивости национальной правовой системы требует комплексного подхода, сочетающего развитие технологий, совершенствование законодательства и укрепление международного взаимодействия.

В условиях стремительного развития цифровых технологий и роста современных цифровых угроз особую актуальность приобретает совершенствование механизмов правового регулирования в сфере цифровой безопасности. Эффективное функционирование правовой системы в цифровую эпоху требует комплексного подхода, направленного на адаптацию законодательства к новым технологическим реалиям, обеспечение защиты прав человека и укрепление международного сотрудничества.

Одним из ключевых направлений совершенствования правового регулирования является дальнейшее развитие национального законодательства в сфере цифровой безопасности. Современные цифровые угрозы требуют своевременного обновления нормативно-правовой базы, регулирующей вопросы кибербезопасности, защиты персональных данных, функционирования информационных систем и противодействия киберпреступности. Законодательство должно учитывать высокую динамику развития цифровых технологий и обеспечивать эффективное регулирование общественных отношений в цифровой среде.

Особое значение приобретает формирование международных правовых стандартов цифрового права. Транснациональный характер современных цифровых угроз делает необходимым создание единых подходов к регулированию цифрового пространства, обмену информацией и обеспечению международной информационной безопасности. Разработка унифицированных международных механизмов позволит повысить эффективность противодействия киберпреступности и укрепить взаимодействие государств в сфере цифровой безопасности.

В современных условиях важным направлением правового регулирования становится использование технологий искусственного интеллекта и цифровых платформ. Активное внедрение автоматизированных систем в государственное управление, финансовую сферу и правоприменительную деятельность требует

разработки правовых и этических механизмов регулирования искусственного интеллекта. Особое внимание должно уделяться вопросам прозрачности алгоритмов, защиты персональных данных, предотвращения дискриминации и сохранения человеческого контроля при принятии юридически значимых решений.

Дополнительную актуальность приобретает усиление механизмов защиты персональных данных. В условиях цифровизации объемы обрабатываемой информации постоянно увеличиваются, что создает риск незаконного использования и распространения конфиденциальных сведений. В связи с этим государствам необходимо совершенствовать механизмы хранения, обработки и защиты цифровых данных, а также обеспечивать соблюдение прав граждан на неприкосновенность частной жизни.

Эффективное развитие цифрового права невозможно без повышения уровня цифровой грамотности населения и подготовки квалифицированных специалистов в сфере информационной безопасности. Современные условия требуют модернизации системы юридического образования, развития научных исследований в области цифрового права и формирования профессиональных компетенций, связанных с регулированием цифровой среды.

Для Республики Казахстан совершенствование правового регулирования в условиях глобальной цифровой трансформации является одним из приоритетных направлений государственной политики. Развитие цифрового государства, внедрение международных стандартов информационной безопасности и укрепление международного сотрудничества создают основу для повышения устойчивости национальной правовой системы к современным цифровым вызовам.

Глобальная цифровая трансформация оказывает существенное влияние на развитие современной правовой системы и формирование новых механизмов обеспечения национальной и международной безопасности. В условиях активного внедрения цифровых технологий возрастает роль цифрового права, совершенствования механизмов правового регулирования и укрепления международного сотрудничества в сфере противодействия современным цифровым угрозам.

Проведенный анализ показывает, что развитие цифровой среды сопровождается не только расширением возможностей государственного управления и международного взаимодействия, но и ростом киберпреступности, увеличением числа кибератак, угроз информационной безопасности и рисков, связанных с незаконным использованием персональных данных. Особенностью современных цифровых угроз является их транснациональный характер, что делает необходимым развитие эффективных механизмов международного правового сотрудничества.

В современных условиях правовая система сталкивается с необходимостью адаптации к новым технологическим реалиям. Развитие цифровых платформ, использование искусственного интеллекта и автоматизация отдельных юридических процессов требуют постоянного совершенствования законодательства и формирования современных подходов к регулированию

цифрового пространства. Особое значение приобретают вопросы обеспечения баланса между технологическим развитием, защитой прав человека и сохранением устойчивости национальной системы безопасности.

Для Республики Казахстан обеспечение цифровой безопасности становится одним из стратегических направлений государственной политики. Развитие цифрового государства, совершенствование законодательства в сфере информатизации и участие в международном сотрудничестве создают основу для укрепления национальной правовой системы в условиях глобальных цифровых вызовов. Вместе с тем дальнейшее развитие цифровой среды требует усиления механизмов киберзащиты, повышения цифровой грамотности и подготовки специалистов в области цифрового права и информационной безопасности.

1. **Susskind R.** *Online Courts and the Future of Justice*. — Oxford : Oxford University Press, 2019. — 368 p.
2. **Katsh E., Rabinovich-Einy O.** *Digital Justice: Technology and the Internet of Disputes*. — New York : Oxford University Press, 2017. — 272 p.
3. **Brenner S.W.** *Cybercrime and the Law: Challenges, Issues, and Outcomes*. — Boston : Northeastern University Press, 2012. — 336 p.
4. OECD Digital Security Risk Management for Economic and Social Prosperity : OECD Recommendation and Companion Document. — Paris : OECD Publishing, 2021.
5. United Nations E-Government Survey 2024 : Digital Government for Sustainable Development. — New York : United Nations, 2024.

ІШКІ ІСТЕР ОРГАНДАРЫНЫҢ ҚҰҚЫҚ ҚОЛДАНУ ҚЫЗМЕТІ САЛАСЫНДАҒЫ ҚАЗІРГІ ЗАМАНҒЫ СЫН-ҚАТЕРЛЕРІ

АБЕНОВ Ришат Талгатович
Қазақстан Республикасы Ш. Қабылбаева атындағы Қостанай академиясы, Қостанай қаласы

Ғылыми баяндамада қоғамдық қатынастарды цифрландыру және қылмысты трансформациялау жағдайында Қазақстан Республикасы ішкі істер органдарының құқық қолдану қызметі саласындағы қазіргі заманғы сын-қатерлер қаралады. Киберқылмысқа қарсы іс-қимыл, жедел-іздестіру қызметін жетілдіру, цифрлық дәлелдемелерге жол беруді қамтамасыз ету, халықаралық ынтымақтастық және жедел бақылаудың қазіргі заманғы технологияларын пайдалану кезінде азаматтардың конституциялық құқықтарын сақтау проблемалары зерттелуде. Ішкі істер органдарының құқық қолдану тәжірибесін талдауға, интернет-алаяқтықты тергеу проблемаларына, қылмыстық қызметте криптографияларды және анонимдеу технологияларын пайдалануға ерекше назар аударылды. IP-телефония, VPN-сервистер, мессенджерлер және таратылған цифрлық платформалар арқылы жасалатын трансұлттық қылмыстарды анықтау және тергеу проблемалары талданады. Жеке өмірге қол сұғылмаушылық құқығын, дербес деректерді қорғауды және азаматтардың конституциялық құқықтарын шектеуді соттық бақылауды қоса алғанда, құқық қорғау қызметінің тиімділігі мен адам құқықтарын қорғау арасындағы теңгерімді қамтамасыз ету мәселелеріне ерекше назар аударылды. Киберполиция бөлімшелерін кадрлық қамтамасыз ету проблемалары, ішкі істер органдары қызметкерлерінің біліктілігін арттыру және цифрлық криминалистика мен ақпараттық қауіпсіздік саласында қазіргі заманғы білім беру бағдарламаларын енгізу қажеттілігі зерттелуде. Заңнаманы, сот және тергеу практикасын талдау негізінде құқықтық реттеуді жетілдіру, жедел-іздестіру қызметін жаңғырту, халықаралық ынтымақтастықты дамыту және жасанды интеллект, үлкен деректерді талдау және қылмыстарды анықтаудың автоматтандырылған жүйелерін қоса алғанда, қазіргі заманғы цифрлық технологияларды енгізу бойынша ұсыныстар әзірленді.

Қоғам дамуының қазіргі кезеңі қоғамдық қатынастарды белсенді цифрландырумен, ақпараттық-коммуникациялық технологияларды кеңінен енгізумен және цифрлық экономиканың қарқынды дамуымен сипатталады. Электрондық сервистерді, қашықтықтан банктік жүйелерді, мобильді қосымшалар мен интернет-коммуникацияларды пайдалану күнделікті өмірдің ажырамас бөлігіне айналды. Сонымен бірге көрсетілген процестер қоғамдық қауіпсіздікке жаңа қатерлердің туындауына ықпал етті және қылмыстың жай-күйіне елеулі түрде әсер етті.

Қазіргі заманғы қылмыс цифрлық ортаға белсенді бейімделуде. Қылмыстық топтар құқыққа қарсы әрекеттер жасау, қылмыс іздерін жасыру, қызметті үйлестіру және ақша қаражатын заңдастыру үшін ақпараттық технологияларды пайдаланады. Интернет-алаяқтық, ақпараттық жүйелерге заңсыз қол жеткізу, дербес деректерді ұрлау, зиянды бағдарламалық қамтамасыз етуді тарату және қылмыстық қызметте криптовалюталарды пайдалану ерекше қауіп төндіреді. Осындай жағдайларда Қазақстан Республикасының ішкі істер органдары құқық қолдану қызметін жетілдіруді, заңнаманы жаңғыртуды және құқық қорғау органдарының қызметіне қазіргі заманғы цифрлық технологияларды енгізуді талап ететін принципті жаңа сын-қатерлерге тап болады.

Қазіргі заманғы құқық қорғау жүйесінің ең маңызды проблемаларының бірі ақпараттық-коммуникациялық технологияларды пайдалану арқылы жасалатын қылмыстардың өсуі болып табылады [1]. Соңғы жылдары телефон қоңыраулары, интернет-платформалар, әлеуметтік желілер және мессенджерлер арқылы жасалатын интернет-алаяқтық санының тұрақты өсуі байқалады. Қылмыскерлер өздерін банктердің, құқық қорғау органдарының және мемлекеттік мекемелердің қызметкерлері ретінде көрсете отырып, әлеуметтік инженерия әдістерін белсенді пайдаланады.

Тәжірибе көрсеткендей, мұндай қылмыстардың едәуір бөлігі қашықтан жасалады және трансұлттық сипатта болады. VPN-сервистерді, IP-телефонияны, шетелдік серверлер мен криптовалюталарды пайдалану құқық қорғау органдарының қылмыс жасауға қатысы бар адамдарды анықтау жөніндегі қызметін айтарлықтай қиындатады.

Мәселен, 2025 жылы Қазақстан Республикасы ІІМ киберполиция бөлімшелері абоненттік нөмірлерді ауыстыру және IP-телефонияны пайдалану арқылы телефон алаяқтығын жүзеге асырған ұйымдасқан топтың қызметіне тосқауыл қойды [2]. Қылмыскерлер өздерін банктер мен құқық қорғау органдарының қызметкерлері ретінде танытып, азаматтарды «қауіпсіз шоттарға» ақша аударуға көндірді. Құқыққа қарсы әрекет нәтижесінде жәбірленушілерге аса ірі көлемде залал келтірілген.

Қылмыстық істі тергеу шетелдік цифрлық инфрақұрылым мен бөлінген желілік сервистерді пайдаланумен қиындай түсті. Қылмыстық схемаға қатысушыларды анықтау үшін шет мемлекеттердің құқық қорғау органдарымен халықаралық өзара іс-қимыл жасау, компьютерлік-техникалық сараптамалар жүргізу және күдіктілердің желілік белсенділігін талдау қажет болды. Көрсетілген мысал халықаралық ынтымақтастық тетіктерін және қылмыстарды тергеудің цифрлық әдістерін одан әрі жетілдіру қажеттігін куәландырады.

Ішкі істер органдары үшін маңызды сын-қатер жедел-іздестіру қызметін қылмысты цифрландыру шарттарына бейімдеу қажеттілігі болып табылады [3]. Қазақстан Республикасының жедел-іздестіру қызметі саласындағы қолданыстағы заңнамасы көбінесе қылмыстың дәстүрлі нысандарына қарсы іс-қимылға бағдарланған. Сонымен бірге қазіргі криминалдық орта қылмыстардың цифрлық іздерін анықтау мен тіркеудің жаңа тетіктерін талап етеді.

Дәлелді ақпараттың едәуір бөлігі қазіргі уақытта электрондық деректер нысанында бар: желілік журналдар, метадеректер, электрондық хабарламалар, сандық файлдар және ақпараттық-телекоммуникациялық желілерде орналастырылған өзге де ақпарат [4]. Осындай мәліметтерді алу және талдау үшін арнайы техникалық құралдар, заманауи бағдарламалық кешендер және нақты құқықтық реттеу қажет.

Іс жүзінде ішкі істер органдары цифрлық дәлелдемелерді процессуалдық заңдастыру проблемаларымен бетпе-бет келеді [5]. Бірқатар қылмыстық істерде қорғаушы тарап электрондық дәлелдемелерді алу, көшіру және сақтау тәртібінің бұзылуын көрсете отырып, оларға жол беруге болатынын даулайды. Сот практикасы цифрлық жеткізгіштерді алып қою және электрондық ақпаратты

тіркеу кезінде іс жүргізу талаптарын сақтамау дәлелдемелерді жарамсыз деп тануға әкеп соғуы мүмкін екенін көрсетеді.

Ақпараттық-телекоммуникациялық желілерде жасалатын қылмыстарды тергеу ерекше қиындық туғызады. Дәстүрлі қылмыстарға қарағанда, киберқылмыстар аумақтық шекаралардың жоқтығымен және құқыққа қарсы әрекеттерді қашықтықтан жасау мүмкіндігімен сипатталады [6]. Қылмыскерлер анонимдеу технологиясын, шифрланған байланыс арналарын және таратылған серверлік инфрақұрылымдарды пайдаланады, бұл құқық қорғау органдарының қызметін айтарлықтай қиындатады.

Бұдан басқа, қазіргі жағдайда қылмыстық қызметте криптовалюталардың рөлі артады. Криптовалюталық платформалар ақша қаражатын заңдастыру, есірткі құралдарының заңсыз айналымы, қылмыстық қызметті қаржыландыру және қаржылық операцияларды жасыру үшін пайдаланылады [7]. Осындай қылмыстарды тергеу кезінде құқық қорғау органдары цифрлық активтердің иелерін анықтау және ақша қаражатының қозғалысын қадағалау проблемасына тап болады.

Қылмыстық істерді тергеу тәжірибесі көрсеткендей, криптовалюталық транзакциялар туралы ақпаратты алу көбінесе халықаралық өзара іс-қимылды және цифрлық криминалистика саласындағы мамандарды тартуды талап етеді [8]. Алайда цифрлық деректермен жедел алмасудың бірыңғай халықаралық тетіктерінің болмауы осындай қылмыстарды тергеуді айтарлықтай қиындатады.

Құқық қорғау қызметінің тиімділігі мен адам мен азаматтың конституциялық құқықтары мен бостандықтарын сақтау арасындағы теңгерімді қамтамасыз ету қазіргі заманғы құқық қолдану қызметінің маңызды бағыты болып табылады. Жедел бақылаудың қазіргі заманғы технологияларын пайдалану құқық қорғау органдарына азаматтардың цифрлық ортадағы қызметі туралы айтарлықтай көлемде ақпарат алуға мүмкіндік береді. Сонымен қатар, мемлекеттің техникалық мүмкіндіктерін кеңейту сөзсіз жеке өмірге қол сұғылмаушылық, хат алмасу құпиясы және дербес деректерді қорғау мәселелерін қозғайды [9].

Бірқатар қылмыстық істерде қорғаушы тарап күдіктілердің желілік белсенділігі туралы ақпаратты алудың заңдылығын даулап, жедел бақылаудың жекелеген іс-шараларын жүргізуге сот рұқсатының жоқтығын көрсетті. Сот практикасы азаматтардың конституциялық құқықтарын шектеу кезінде заңдылық, мөлшерлестік және негізділік қағидаттарын қатаң сақтау қажеттігін куәландырады.

Осылайша, құқық қорғау қызметін жаңғырту сот және прокурорлық бақылау тетіктерін дамытумен, адам құқықтарын қорғау кепілдіктерін күшейтумен және дербес деректер туралы заңнаманы жетілдірумен қатар жүруі тиіс.

Ішкі істер органдары үшін негізгі сын-қатерлердің бірі ақпараттық-коммуникациялық технологияларды пайдалану арқылы жасалатын қылмыстарды тергеу саласындағы білікті кадрлардың тапшылығы болып қалуда [10]. Қазіргі заманғы киберқылмыстар ақпараттық қауіпсіздік, цифрлық

криминалистика, үлкен деректерді талдау және компьютерлік-техникалық сараптама саласында арнайы білімнің болуын талап етеді.

Тәжірибе көрсетіп отырғандай, сандық ортадағы күрделі қылмыстарды тергеу көбінесе ақпараттық қауіпсіздік саласындағы IT-мамандар мен сарапшыларды тартуды талап етеді [11]. Бұл киберполицияның мамандандырылған бөлімшелерін одан әрі дамыту және ішкі істер органдарының қызметкерлерін даярлау жүйесін жетілдіру қажеттігін куәландырады.

Бұдан басқа, технологиялардың қарқынды дамуы құқық қорғау органдары қызметкерлерінің біліктілігін ұдайы арттыруды талап етеді. Цифрлық криминалистиканы, желілік белсенділікті талдау әдістерін және цифрлық ортадағы қылмыстарды тергеу ерекшеліктерін зерделеуге бағытталған қазіргі заманғы білім беру бағдарламаларын енгізу ерекше маңызға ие болады.

Қазіргі заманғы сын-қатерлер Қазақстан Республикасы ішкі істер органдарының құқық қолдану қызметін кешенді жетілдіруді талап етеді. Бірінші кезекте цифрлық ортада жедел-іздестіру қызметін құқықтық реттеуді одан әрі дамыту, электрондық дәлелдемелермен жұмыс істеудің іс жүргізу тәртібін бекіту және халықаралық ынтымақтастық тетіктерін жетілдіру қажет.

Ішкі істер органдары үлкен деректерді талдау жүйелерін, жасанды интеллект технологияларын, қылмыстарды анықтаудың автоматтандырылған жүйелері мен сандық криминалистиканы қоса алғанда, қазіргі заманғы сандық технологияларды белсенді пайдалануы тиіс. Мұндай технологияларды пайдалану ақпараттық-коммуникациялық технологияларды пайдалана отырып жасалатын қылмыстарды анықтау мен тергеудің тиімділігін арттыруға мүмкіндік береді.

Сонымен бір мезгілде адамның және азаматтың конституциялық құқықтары мен бостандықтарының сақталуын, дербес деректердің қорғалуын және құқық қорғау органдарының қызметіне тиімді сот бақылауын қамтамасыз ету қажет. Құқық қорғау жүйесін жаңғырту заңдылық, мөлшерлестік және адам құқықтарын құрметтеу қағидаттары негізінде жүзеге асырылуға тиіс.

Осылайша, ішкі істер органдарының қазіргі заманғы құқық қолдану қызметі елеулі технологиялық және ұйымдастырушылық сын-қатерлер жағдайында жүзеге асырылады. Қоғамды цифрландыру және қылмысты трансформациялау құқық қорғау органдарының қызметін айтарлықтай қиындатады және заңнаманы кешенді жетілдіруді, қазіргі заманғы технологияларды енгізуді және құқық қорғау органдары қызметкерлерінің кәсіби деңгейін арттыруды талап етеді.

Жедел-іздестіру қызметін жаңғыртусыз, халықаралық ынтымақтастықты дамытусыз және цифрлық ортада қылмысқа қарсы іс-қимылдың қазіргі заманғы тетіктерін қалыптастырусыз қазіргі заманғы қылмысқа қарсы тиімді іс-қимыл жасау мүмкін емес. Демек, Қазақстан Республикасы ішкі істер органдарының қызметін одан әрі жетілдіру қазіргі заманғы технологиялық шындықты, халықаралық тәжірибені және азаматтардың құқықтары мен бостандықтарын сенімді қорғауды қамтамасыз ету қажеттігін ескере отырып жүзеге асырылуға тиіс.

1. **Швыряев П.С.** Проблема киберпреступности в России: актуальное состояние и перспективы решения // https://cyberleninka.ru/article/n/problema-kiberprestupnosti-v-rossii-aktualnoe-sostoyanie-i-perspektivy-resheniya
2. Киберполиция Казахстана в 2025 году ликвидировала за рубежом 7 call-центров // https://www.gov.kz/memleket/entities/qriim/press/news/details/1136438?lang=ru
3. **Шаров В.И.** «Цифровая оперативно-розыскная деятельность» и цифровизация противодействия преступлениям // https://cyberleninka.ru/article/n/tsifrovaya-operativno-rozysknaya-deyatelnost-i-tsifrovizatsiya-protivodeystviya-prestupleniyam
4. **Дмитриева А.А.** Концепция электронного доказательства в уголовном судопроизводстве // https://cyberleninka.ru/article/n/kontseptsiya-elektronnogo-dokazatelstva-v-ugolovnom-sudoproizvodstve
5. **Валитова В.И.** Проблема применения «электронных» доказательств в уголовном процессе // https://cyberleninka.ru/article/n/problema-primeneniya-elektronnyh-dokazatelstv-v-ugolovnom-protsesse
6. **Баймагамбетов Т.М.** Киберпреступность: некоторые виды преступлений, как следствие глобального роста объема информации // https://cyberleninka.ru/article/n/kiberprestupnost-nekotorye-vidy-prestupleniy-kak-sledstvie-globalnogo-rosta-obema-informatsii
7. **Миронов А.О.** Роль криптовалют в совершении преступлений террористической и экстремисткой направленности в современных условиях // https://cyberleninka.ru/article/n/rol-kriptovalyut-v-sovershenii-prestupleniy-terroristicheskoy-i-ekstremistkoy-napravlennosti-v-sovremennyh-usloviyah
8. **Пушкарев В.В.** Преступления с использованием криптовалюты: актуальные вопросы уголовного преследования // https://cyberleninka.ru/article/n/prestupleniya-s-ispolzovaniem-kriptovalyuty-aktualnye-voprosy-ugolovnogo-presledovaniya
9. **Иванов В.В.** Защита охраняемых законом тайн при производстве следственных действий с мобильным телефоном и иными электронными носителями информации // https://cyberleninka.ru/article/n/zaschita-ohranyaemyh-zakonom-tayn-pri-proizvodstve-sledstvennyh-deystviy-s-mobilnym-telefonom-i-inymi-elektronnymi-nositelyami
10. **Ивлев П.В.** Преступления в сфере кибербезопасности: новые вызовы // https://cyberleninka.ru/article/n/prestupleniya-v-sfere-kiberbezopasnosti-novye-vyzovy
11. **Нечай А.А.** Особенности подготовки специалистов для расследования преступлений в сфере компьютерной информации // https://cyberleninka.ru/article/n/osobennosti-podgotovki-spetsialistov-dlya-rassledovaniya-prestupleniy-v-sfere-kompyuternoy-informatsii.

НЕВЗАИМОЗАМЕНЯЕМЫЕ ТОКЕНЫ КАК ЭЛЕМЕНТ МЕХАНИЗМА ПРЕДУПРЕЖДЕНИЯ НЕЗАКОННОГО ВЫВОДА ЦИФРОВЫХ АКТИВОВ В РЕСПУБЛИКЕ КАЗАХСТАН

АБУБАКИРОВА Гулнур Муратбековна
Кыргызский Национальный университет имени Ж. Баласагына, г.Бишкек, Кыргызская Республика

В статье исследуются уголовно-правовые аспекты использования невзаимозаменяемых токенов (NFT) в механизме предупреждения незаконного вывода цифровых активов в Республике Казахстан. Рассматриваются правовая природа NFT, особенности их функционирования в цифровой среде и основные риски, связанные с использованием цифровых токенов в схемах легализации преступных доходов. Особое внимание уделяется проблемам анонимности транзакций, трансграничному характеру цифровых операций и недостаточности действующего правового регулирования. Проанализированы современные подходы к финансовому мониторингу цифровых активов и отдельные аспекты правоохранительной практики. На основе проведенного исследования предложены меры по совершенствованию уголовного и цифрового законодательства Республики Казахстан, направленные на повышение эффективности противодействия незаконному выводу цифровых активов и обеспечению финансовой безопасности государства.

Современный этап цифровой трансформации Республики Казахстан сопровождается не только расширением возможностей цифровой экономики, но и формированием новых угроз финансовой безопасности государства. Развитие криптовалютного рынка, рост популярности цифровых активов и внедрение децентрализованных технологий создают условия для появления сложных схем незаконного вывода активов, их сокрытия и последующей легализации через цифровую среду. Особую актуальность данная проблема приобретает в условиях активного развития государственной политики цифровизации. В 2026 году в Республике Казахстан официально объявлен Год цифровизации и искусственного интеллекта, что подтверждает стратегическую значимость цифровых технологий для дальнейшего развития государства [1].

Послание Президента Республики Казахстан Касым-Жомарта Токаева также демонстрирует усиление внимания государства к вопросам цифровой экономики, цифровых активов и обеспечения прозрачности финансовых процессов [2]. В документе отдельно подчеркивается необходимость ускоренного формирования полноценной экосистемы цифровых активов, развития цифрового тенге и совершенствования механизмов противодействия киберпреступности. На этом фоне проблема использования невзаимозаменяемых токенов (с англ. non fungible tokens) (далее - NFT) приобретает не только технологическое, но и уголовно-правовое значение.

NFT представляют собой уникальные цифровые токены, существующие на основе технологии блокчейн и подтверждающие право владения определенным цифровым объектом. Первоначально подобные токены использовались

преимущественно в сфере цифрового искусства и коллекционирования, однако дальнейшее развитие рынка привело к расширению сфер их применения. Сегодня NFT применяются в цифровой торговле, инвестиционной деятельности, игровой индустрии, обороте объектов интеллектуальной собственности и финансовых транзакциях. Одновременно с этим начали формироваться риски использования таких токенов в схемах сокрытия происхождения активов, их анонимного перемещения и легализации преступных доходов [3].

Сложность уголовно-правовой оценки NFT связана с отсутствием устойчивой правоприменительной практики, высокой скоростью транзакций, трансграничным характером цифровых операций и технической сложностью отслеживания движения цифровых активов [4]. В научной литературе уже обращается внимание на использование NFT в схемах легализации преступных доходов через дробление транзакций, применение криптовалютных миксеров, анонимных криптокошельков и P2P-платформ. Дополнительную проблему создает отсутствие единообразного подхода к правовой квалификации подобных активов в уголовном законодательстве и механизмах финансового мониторинга.

Особую значимость теме придает принятие Цифрового кодекса Республики Казахстан, который закрепил основы регулирования цифровой среды, цифровых объектов и цифровых данных [5]. В Кодексе отдельно подчеркиваются принципы безопасности государства при использовании цифровых технологий, необходимость укрепления законности в цифровой среде и обеспечение баланса публичных и частных интересов. В условиях активного развития цифрового оборота именно правоохранительная практика становится ключевым элементом формирования эффективного механизма предупреждения незаконного вывода цифровых активов [6].

Цель статьи заключается в анализе уголовно-правовых аспектов использования невзаимозаменяемых токенов в механизме предупреждения незаконного вывода цифровых активов в Республике Казахстан.

Для достижения поставленной цели были определены следующие задачи:

-рассмотреть правовую природу невзаимозаменяемых токенов и особенности их функционирования в цифровой среде;

-выявить основные риски использования NFT в схемах незаконного вывода и легализации цифровых активов;

-проанализировать перспективы совершенствования механизмов предупреждения незаконного оборота цифровых активов в правоохранительной практике Республики Казахстан.

Объектом статьи выступают общественные отношения, возникающие в сфере предупреждения незаконного вывода цифровых активов с использованием невзаимозаменяемых токенов.

Предмет статьи составляют нормы цифрового, уголовного и финансового законодательства Республики Казахстан, регулирующие оборот цифровых активов, а также правоприменительная практика противодействия преступлениям в цифровой среде.

Статья включает анализ современных подходов к регулированию цифровых активов, оценку рисков использования NFT в преступных схемах и рассмотрение

возможных направлений совершенствования правоохранительных механизмов в условиях цифровизации экономики Казахстана.

Правовая природа NFT и особенности их функционирования в цифровой среде

Развитие цифровой экономики привело к формированию новых объектов имущественных отношений, существующих исключительно в электронной среде. Одним из наиболее технологически сложных и одновременно правово-неопределенных цифровых объектов стали невзаимозаменяемые токены (NFT), получившие широкое распространение в сфере цифровых активов, электронной коммерции и виртуальных платформ. В отличие от традиционных криптовалют, обладающих свойством взаимозаменяемости, NFT представляют собой уникальные цифровые токены, подтверждающие принадлежность конкретного цифрового объекта определенному владельцу [3]. Их уникальность обеспечивается технологией блокчейн, позволяющей фиксировать сведения о происхождении, передаче и текущем статусе цифрового актива в распределенном реестре.

Современное понимание NFT основывается на применении технологии смарт-контрактов, функционирующих преимущественно в сети Ethereum. В научной литературе подчеркивается, что NFT являются криптографически уникальными, неделимыми и верифицируемыми токенами, способными подтверждать право владения как цифровыми, так и физическими объектами. Фактически NFT стали механизмом технологического закрепления дефицита в цифровой среде, где ранее любой цифровой объект мог бесконтрольно копироваться без возможности подтверждения оригинальности [3].

Первоначально NFT использовались преимущественно в сфере цифрового искусства и игровой индустрии. Однако в дальнейшем их применение значительно расширилось. На современном этапе NFT применяются в обороте объектов интеллектуальной собственности, цифровых коллекционных предметов, виртуальной недвижимости, игровых активов, музыкального контента, а также в инвестиционной деятельности. Подобное расширение функционала обусловило возникновение новых уголовно-правовых рисков, связанных с использованием цифровых токенов в схемах незаконного вывода и легализации активов.

Особенностью NFT является высокий уровень анонимности совершаемых операций. Несмотря на открытость блокчейн-технологии, идентификация конечного владельца токена зачастую затруднена ввиду использования анонимных криптовалютных кошельков, децентрализованных платформ и сервисов сокрытия цифровых следов. Указанное обстоятельство существенно осложняет деятельность правоохранительных органов при выявлении источников происхождения цифровых активов и отслеживании цепочек транзакций. Дополнительную проблему создает трансграничный характер цифровых операций, поскольку размещение токенов, хранение цифровых активов и проведение финансовых операций могут осуществляться одновременно в различных юрисдикциях.

В научных исследованиях уже отмечается, что NFT могут использоваться в качестве инструмента легализации преступных доходов посредством искусственного завышения стоимости цифровых объектов, фиктивных сделок купли-продажи и повторного оборота токенов между взаимосвязанными лицами. Подобные механизмы позволяют формально создавать видимость законного происхождения цифровых активов, затрудняя установление их первоначального преступного источника [4].

В условиях Республики Казахстан проблема правового регулирования NFT приобретает особую актуальность на фоне активного развития цифровой среды и формирования государственной политики цифровизации. Принятый Цифровой кодекс Республики Казахстан закрепил основные принципы регулирования общественных отношений в цифровой среде, включая вопросы обращения цифровых объектов и обеспечения безопасности государства при применении цифровых технологий. Вместе с тем действующее законодательство пока не содержит полноценного механизма уголовно-правовой квалификации операций с NFT, что создает определенные сложности для правоприменительной практики [5].

Отсутствие единообразного подхода к определению правового статуса NFT также влияет на эффективность финансового мониторинга. В отличие от традиционных объектов имущественных отношений, NFT обладают высокой волатильностью стоимости и могут использоваться для многократного перемещения активов между различными цифровыми платформами за короткий промежуток времени. При этом операции с цифровыми токенами зачастую осуществляются вне традиционной банковской системы, что снижает возможности государственного контроля за движением цифровых активов [4].

Дополнительную сложность представляет проблема оценки NFT в рамках уголовного судопроизводства. Стоимость токенов может существенно изменяться в зависимости от рыночной конъюнктуры, популярности цифрового объекта или искусственного завышения цены участниками сделки. В результате правоохранительные органы сталкиваются с трудностями при определении размера причиненного ущерба, установлении факта легализации преступных доходов и квалификации противоправных действий.

Таким образом, NFT в современных условиях выступают не только инновационным цифровым инструментом, но и потенциальным объектом противоправного использования в сфере незаконного вывода цифровых активов. Их технологические особенности, высокий уровень анонимности и недостаточная урегулированность в законодательстве создают предпосылки для формирования новых способов сокрытия и легализации преступных доходов. В связи с этим дальнейшее совершенствование уголовно-правовых и криминалистических механизмов противодействия незаконному обороту цифровых активов становится одним из приоритетных направлений развития правоохранительной системы Республики Казахстан [5].

Проведенное исследование показывает, что развитие цифровой экономики и расширение оборота цифровых активов в Республике Казахстан сопровождаются возникновением новых уголовно-правовых рисков, связанных

с незаконным выводом активов, их сокрытием и последующей легализацией через цифровую среду. Особую актуальность данная проблема приобретает в условиях активного внедрения блокчейн-технологий, цифровых платформ и децентрализованных финансовых инструментов, среди которых особое место занимают NFT.

Установлено, что NFT обладают рядом технологических особенностей, существенно отличающих их от традиционных цифровых финансовых инструментов. Уникальность токенов, возможность анонимного перемещения цифровых активов, высокая скорость транзакций и трансграничный характер операций создают благоприятные условия для использования NFT в схемах легализации преступных доходов и незаконного вывода активов. При этом действующее законодательство Республики Казахстан пока не содержит полноценного механизма уголовно-правового регулирования подобных цифровых объектов, что создает трудности для правоохранительной практики и финансового мониторинга.

Анализ научной литературы и зарубежной правоприменительной практики показал, что NFT уже используются в противоправных схемах посредством фиктивных сделок купли-продажи цифровых объектов, искусственного завышения стоимости токенов, применения анонимных криптовалютных кошельков, P2P-платформ и сервисов сокрытия цифровых следов. В условиях недостаточной урегулированности цифрового рынка подобные механизмы существенно осложняют выявление происхождения цифровых активов и установление их связи с преступной деятельностью.

В результате исследования сделан вывод о необходимости дальнейшего совершенствования уголовного и цифрового законодательства Республики Казахстан в части регулирования оборота NFT и иных цифровых активов. Представляется целесообразным закрепление в законодательстве официального определения невзаимозаменяемых токенов как самостоятельного вида цифровых активов с установлением особенностей их оборота, идентификации и финансового контроля.

В целях повышения эффективности противодействия незаконному выводу цифровых активов предлагается внести следующие изменения в законодательство Республики Казахстан:

1. Дополнить Цифровой кодекс Республики Казахстан отдельной нормой, закрепляющей правовой статус NFT, их признаки и особенности обращения в цифровой среде.

2. Закрепить обязанность операторов цифровых платформ и криптовалютных сервисов, осуществляющих операции с NFT, проводить идентификацию пользователей по принципу KYC (с англ. know your customer) с обязательным хранением информации о совершенных транзакциях.

3. Дополнить нормы финансового мониторинга положениями о признании операций с NFT потенциально высокорисковыми при наличии признаков дробления транзакций, искусственного завышения стоимости токенов или многократного оборота цифрового объекта между взаимосвязанными лицами.

4. Внести изменения в Уголовный кодекс Республики Казахстан, предусматривающие возможность признания NFT предметом легализации (отмывания) преступных доходов наряду с иными цифровыми активами.

5. Предусмотреть в уголовно-процессуальном законодательстве механизм временной блокировки, ареста и цифрового отслеживания NFT-токенов в рамках расследования преступлений, связанных с незаконным выводом активов и легализацией преступных доходов.

6. Разработать специализированные методические рекомендации для правоохранительных органов по выявлению преступных схем с использованием NFT, включая анализ блокчейн-транзакций, цифровую идентификацию пользователей и порядок взаимодействия с международными цифровыми платформами.

Таким образом, эффективное предупреждение незаконного вывода цифровых активов в современных условиях невозможно без комплексного совершенствования уголовно-правовых, цифровых и криминалистических механизмов регулирования NFT. Развитие законодательства в данной сфере позволит повысить уровень финансовой безопасности государства, обеспечить прозрачность цифрового оборота и усилить эффективность правоохранительной деятельности в условиях цифровизации Республики Казахстан.

Предлагаемые изменения могут быть использованы при совершенствовании механизмов финансового мониторинга, расследовании преступлений, связанных с цифровыми активами, а также при формировании национальной модели правового регулирования NFT в Республике Казахстан.

---

1. Указ Президента Республики Казахстан № 1151 «Об объявлении Года цифровизации и искусственного интеллекта» от 6 января 2026 года // https://adilet.zan.kz/rus/docs/U2600001151 (дата обращения 01.05.2026г.)

2. **Послание Главы государства Касым-Жомарта Токаева народу Казахстана** «Казахстан в эпоху искусственного интеллекта: актуальные задачи и их решения через цифровую трансформацию» от 8 сентября 2025 года // https://adilet.zan.kz/rus/docs/K25002025_1 (дата обращения 01.05.2026г.)

3. **Valeonti F., Bikakis A., Terras M., Speed C., Hudson-Smith A., Chalkias K.** Crypto Collectibles, Museum Funding and OpenGLAM: Challenges, Opportunities and the Potential of Non-Fungible Tokens (NFTs) // Applied Sciences. – 2021. – Vol. 11, No. 21. – Article 9931. – DOI: 10.3390/app11219931.

4. **Науменко О.А.** Криминалистический анализ отдельных признаков использования NFT-токенов в преступных целях // Вестник Волгоградской академии МВД России. 2023. № 4(67). –С. 150–156.

5. Цифровой Кодекс Республики Казахстан № 255-VIII ЗРК от 9 января 2026 года // https://adilet.zan.kz/rus/docs/K2600000255 (дата обращения 01.05.2026г.)

6. Постановление Правительства Республики Казахстан № 60 «Об утверждении Плана мероприятий по проведению Года цифровизации и искусственного интеллекта» от 31 января 2026 года // https://adilet.zan.kz/rus/docs/P2600000060 (дата обращения 01.05.2026г.).

К ВОПРОСУ О ПОНЯТИЯХ «ОБЪЕКТ» И «ЦИФРОВОЙ ОБЪЕКТ» В ДЕЙСТВУЮЩЕМ ПРАВЕ РЕСПУБЛИКИ КАЗАХСТАН

АСКАРОВ Аслан Аскарович
Академия правоохранительных органов при Генеральной прокуратуре Республики Казахстан, г.Косшы

В статье исследуются теоретико-правовые подходы к определению понятий «объект» и «цифровой объект» в действующем праве Республики Казахстан в условиях цифровизации общественных отношений. Проведен анализ лингвистических, доктринальных и нормативных подходов к пониманию объекта права, а также исследованы особенности формирования категории цифрового объекта в современном законодательстве. Особое внимание уделено положениям Цифрового кодекса Республики Казахстан, закрепляющего цифровой объект как самостоятельный элемент цифровой среды и формирующего основы нового направления правового регулирования цифровых правоотношений.

На основе сравнительно-правового анализа законодательства Европейского Союза, США, Сингапура и ОАЭ выявлены основные тенденции развития правового регулирования цифровых объектов, цифровых активов и виртуальных элементов цифровой экономики. Отдельно рассмотрена технология NFT как пример трансформации традиционного понимания объекта гражданских прав в цифровой среде, а также как форма существования уникального цифрового объекта, обладающего имущественной ценностью и участвующего в цифровом обороте.

Сделан вывод о необходимости дальнейшего совершенствования понятийного аппарата цифрового законодательства Республики Казахстан, разграничения смежных цифровых категорий и формирования самостоятельного правового режима цифровых объектов в условиях развития современной цифровой экономики.

Современный этап развития Республики Казахстан характеризуется стремительной цифровой трансформацией практически всех сфер общественных отношений. Информационные технологии, искусственный интеллект, цифровые платформы, электронные сервисы, цифровые активы и иные технологические решения постепенно становятся не вспомогательным, а базовым элементом государственного управления, экономики и правового регулирования. В Послании Главы государства Касым-Жомарта Токаева народу Казахстана от 8 сентября 2025 года «Казахстан в эпоху искусственного интеллекта: актуальные задачи и их решения через цифровую трансформацию» подчеркивается, что мир вступил в эпоху тотальной цифровизации и искусственного интеллекта, а одной из стратегических задач государства обозначено формирование полноценной цифровой страны [1]. Особое внимание в указанном документе уделено необходимости ускоренного развития цифровой среды, внедрения технологий искусственного интеллекта, цифровых активов, платформенной экономики и принятия Цифрового кодекса Республики Казахстан [1].

Закрепление данных направлений на законодательном уровне стало важным этапом формирования новой модели правового регулирования цифровой среды. Принятый Цифровой кодекс Республики Казахстан от 9 января 2026 года № 255-VIII ЗРК (далее - Цифровой кодекс РК) впервые системно закрепил категорию «цифровой объект» как самостоятельный элемент цифровой среды [2]. В

соответствии со статьей 20 Цифрового кодекса РК цифровой объект определяется как обособленный элемент цифровой среды, созданный, используемый или передаваемый посредством цифровых технологий и позволяющий субъектам цифровой среды осуществлять правомочия владения, пользования либо распоряжения в пределах, установленных законодательством Республики Казахстан [2]. Появление подобной легальной конструкции свидетельствует о постепенном переходе казахстанского законодательства к самостоятельному регулированию цифровых правоотношений, выходящих за рамки традиционного понимания объектов права.

При этом категория «объект» продолжает оставаться одной из ключевых и дискуссионных в юридической науке. Традиционно объект правоотношения связывался преимущественно с материальными благами, вещами и результатами человеческой деятельности. Однако развитие цифровых технологий привело к формированию новых общественных отношений, в рамках которых объект приобретает нематериальный и виртуальный характер.

Особенно отчетливо трансформация категории объекта проявляется в сфере цифровых активов, цифровых данных и распределенных информационных систем. Современные цифровые конструкции уже не могут рассматриваться исключительно через классические категории имущества либо информации, поскольку существуют исключительно в цифровой среде и участвуют в самостоятельном цифровом обороте [2].

Следовательно, развитие цифрового законодательства объективно требует переосмысления самой категории объекта в праве. В условиях цифровизации общественных отношений возникает необходимость определения соотношения понятий «объект» и «цифровой объект», выявления их общих и отличительных признаков, а также определения места цифрового объекта в системе объектов права Республики Казахстан. Отсутствие четких научных и законодательных критериев способно привести к неоднозначности правоприменительной практики, противоречиям в квалификации цифровых правоотношений и проблемам правовой защиты участников цифровой среды.

Отдельного внимания заслуживает вопрос юридической терминологии. В казахстанской правовой системе проблема разграничения близких по содержанию правовых категорий уже становилась предметом научной дискуссии. В частности, Р.А. Медиев в статье «К вопросу о различии терминологии «тайные» и «негласные» в действующем праве РК» обращает внимание на отсутствие единообразия в использовании юридических терминов и указывает, что недостаточная определенность понятийного аппарата способна негативно отражаться на правоприменении [3]. Подобный подход имеет принципиальное значение и применительно к категориям «объект» и «цифровой объект», поскольку формирование нового цифрового законодательства невозможно без внутренне согласованной и логически выстроенной терминологической системы.

Несмотря на активное развитие цифрового законодательства, в отечественной юридической науке до настоящего времени отсутствует комплексное теоретико-правовое разграничение понятий «объект» и «цифровой

объект». Значительная часть научных публикаций посвящена вопросам цифровизации экономики, оборота цифровых активов, информационной безопасности либо регулирования искусственного интеллекта, однако сама категория цифрового объекта чаще рассматривается фрагментарно и без системного анализа ее правовой природы. Недостаточная разработанность данной проблематики формирует научный пробел как на уровне правовой теории, так и в сфере практического применения законодательства Республики Казахстан.

Цель настоящей статьи заключается в комплексном анализе понятий «объект» и «цифровой объект» в действующем праве Республики Казахстан, выявлении особенностей их правовой природы, определении соотношения указанных категорий, а также формировании теоретических подходов к совершенствованию понятийного аппарата цифрового законодательства Республики Казахстан.

Материалы и методы. Методологическую основу исследования составили общенаучные и специальные методы научного познания, включая формально-юридический, сравнительно-правовой, системно-структурный, логико-правовой и сравнительно-доктринальный методы. В ходе исследования использованы нормы действующего законодательства Республики Казахстан, международные нормативные акты, научные труды отечественных и зарубежных ученых, а также материалы, посвященные правовому регулированию цифровых объектов и NFT-технологий.

Проведенный анализ действующего законодательства Республики Казахстан, научной литературы, толковых словарей русского языка, а также зарубежных подходов к регулированию цифровой среды позволяет сделать вывод о том, что категория «цифровой объект» постепенно трансформируется в самостоятельный элемент современной правовой системы. Вместе с тем в юридической доктрине и законодательстве до настоящего времени сохраняется неоднозначность как в понимании категории «объект», так и в определении сущности цифрового объекта.

Первоначально понятие объекта формировалось преимущественно в философском и лингвистическом значении. В толковом словаре русского языка С.И. Ожегова термин объект определяется как явление, предмет или лицо, на которое направлена определенная деятельность, внимание либо воздействие [4]. В словаре Д.Н. Ушакова объект рассматривается как предмет внешнего мира, существующий независимо от сознания человека и выступающий предметом познания либо деятельности [5]. В.И. Даль связывал понятие объекта с тем, на что направлено действие или мысль субъекта [6].

Проведенный анализ показывает, что во всех приведенных подходах ключевым признаком объекта выступает его направленность на восприятие, воздействие, регулирование либо использование со стороны субъекта. Однако классическое понимание объекта исторически формировалось преимущественно через материальные категории. В условиях цифровизации подобный подход уже не позволяет в полной мере охватить современные формы общественных отношений.

В юридической науке понятие объекта традиционно рассматривалось через категорию объекта правоотношения. Так, С.С. Алексеев определял объект правоотношения как то, по поводу чего складываются субъективные права и юридические обязанности [7]. О.С. Иоффе связывал объект правоотношения с материальными и нематериальными благами, на достижение либо использование которых направлено поведение субъектов [8]. Ю.К. Толстой отмечал, что объектом правоотношения может выступать не только вещь, но и результат интеллектуальной деятельности, информация либо иное нематериальное благо [9].

Анализ данных подходов позволяет установить, что развитие права постепенно расширяло содержание категории объекта от исключительно материального понимания к более сложным нематериальным конструкциям. Особенно активно данный процесс начал проявляться с развитием цифровых технологий, платформенной экономики и распределенных информационных систем.

Существенные изменения в понимании объекта произошли после формирования цифровой среды как самостоятельного пространства общественных отношений. Цифровые данные, цифровые активы, токенизированные ресурсы, программное обеспечение, виртуальные платформы и распределенные реестры фактически стали участвовать в гражданском обороте, выступать предметом имущественных прав и объектом правовой защиты. Вследствие этого возникла необходимость законодательного закрепления новой категории - цифрового объекта.

Результаты анализа действующего законодательства Республики Казахстан показывают, что наиболее системное закрепление данной категории содержится в Цифровом кодексе Республики Казахстан от 9 января 2026 года № 255-VIII ЗРК. В соответствии со статьей 20 Кодекса цифровой объект определяется как обособленный элемент цифровой среды, созданный, используемый или передаваемый посредством цифровых технологий, обладающий уникальными цифровыми характеристиками и позволяющий субъектам цифровой среды осуществлять правомочия владения, пользования либо распоряжения [2].

Принципиально важным является то обстоятельство, что законодатель впервые выделяет цифровой объект как самостоятельный объект цифровой среды, а не как разновидность информации либо исключительно технический элемент. Более того, Цифровой кодекс РК закрепляет широкий перечень видов цифровых объектов, к которым отнесены цифровые записи, цифровые активы, цифровые ресурсы, программное обеспечение, цифровые платформы, цифровые системы и объекты цифровой инфраструктуры [2].

Полученные результаты позволяют сделать вывод о том, что казахстанское законодательство постепенно переходит от фрагментарного регулирования цифровых технологий к формированию самостоятельной отрасли цифрового права. При этом категория цифрового объекта становится системообразующим элементом данной конструкции.

Анализ зарубежного законодательства показывает отсутствие единого подхода к определению цифрового объекта. Однако большинство современных

правовых систем постепенно расширяют регулирование цифровых активов, виртуальных объектов и иных элементов цифровой экономики. Наиболее показательной в данном контексте является европейская модель, в рамках которой понимание цифрового объекта формируется через категории цифровых услуг, виртуальных активов и электронных ресурсов [10].

В Соединенных Штатах Америки единое законодательное определение цифрового объекта отсутствует. Американская правовая модель строится преимущественно через регулирование цифровых активов, интеллектуальной собственности и электронных данных. При этом в судебной практике цифровые активы все чаще рассматриваются как имущество, обладающее самостоятельной имущественной ценностью [11].

В законодательстве Сингапура и Объединенных Арабских Эмиратов наблюдается более технологически ориентированный подход. В данных государствах цифровые активы и виртуальные объекты рассматриваются как самостоятельные элементы цифровой экономики, подлежащие специальному регулированию. Особое внимание уделяется токенизированным активам, блокчейн-системам и цифровым платформам [12].

Отдельного внимания заслуживает опыт Европейского Союза в сфере регулирования криптоактивов. Принятый регламент MiCA фактически закрепляет самостоятельный правовой режим цифровых активов, обладающих признаками имущественной ценности и участвующих в цифровом обороте [13]. Несмотря на отсутствие прямого термина «цифровой объект», содержание данного регулирования фактически формирует правовую основу для признания цифровых конструкций самостоятельными объектами права.

Результаты сравнительно-правового анализа представлены в таблице 1.

Таблица 1 Подходы к определению цифрового объекта в зарубежных правовых системах

Государство	Основной подход	Особенности регулирования
Республика Казахстан	Цифровой объект закреплен законодательно	Системное определение цифрового объекта и его видов в Цифровом кодексе
Европейский союз	Регулирование цифровых услуг и цифровых активов	Акцент на цифровых платформах и криптоактивах
США	Регулирование цифровых активов и электронных данных	Отсутствие единого понятия цифрового объекта
Сингапур	Технологический подход	Развитое регулирование токенизированных активов
ОАЭ	Специальное регулирование виртуальных активов	Формирование самостоятельного режима цифровых активов

Источник – составлено автором на основе Цифрового кодекса Республики Казахстан [2], Regulation (EU) 2022/2065 (Digital Services Act) [10], Regulation (EU) 2023/1114 (MiCA) [13], а также научных трудов Fairfield J. [11] и Low G. [12].

Проведенный анализ позволяет установить несколько ключевых закономерностей.

Во-первых, во всех современных правовых системах наблюдается постепенное расширение содержания категории объекта за пределы исключительно материального понимания.

Во-вторых, цифровой объект постепенно приобретает признаки самостоятельной правовой категории, обладающей собственными характеристиками, особенностями оборота и механизмами правовой защиты.

В-третьих, законодательство Республики Казахстан в настоящее время демонстрирует один из наиболее системных подходов к нормативному закреплению цифрового объекта среди государств постсоветского пространства.

В-четвертых, дальнейшее развитие цифрового законодательства неизбежно потребует более четкого разграничения понятий «объект», «цифровой объект», «цифровой актив», «цифровая запись» и «цифровые данные», поскольку их смешение способно привести к противоречиям правоприменительной практики.

Отдельно следует отметить, что цифровой объект обладает рядом признаков, отличающих его от традиционного объекта права. К числу таких признаков относятся нематериальный характер, технологическая зависимость, возможность распределенного существования, трансграничность цифрового оборота, наличие уникальных цифровых идентификаторов, а также способность функционировать в рамках автоматизированных систем без непосредственного участия человека.

В результате проведенного анализа сформулирован вывод о том, что цифровой объект представляет собой не только разновидность информации либо технический элемент цифровой среды, а самостоятельную правовую категорию, формирующую основу современного цифрового законодательства Республики Казахстан.

Обозначенные результаты приобретают особую практическую значимость в условиях стремительного развития технологий распределенного реестра, токенизированных активов и виртуального цифрового оборота. Наиболее показательной иллюстрацией трансформации традиционного понимания объекта права в цифровой среде выступает технология NFT (Non-Fungible Token), позволяющая удостоверять уникальность, принадлежность и оборот цифровых объектов посредством блокчейн-инфраструктуры.

Проведенный анализ показывает, что NFT выступают одной из наиболее показательных форм трансформации традиционного понимания объекта права в условиях цифровой среды. Если ранее объект преимущественно связывался с материальными вещами либо результатами интеллектуальной деятельности, то NFT фактически сформировали новую модель существования объекта, при которой юридически значимой становится уникальная цифровая запись, подтверждающая принадлежность определенного актива конкретному субъекту.

С технологической точки зрения NFT представляют собой незаменимые токены, функционирующие в блокчейн-среде и подтверждающие уникальность, происхождение и принадлежность определенного цифрового либо материального актива [14]. В отличие от криптовалют, обладающих свойством взаимозаменяемости, NFT являются индивидуализированными цифровыми

объектами, каждый из которых имеет уникальный идентификатор и самостоятельную историю оборота [14]. Именно данный признак позволяет рассматривать NFT как самостоятельный цифровой объект, обладающий признаками индивидуальной определенности.

Проведенное исследование позволяет рассматривать NFT как пример практической реализации категории цифрового объекта, закрепленной в Цифровом кодексе Республики Казахстан. В соответствии со статьей 20 Цифрового кодекса Республики Казахстан цифровой объект представляет собой обособленный элемент цифровой среды, обладающий уникальными цифровыми характеристиками и позволяющий субъектам осуществлять правомочия владения, пользования и распоряжения [2]. NFT полностью соответствуют указанным признакам, поскольку существуют исключительно в цифровой среде, имеют уникальную цифровую идентификацию и участвуют в цифровом обороте.

Особый интерес представляет соотношение NFT и традиционных объектов гражданских прав. NFT не всегда следует рассматривать исключительно как разновидность цифрового актива либо цифровой записи, поскольку в ряде случаев они выполняют функцию цифрового удостоверения прав на иной объект. Наиболее отчетливо это проявляется при токенизации произведений искусства, игровых активов и виртуальной недвижимости.

В современной юридической доктрине NFT все чаще рассматриваются в качестве самостоятельного объекта гражданских прав. При этом особенность NFT заключается в том, что данный цифровой объект не является результатом интеллектуальной деятельности сам по себе, даже если удостоверяет права на определенный объект интеллектуальной собственности. Как справедливо отмечает К.А. Суворова, NFT представляет собой уникальный цифровой сертификат, подтверждающий принадлежность определенного цифрового актива, однако приобретение NFT не всегда означает переход исключительных прав на связанный с ним объект интеллектуальной собственности [15].

Указанный подход имеет принципиальное значение и для казахстанского законодательства. С позиции теории гражданского права NFT целесообразно рассматривать не как вещь в классическом понимании, а как разновидность иного имущества либо цифрового объекта, существующего исключительно в цифровой среде. При этом ключевым признаком NFT выступает его невзаимозаменяемость, отличающая его как от цифровой валюты, так и от большинства иных цифровых активов [15].

Представляется, что в условиях развития цифрового законодательства Республики Казахстан NFT могут быть включены в систему объектов гражданских прав как самостоятельная разновидность цифровых объектов, обладающих имущественной ценностью, уникальной цифровой идентификацией и способностью участвовать в гражданском обороте.

В зарубежной практике отсутствует единый подход к определению NFT. В одних правопорядках NFT рассматриваются как разновидность цифровых активов, в других - как технологический механизм подтверждения прав на цифровой либо материальный объект. Для Республики Казахстан данная

проблема приобретает особую актуальность после принятия Цифрового кодекса Республики Казахстан.

Отсутствие четкого правового регулирования NFT способно привести к спорам относительно объема передаваемых имущественных и исключительных прав, а также порядка использования цифрового контента.

NFT обладают имущественной ценностью и способны участвовать в гражданском обороте, что позволяет рассматривать их в качестве самостоятельного цифрового объекта. Одновременно NFT существуют исключительно в цифровой среде, что отличает их от классических объектов гражданских прав.

В связи с этим дальнейшее развитие законодательства Республики Казахстан потребует нормативного определения правового режима NFT и их места в системе объектов гражданских прав.

Проведенное исследование позволяет сделать вывод о том, что развитие цифровых технологий и формирование цифровой среды обусловили существенную трансформацию традиционного понимания объекта в современном праве. Если классическая юридическая доктрина преимущественно связывала объект правоотношения с материальными благами, вещами либо результатами человеческой деятельности, то современный этап цифровизации общественных отношений привел к формированию новых разновидностей объектов, существующих исключительно в цифровом пространстве.

Анализ действующего законодательства Республики Казахстан показал, что принятие Цифрового кодекса Республики Казахстан стало важным этапом формирования самостоятельной системы правового регулирования цифровой среды. Закрепление категории «цифровой объект» свидетельствует о постепенном переходе национального законодательства к признанию цифровых конструкций самостоятельными объектами права, обладающими собственными признаками, особенностями оборота и механизмами правовой защиты.

Отдельного внимания заслуживает технология NFT, которая в настоящее время выступает наиболее наглядным примером трансформации категории объекта в условиях цифровой среды. Проведенный анализ показал, что NFT обладают признаками самостоятельного цифрового объекта, поскольку существуют исключительно в цифровой форме, имеют уникальную цифровую идентификацию, участвуют в гражданском обороте и обладают имущественной ценностью. При этом NFT не всегда следует рассматривать как объект интеллектуальной собственности, поскольку в большинстве случаев токен выступает способом подтверждения либо фиксации прав на иной цифровой актив.

С позиции современной теории гражданского права NFT целесообразно рассматривать как разновидность цифрового объекта либо иного имущества, существующего в цифровой среде и обладающего признаками невзаимозаменяемости. Указанный подход имеет существенное значение для дальнейшего развития цифрового законодательства Республики Казахстан, поскольку позволяет определить место NFT в системе объектов гражданских прав.

В результате исследования установлено, что дальнейшее развитие цифрового законодательства Республики Казахстан потребует более четкого разграничения понятий «объект», «цифровой объект», «цифровой актив», «цифровая запись» и «NFT». Отсутствие единообразного понятийного аппарата способно привести к противоречиям правоприменительной практики и осложнить формирование устойчивого механизма регулирования цифровых правоотношений.

Представляется, что перспективным направлением совершенствования законодательства Республики Казахстан является формирование самостоятельного правового режима цифровых объектов, включая определение правовой природы NFT, особенностей их оборота, объема имущественных прав участников цифровой среды, а также механизмов защиты цифровых прав в условиях развития технологий искусственного интеллекта и цифровой экономики.

1.Указ Президента Республики Казахстан № 1042 О мерах по реализации Послания Главы государства народу Казахстана от 8 сентября 2025 года «Казахстан в эпоху искусственного интеллекта: актуальные задачи и их решения через цифровую трансформацию» от 13 октября 2025 года. [Электронный ресурс] - Режим доступа: https://adilet.zan.kz/rus/docs/U2500001042
2.Цифровой кодекс Республики Казахстан № 255-VIII ЗРК от 9 января 2026 года. [Электронный ресурс] - Режим доступа: https://adilet.zan.kz/rus/docs/K2600000255
3.**Медиев Р.А.** К вопросу о различии терминологии «тайные» и «негласные» в действующем праве РК // Труды Карагандинской академии МВД РК имени Б. Бейсенова. — 2013. — С. 110–112.
4.**Ожегов С.И., Шведова Н.Ю.** Толковый словарь русского языка. — М. Азбуковник, 2000. — 944 с.
5.**Ушаков Д.Н.** Толковый словарь русского языка. — М. Астрель, 2008. — 1056 с.
6.**Даль В.И.** Толковый словарь живого великорусского языка. — М. Эксмо, 2007. — 928 с.
7.**Алексеев С.С.** Общая теория права. В 2 т. Т. 2. — М. Юридическая литература, 1982. — 360 с.
8.**Иоффе О.С.** Правоотношение по советскому гражданскому праву. — Л. Издательство ЛГУ, 1949. — 144 с.
9.**Толстой Ю.К.** К теории правоотношения. — Л. Издательство ЛГУ, 1959. — 88 с.
10.Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services (Digital Services Act).
11.**Fairfield J.** Owned. Property, Privacy, and the New Digital Serfdom. — Cambridge University Press, 2017. — 296 p.
12.**Low G.** Smart Contracts and Digital Assets in Singapore Law // Singapore Academy of Law Journal. — 2021. — Vol. 33. — P. 1–25.
13.Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on Markets in Crypto-assets (MiCA).
14.**Bankov B.** Overview, History and Challenges of the NFT (Non-Fungible Token) Technology // University of Economics – Varna, Bulgaria. — 2022. — P. 119–125.
15.**Суворова К.А.** NFT как объект гражданских прав // Цивилистика от прошлого к современности. — 2022. — С. 1407–1410.

ЦИФРОВИЗАЦИЯ ПРАВОПРИМЕНИТЕЛЬНОЙ ДЕЯТЕЛЬНОСТИ: РИСКИ, ПЕРСПЕКТИВЫ И ТРАНСФОРМАЦИЯ ЮРИДИЧЕСКОЙ ОТВЕТСТВЕННОСТИ В УСЛОВИЯХ ГЛОБАЛЬНЫХ ВЫЗОВОВ

АХМЕТОВ Казбек Раимбекович
Академия КНБ РК, г. Алматы, Казахстан

В статье рассматриваются современные тенденции цифровизации правоприменительной деятельности в Республике Казахстан в условиях глобальной трансформации правовой системы. Анализируются ключевые направления внедрения цифровых технологий в деятельность государственных и правоохранительных органов, включая электронное правосудие, цифровой документооборот и элементы искусственного интеллекта. Особое внимание уделяется проблемам обеспечения информационной безопасности, защиты персональных данных, правового регулирования цифровых доказательств и трансформации юридической ответственности в цифровой среде. Исследуются современные вызовы, связанные с развитием киберпреступности и необходимостью адаптации национального законодательства к новым технологическим реалиям. На основе анализа международного опыта и современных тенденций развития цифрового права предлагаются направления совершенствования правового регулирования и повышения эффективности правоприменительной деятельности в Казахстане.

Современный этап развития общества характеризуется масштабной цифровой трансформацией, затрагивающей практически все сферы государственной и общественной жизни. В условиях глобализации и стремительного развития информационных технологий особую значимость приобретает процесс цифровизации правоприменительной деятельности, оказывающий существенное влияние на функционирование правоохранительной и судебной систем. Республика Казахстан, ориентированная на построение цифрового государства и модернизацию системы государственного управления, активно внедряет цифровые технологии в деятельность государственных органов, включая сферу правосудия и правоохранительной деятельности.

Использование электронного документооборота, автоматизированных информационных систем, технологий искусственного интеллекта и цифровых платформ способствует повышению эффективности правоприменительной деятельности, ускорению процессов рассмотрения дел и улучшению доступа граждан к юридическим услугам. Вместе с тем цифровизация порождает новые правовые риски и вызовы, связанные с обеспечением информационной безопасности, защитой персональных данных, регулированием цифровых доказательств и определением юридической ответственности в цифровой среде.

В современных условиях правовая система сталкивается с необходимостью адаптации к новым технологическим реалиям, поскольку традиционные механизмы правового регулирования не всегда способны эффективно реагировать на быстро меняющиеся формы цифрового взаимодействия и трансформацию общественных отношений. Особую актуальность приобретают вопросы совершенствования законодательства в сфере цифрового права, противодействия киберпреступности и формирования единых подходов к

регулированию использования цифровых технологий в правоприменительной практике.

Целью настоящей статьи является исследование влияния цифровизации на правоприменительную деятельность в Республике Казахстан, а также определение основных рисков, перспектив и направлений трансформации юридической ответственности в условиях глобальных вызовов цифровой эпохи.

Цифровизация юридической сферы представляет собой процесс внедрения информационно-коммуникационных технологий в деятельность государственных, правоохранительных и судебных органов с целью повышения эффективности правового регулирования и совершенствования механизмов правоприменения. В современных условиях цифровизация становится не только инструментом модернизации государственного управления, но и одним из ключевых факторов трансформации всей правовой системы.

В Республике Казахстан цифровая трансформация правоприменительной деятельности осуществляется в рамках государственной политики по развитию цифрового государства и совершенствованию системы оказания государственных услуг. Значительное внимание уделяется внедрению современных информационных технологий в деятельность судебных и правоохранительных органов, что способствует повышению прозрачности, оперативности и доступности правосудия [1].

Одним из важнейших направлений цифровизации является развитие электронного правосудия. Использование электронных сервисов позволяет гражданам подавать заявления и процессуальные документы в онлайн-формате, участвовать в судебных заседаниях дистанционно, а также получать доступ к судебным актам через цифровые платформы. Внедрение электронного судопроизводства способствует сокращению временных затрат, снижению бюрократических процедур и повышению открытости судебной системы.

Не менее важным элементом цифровой трансформации выступает цифровой документооборот. Переход от бумажных носителей к электронным системам хранения и обработки информации позволяет существенно повысить скорость обмена данными между государственными органами, минимизировать риск потери документов и обеспечить более эффективный контроль за процессами правоприменительной деятельности. Кроме того, цифровизация документооборота способствует оптимизации административных процедур и снижению коррупционных рисков.

В современных условиях активно развивается автоматизация юридических процедур, связанная с использованием специализированных информационных систем и цифровых алгоритмов. Автоматизация позволяет ускорить обработку юридически значимой информации, систематизировать правовые данные и повысить точность выполнения отдельных процедур. Особенно актуальным данное направление становится в сфере регистрации, учета, анализа правонарушений и обработки больших массивов информации.

Отдельное значение приобретает использование технологий искусственного интеллекта и аналитических систем в деятельности правоохранительных и судебных органов. Аналитические цифровые платформы способны выявлять

закономерности, прогнозировать возможные правонарушения и повышать эффективность анализа доказательственной базы. Вместе с тем внедрение искусственного интеллекта в правоприменительную практику требует разработки четких правовых и этических механизмов регулирования, поскольку автоматизированные решения не должны подменять принцип объективности и человеческого контроля [2].

В целом внедрение цифровых технологий оказывает значительное влияние на эффективность правоприменительной деятельности. Цифровизация способствует ускорению юридических процедур, повышению доступности правосудия, укреплению прозрачности деятельности государственных органов и совершенствованию механизмов взаимодействия государства и общества. Однако одновременно с этим формируются новые правовые риски и вызовы, требующие дальнейшего совершенствования нормативно-правовой базы и адаптации правовой системы к условиям цифровой эпохи.

Несмотря на значительные преимущества цифровизации правоприменительной системы, активное внедрение цифровых технологий сопровождается возникновением новых рисков и угроз, затрагивающих как деятельность государственных органов, так и вопросы обеспечения прав и свобод граждан. В условиях стремительного развития цифровой среды правовая система сталкивается с необходимостью своевременного реагирования на современные вызовы, связанные с информационной безопасностью, защитой данных и трансформацией механизмов правового регулирования.

Одной из наиболее актуальных проблем является рост киберугроз и увеличение количества преступлений, совершаемых с использованием информационных технологий. Развитие цифровой инфраструктуры правоохранительных и судебных органов повышает зависимость государственных систем от устойчивости электронных платформ и каналов передачи данных. Несанкционированный доступ к информационным системам, кибератаки, утечка служебной информации и вмешательство в цифровые базы данных способны нанести существенный ущерб как государственным институтам, так и гражданам. В связи с этим особое значение приобретает обеспечение кибербезопасности и совершенствование механизмов защиты государственных информационных ресурсов.

Серьезным вызовом также выступает проблема защиты персональных данных. В процессе цифровизации правоприменительной деятельности осуществляется обработка значительных объемов конфиденциальной информации, включая персональные сведения граждан, материалы уголовных и административных дел, а также данные, содержащие юридически значимую информацию. Недостаточный уровень защиты цифровых систем может привести к утечке персональных данных, нарушению права на неприкосновенность частной жизни и снижению доверия общества к государственным институтам.

В современных условиях все большую актуальность приобретает проблема алгоритмической предвзятости и ошибок искусственного интеллекта. Использование автоматизированных систем и аналитических алгоритмов в деятельности правоохранительных органов может сопровождаться риском

принятия необъективных решений, основанных на некорректных данных или ошибках программного обеспечения. Искусственный интеллект способен значительно повысить скорость обработки информации, однако он не обладает способностью к полноценной правовой и этической оценке обстоятельств конкретного дела. В связи с этим возникает необходимость сохранения принципа обязательного человеческого контроля при принятии юридически значимых решений.

Дополнительные сложности связаны с правовым регулированием цифровых доказательств. В условиях цифровизации возрастает количество дел, в которых доказательственная база представлена в электронной форме. Вместе с тем действующее законодательство не всегда содержит достаточные механизмы оценки достоверности цифровых доказательств, порядка их хранения, фиксации и использования в судебной практике. Это создает риск возникновения процессуальных ошибок и затрудняет обеспечение принципов объективности и законности при рассмотрении дел.

Отдельного внимания требует проблема транснациональной цифровой преступности. Современные киберпреступления зачастую выходят за пределы юрисдикции одного государства, что существенно осложняет деятельность правоохранительных органов и требует расширения международного сотрудничества в сфере противодействия цифровым угрозам. В условиях глобализации правоприменительная система Казахстана сталкивается с необходимостью адаптации национального законодательства к международным стандартам цифровой безопасности и укрепления взаимодействия с зарубежными государствами в области обмена информацией и совместного расследования киберпреступлений [3].

Развитие цифровых технологий оказывает существенное влияние не только на механизмы правоприменительной деятельности, но и на саму природу юридической ответственности. В условиях цифровизации общественных отношений появляются новые формы противоправного поведения, изменяются способы совершения правонарушений и усложняются механизмы определения субъектов ответственности. В связи с этим традиционные подходы к правовому регулированию требуют адаптации к современным технологическим реалиям.

Одним из наиболее заметных последствий цифровой трансформации стало распространение киберпреступности. Использование цифровых технологий создает условия для совершения мошенничества, незаконного доступа к информационным системам, распространения вредоносного программного обеспечения, кражи персональных данных и иных противоправных действий в виртуальной среде. Особенностью подобных правонарушений является их высокая латентность, сложность выявления и возможность совершения преступлений за пределами территориальной юрисдикции одного государства.

В условиях цифровой среды трансформируется и содержание юридической ответственности. Возникает необходимость разработки новых механизмов регулирования ответственности за распространение цифрового контента, нарушение правил обработки персональных данных, незаконное использование информационных систем и злоупотребление технологиями искусственного

интеллекта. Особую сложность представляет определение степени ответственности при использовании автоматизированных решений, поскольку современные цифровые системы способны самостоятельно выполнять отдельные функции анализа и принятия решений.

Дополнительной проблемой становится вопрос определения субъекта юридической ответственности при использовании технологий искусственного интеллекта. В ситуациях, когда автоматизированная система допускает ошибку или причиняет вред, возникает необходимость установления круга лиц, несущих ответственность за последствия функционирования цифровых алгоритмов. В подобных случаях ответственность может затрагивать разработчиков программного обеспечения, операторов информационных систем, государственных органов либо иных участников цифрового взаимодействия. Однако существующее законодательство не всегда содержит четкие механизмы регулирования подобных правоотношений.

В Республике Казахстан вопросы цифровой безопасности и противодействия киберпреступности постепенно приобретают приоритетное значение. Государством принимаются меры по совершенствованию законодательства в сфере информатизации, защиты персональных данных и обеспечения информационной безопасности. Вместе с тем стремительное развитие технологий требует дальнейшего обновления нормативно-правовой базы, способной эффективно регулировать отношения, возникающие в цифровой среде.

Особую актуальность приобретает необходимость формирования правовых и этических стандартов использования искусственного интеллекта в деятельности государственных органов. Внедрение цифровых технологий должно осуществляться с соблюдением принципов законности, прозрачности, защиты прав человека и недопустимости дискриминации. Автоматизация правоприменительной деятельности не должна приводить к снижению уровня правовых гарантий и ограничению возможностей судебной защиты граждан.

В условиях глобальной цифровой трансформации вопросы совершенствования правоприменительной деятельности приобретают международный характер. Развитие цифровых технологий, рост транснациональной киберпреступности и расширение цифрового взаимодействия между государствами требуют формирования единых подходов к правовому регулированию и укрепления международного сотрудничества в сфере цифрового права и информационной безопасности.

Многие зарубежные государства активно внедряют цифровые технологии в деятельность судебных и правоохранительных органов. В ряде стран функционируют системы электронного правосудия, позволяющие осуществлять дистанционное рассмотрение дел, подачу документов в онлайн-формате и автоматизированную обработку юридически значимой информации. Использование цифровых платформ способствует повышению доступности правосудия, снижению административной нагрузки и ускорению процессов принятия решений. Одновременно с этим зарубежная практика показывает, что эффективная цифровизация невозможна без надежных механизмов защиты

информации и четкого нормативного регулирования использования цифровых технологий.

Особое внимание на международном уровне уделяется вопросам регулирования искусственного интеллекта. В настоящее время многие государства и международные организации разрабатывают правовые и этические стандарты применения технологий искусственного интеллекта в сфере государственного управления и правоприменительной деятельности. Основными принципами такого регулирования выступают обеспечение прозрачности алгоритмов, защита прав человека, недопустимость дискриминации и сохранение человеческого контроля при принятии юридически значимых решений.

Важным направлением международного сотрудничества является противодействие киберпреступности. Современные цифровые угрозы нередко выходят за пределы одной юрисдикции, что требует координации действий правоохранительных органов различных государств. Международный обмен информацией, совместные расследования и унификация правовых механизмов становятся необходимыми условиями эффективной борьбы с преступлениями в цифровой среде. В этой связи особую значимость приобретает адаптация национального законодательства к международным стандартам цифровой безопасности [4].

Для Республики Казахстан изучение международного опыта имеет важное практическое значение. В последние годы в стране реализуются программы цифровизации государственного управления, внедряются электронные государственные услуги и развиваются элементы электронного правосудия. Вместе с тем дальнейшее развитие правовой системы требует совершенствования механизмов правового регулирования цифровой среды, повышения уровня цифровой грамотности специалистов и укрепления системы информационной безопасности.

Перспективы развития правовой системы Казахстана во многом связаны с дальнейшей интеграцией цифровых технологий в деятельность государственных органов и модернизацией юридической науки и образования. Современные реалии требуют подготовки специалистов, обладающих не только правовыми знаниями, но и компетенциями в сфере цифровых технологий, информационной безопасности и анализа данных. Кроме того, возрастает значение научных исследований, направленных на изучение правовых последствий цифровизации и разработку эффективных моделей регулирования цифровых общественных отношений.

В условиях стремительного развития цифровых технологий и трансформации правоприменительной деятельности особую актуальность приобретает необходимость совершенствования механизмов правового регулирования. Эффективное функционирование правовой системы в цифровую эпоху требует не только внедрения современных технологий, но и формирования устойчивой нормативно-правовой базы, способной своевременно реагировать на новые вызовы и угрозы.

Одним из приоритетных направлений является усиление системы информационной и кибербезопасности. В условиях роста количества цифровых угроз государственным органам необходимо совершенствовать механизмы защиты информационных систем, обеспечивать безопасность хранения и передачи данных, а также развивать современные методы противодействия киберпреступности. Особое значение имеет создание эффективной системы межведомственного взаимодействия в сфере обеспечения цифровой безопасности.

Не менее важным направлением выступает совершенствование законодательства в области защиты персональных данных. В процессе цифровизации правоприменительной деятельности государственные органы осуществляют обработку значительных объемов конфиденциальной информации, что требует усиления правовых гарантий защиты частной жизни граждан. В этой связи необходима дальнейшая модернизация национального законодательства с учетом международных стандартов информационной безопасности и цифровых прав человека [5].

Отдельного внимания требует разработка правовых и этических механизмов регулирования использования искусственного интеллекта. Внедрение автоматизированных систем в деятельность правоохранительных и судебных органов должно сопровождаться четким определением пределов использования цифровых алгоритмов и обязательным сохранением человеческого контроля при принятии юридически значимых решений. Кроме того, необходимо установить механизмы юридической ответственности за ошибки и нарушения, возникающие при использовании технологий искусственного интеллекта.

Важным направлением совершенствования правового регулирования является развитие законодательства о цифровых доказательствах. В современных условиях возрастает необходимость создания единых процедур фиксации, хранения, проверки и использования электронной информации в судебной и правоохранительной практике. Законодательное закрепление механизмов работы с цифровыми доказательствами позволит повысить уровень объективности и законности правоприменительной деятельности.

Особую роль играет повышение цифровой компетентности сотрудников правоохранительных, судебных и иных государственных органов. Эффективное использование современных технологий невозможно без подготовки квалифицированных специалистов, обладающих знаниями в области цифрового права, информационной безопасности и аналитических систем. В связи с этим необходимо совершенствовать систему юридического образования и развивать научные исследования в сфере цифровизации правовой системы.

Для Республики Казахстан также важным направлением остается укрепление международного сотрудничества в области цифрового права и противодействия киберпреступности. Современные цифровые угрозы требуют координации действий на международном уровне, обмена информацией и участия в разработке единых правовых стандартов регулирования цифровой среды.

В условиях глобальной цифровой трансформации цифровизация правоприменительной деятельности становится одним из ключевых направлений модернизации правовой системы Республики Казахстан. Внедрение современных информационных технологий в деятельность правоохранительных и судебных органов способствует повышению эффективности правоприменения, ускорению юридических процедур, развитию электронного правосудия и расширению доступа граждан к государственным услугам.

Вместе с тем цифровизация формирует новые правовые риски и вызовы, связанные с обеспечением информационной безопасности, защитой персональных данных, распространением киберпреступности и использованием технологий искусственного интеллекта. Современные условия требуют адаптации национального законодательства к быстро меняющимся цифровым реалиям и выработки эффективных механизмов регулирования общественных отношений в цифровой среде.

Проведенный анализ показывает, что трансформация юридической ответственности в цифровую эпоху обусловлена изменением характера правонарушений, усложнением механизмов определения субъектов ответственности и необходимостью правового регулирования автоматизированных систем. В связи с этим особую значимость приобретает разработка правовых и этических стандартов использования цифровых технологий в деятельности государственных органов.

Изучение международного опыта свидетельствует о том, что успешная цифровизация правоприменительной системы возможна только при сочетании технологического развития, надежной системы кибербезопасности и эффективного нормативно-правового регулирования. Для Республики Казахстан важное значение имеют дальнейшее совершенствование законодательства, развитие цифровой компетентности специалистов и укрепление международного сотрудничества в сфере цифрового права и информационной безопасности.

1. **Susskind R.** Online Courts and the Future of Justice. — Oxford : Oxford University Press, 2019. — 368 p.
2. **Katsh E., Rabinovich-Einy O.** Digital Justice: Technology and the Internet of Disputes. — New York : Oxford University Press, 2017. — 272 p.
3. **Pagallo U.** The Laws of Robots: Crimes, Contracts, and Torts. — Dordrecht : Springer, 2013. — 214 p.
4. OECD Digital Government Index 2023 : Results and Key Findings. — Paris : OECD Publishing, 2023.
5. United Nations E-Government Survey 2024 : Digital Government for Sustainable Development. — New York : United Nations, 2024.

НОВЫЕ СОСТАВЫ В УК РК: ТЕОРЕТИЧЕСКИЕ И ПРАКТИЧЕСКИЕ ПРОБЛЕМЫ ПРОЦЕССА (ДЕ) КРИМИНАЛИЗАЦИИ

ВОЗНЯК Оксана Александровна
НИЕТУЛЛАЕВ Нурлан Нурмухамбетович
Maqsut Narikbayev University г.Астана, Казахстан

Уголовное законодательство долгое время считалось наиболее структурированным, фундаментальным нормативным актом, подвергающимся изменениям в наименьшей степени. Однако, уже в ходе действия УК РК 1997 года отмечалась чрезвычайная активность законодателя по внесению изменений в процессы установления рамок уголовно-правовых деяний и наказуемости, что выразилось в не всегда оправданной практике изменения положений Уголовного кодекса (всего около восьмидесяти актов по изменению и дополнению). Аналогичная ситуация наблюдается и в отношении действующего УК РК 2014 года, который практически за такой же период времени претерпел уже свыше 100 изменений. Авторы, анализируя качество вносимых изменений и дополнений в УК РК, отмечают, что законодатель недостаточно внимания уделяет системному анализу и криминологическому обоснованию предпринимаемых шагов в этом направлении. Косвенным подтверждением такого вывода могут служить процессы обратной криминализации – декриминализации некоторых составов, в отношении которых до сих пор нет четкого понимания «места» в системе репрессивного законодательства. В рамках исследования основное внимание было уделено вопросу необходимости более тщательного обоснования введения в УК тех или иных новых составов или их исключения.

Действующий Уголовный кодекс Казахстана был принят 3 июля 2014 г. и вступил в силу с 1 января 2015 г. Принятие этого уголовного закона с введением в правовое поле категории «уголовный проступок» вызвало ряд вопросов, связанных с разграничением преступного и непреступного, но наказуемого в административном порядке. Следствием разделения уголовных правонарушений на «преступления» и «уголовные проступки», степень общественной опасности административных правонарушений была еще больше искусственно «снижена». На законодательном уровне это выразилось в «повышении» некоторых видов административных правонарушений до уровня уголовных проступков. Наиболее показательным примером подобного подхода выступает перевод мелкого хищения в систему уголовно наказуемых деяний.

Вместе с тем, ряд преступлений небольшой тяжести, наоборот, претерпел искусственное снижение общественной опасности до уровня уголовных проступков: наиболее характерными примерами такого приема законодателя можно отметить составы «Угроза» (ст.115 УК РК), «Умышленное причинение легкого вреда здоровью» (ст.108 УК РК), «Побои» (ст.109 УК РК) *(сведения по первоначальной редакции УК РК от 03.07.2014 г.)*. Из последних примеров появления новых составов уголовных правонарушений можно отметить криминализацию сталкинга (ст.115-1 УК РК) и т.н. «дропперства» (ст.232-1 УК РК). Данные факты свидетельствуют, что отечественный законодатель взял курс на дробление более опасных или более крупных по объему уголовных правонарушений на менее тяжкие составляющие. Частично такой шаг

законодателя вызван общественным резонансом по фактам бытового насилия (это касается составов «Побои» и «Умышленного причинения легкого вреда здоровью»), частично связан с необходимостью реагирования на «новые веяния» в криминальных схемах преступных групп (установление уголовной ответственности за дропперство)[1, С.44-46].

Мы отмечаем необходимость приведения уголовного закона в соответствие с современными вызовами, но следует иметь ввиду, что в некоторых аспектах такие шаги законодателя идут в разрез с законодательной техникой и, собственно, с практикой противодействия преступности. В частности, на примере составов «Умышленное причинение легкого вреда здоровью» и «Побои» можно наблюдать, что бытовое насилие не всегда сопровождается проявлениями признаков данных составов, зачастую в результате семейного конфликта потерпевшему причиняется куда более существенный вред. Установление отдельной уголовной ответственности за дропперство [2] представляет собой «увод» пособничества из структуры преступных групп от более строгой ответственности (до этого такие лица несли ответственность за тяжкое преступление в статусе соучастников, а в современном виде их ответственность ограничивается в рамках практически уголовного проступка).

Данные обстоятельства прямо или косвенно свидетельствуют об отсутствии единого понимания в отношении выстраивания уголовно-правовой политики по отдельным группам уголовных правонарушений, где нельзя отметить логическую последовательность в предпринимаемых шагах законодателя, который готовит проекты о внесении изменений и дополнений в уголовное законодательство, руководствуясь издержками правоприменительной практики.

На сегодняшний день из уголовного закона были декриминализированы более десяти составов уголовных правонарушений. Часть из них была обратно криминализирована по определенным причинам: ст.108-1, 109-1 УК РК (таблица 1) либо переведены в иную главу (например, бывшая ст.197 УК РК перемещена в главу 8 УК РК под номером 233-1). Вместе с тем, УК РК за это же время было криминализировано порядка тридцати новых составов. Помимо этого, имеются и примеры дробления форм общественно опасного деяния внутри уголовно-правовой нормы (так, в рамках ст.146 УК РК, из состава пыток дифференцировано жестокое обращение [3]).

Таблица 1. Динамика изменений позиции законодателя по умышленному причинению легкого вреда и побоям

Составы	Декриминализация	Криминализация	Административное правонарушение
Умышленное причинение легкого вреда здоровью	**18.01.2011 г. (из УК РК 1997 года, ст.105)**		**18.01.2011 г. (ч.2 ст.79-3 КоАП РК**
		03.07.2014 г. (в новом УК, ст.108)	
	03.07.2017 г. (из УК РК 2014 года)		**03.07.2017 г. (73-1 КоАП РК)**

		16.07.2025 г. (ст.108-1 УК РК)	
Побои	**09.12.2004 г. (из УК РК 1997 года, ст.106)**		**09.12.2004 г. (ст.79-1 КоАП РК 2001 года)**
		03.07.2014 г. (в новом УК, ст.109)	
	03.07.2017г. (из УК РК 2014 года)		**03.07.2017 г. (73-2 КоАП РК)**
		16.07.2025 г. (ст.109-1 УК РК)	

Анализ статистических показателей по регистрации дел по новым составам или вновь введенным составам, а также содержательной части уголовных дел показывает, что при должной интерпретации обстоятельств дела у правоприменителя появляется возможность принятия иного решения. Например, незаконное предоставление доступа к банковскому счету и платежным средствам на самом деле может быть выступать основным функционалом участника преступной группы, что должно влечь ответственность по предикатным составам, а не в рамках ст.232-1 УК РК. Аналогичная ситуация и по составам, предусмотренным в ст.ст.217-1, 218-1 УК РК.

Анализ процесса внесения изменений в уголовный закон показывает, что законодатель не всегда соблюдает условие о необходимости криминологического обоснования предпринимаемых шагов, что может привести к неверной правовой оценке степени общественной опасности криминализируемых или исключаемых из уголовного закона деяний. У научного сообщества по данным вопросам есть сомнения в целесообразности введения ответственности по ранним стадиям некоторых общественно опасных деяний, которые имеют в своей основе очень высокий коррупционный риск, в частности, состав т.н. дропперства (ст.232-1 УК РК) может быть некой «буферной» нормой, позволяющей при определенном раскладе «уводить от ответственности» в сторону мягкого реагирования в отношении членов преступных групп, занимающихся мошенничеством, незаконным оборотом наркотических средств, оружия и иными формами запрещенной деятельности.

Так, непредсказуемость (де)криминализации даже для специалистов отмечал Нечаев А. Автор среди факторов, усугубляющих кризис уголовной политики в области (де)криминализации, определил «неверную оценку законодателем степени общественной опасности запрещенных под угрозой наказания деяний», считая, что «уголовная репрессия все чаще становится для законодателя первым средством разрешения социальных конфликтов и противоречий», а (де)криминализацию предлагает понимать как процесс и результат установления (устранения) уголовно-правового запрета [4]. Аналогичной позиции придерживается и Митюкова Ю.А., отмечая, что «игнорирование обоснования декриминализации может привести к принятию

необоснованных правотворческих решений, не способствующих совершенствованию уголовно-правового регулирования» [5].

Законодателю следует также обратить внимание, что «реагирование» на запросы общества по тем или иным резонансным делам, особенно, в сфере семейно-бытовых отношений, должно учитывать и устои самого уголовного закона, который долгое время определял степень общественной опасности, например, причинения вреда здоровью в определенной последовательности, которая также отражалась и на аналогичной правовой оценке иных деяний, содержащих такие признаки. Например, степень общественной опасности преступлений, имеющих признаки насилия, опасного или не опасного для жизни и здоровья человека, следовало также синхронизировать с новой оценкой степени общественной опасности, которую получили составы умышленного причинения легкого вреда здоровью (в новом варианте ст.108-1 УК РК квалифицированные виды состава определены как преступления небольшой тяжести, в то время как в первоначальной редакции ст.108 УК РК до ее декриминализации – это был уголовный проступок без каких-либо квалифицирующих составов).

---

1. О неоднозначности (де)криминализации побоев см.: **Артюшина О.В.** Частичная декриминализация побоев как экономия мер уголовной репрессии \\ Вестник Казанского юридического института МВД России. – 2016. – №2 (26). – С.44-46. //Вестник 4 (26) 2016.pdf.
2. Закон Республики Казахстан от 16.07.2025 г. «О внесении изменений и дополнений в некоторые законодательные акты Республики Казахстан по вопросам оптимизации уголовного законодательства Республики Казахстан» // https://adilet.zan.kz/rus/docs/Z2500000210#z258.
3. Закон Республики Казахстан от 17.03.2023 г. «О внесении изменений и дополнений в некоторые законодательные акты Республики Казахстан по вопросам прав человека в сфере уголовного судопроизводства, исполнения наказания, а также предупреждения пыток и других жестоких, бесчеловечных или унижающих достоинство видов обращения» // https://adilet.zan.kz/rus/docs/Z2300000212#z44.
4. **Нечаев А.Д.** Концептуальные основы и теоретическое моделирование криминализации и декриминализации: Автореферат дисс. на соиск. уч. степ. к.ю.н., 2017 // Диссертация на тему «Концептуальные основы и теоретическое моделирование криминализации и декриминализации».
5. **Митюкова Ю.А.** Декриминализация преступлений: теоретический и практический аспекты: Автореферат дисс. на соиск. уч. степ. к.ю.н., 2020 // Диссертация на тему «Декриминализация преступлений: теоретический и практический аспекты».

ТРАНСФОРМАЦИЯ ПРАВОВЫХ ИНСТИТУТОВ ОБЕСПЕЧЕНИЯ ОБЩЕСТВЕННОЙ БЕЗОПАСНОСТИ НА ВОЗДУШНОМ ТРАНСПОРТЕ В УСЛОВИЯХ ГЛОБАЛИЗАЦИИ И ЦИФРОВИЗАЦИИ

ДАЕТОВА Аида Асылбековна
Докторант 2 курса Алматинской академии МВД Республики Казахстан имени М. Есбулатова, подполковник полиции

В статье рассматриваются современные правовые и организационные подходы к обеспечению общественной безопасности на объектах воздушного транспорта Республики Казахстан. Особое внимание уделяется трансформации функций транспортной полиции, взаимодействию органов внутренних дел со службами авиационной безопасности, влиянию цифровизации на правоприменительную деятельность, а также международным стандартам защиты гражданской авиации от актов незаконного вмешательства. Обосновывается, что в условиях глобализации аэропорт перестает быть только объектом транспортной инфраструктуры и приобретает значение сложной правовой, технологической и безопасной среды, требующей межведомственной координации, сервисной модели полиции и риск-ориентированного управления.

Обеспечение общественной безопасности на объектах воздушного транспорта в современных условиях приобретает особое значение, поскольку гражданская авиация является не только элементом транспортной системы государства, но и важнейшей частью международной мобильности, экономики, туризма, деловых коммуникаций и трансграничного сотрудничества. Глобализация и цифровизация существенно изменили характер угроз в аэропортах: наряду с традиционными правонарушениями актуализировались риски террористического характера, незаконного оборота запрещенных предметов, кибервмешательства, дестабилизации работы критической инфраструктуры, распространения ложной информации, а также использования цифровых технологий в противоправных целях.

Данные аспекты оказывают влияние не только на характер угроз в сфере воздушного транспорта, но и на содержание правовых институтов, регулирующих обеспечение общественной безопасности. Трансформации подвергаются институты государственного контроля, межведомственного взаимодействия, информационной безопасности, защиты персональных данных и полицейской деятельности, что требует их адаптации к новым условиям функционирования транспортной инфраструктуры.

Международная организация гражданской авиации рассматривает авиационную безопасность как сферу, направленную на предотвращение и пресечение актов незаконного вмешательства в деятельность гражданской авиации [1]. Стандарты и рекомендуемая практика ИКАО ориентированы на постоянное обновление мер защиты с учетом новых угроз и технологических изменений. Непосредственно вопросам авиационной безопасности посвящено Приложение 17 к Чикагской конвенции [2].

Для Казахстана данное положение имеет принципиальное значение, поскольку национальное законодательство должно развиваться не изолированно, а во взаимосвязи с международными обязательствами и стандартами гражданской авиации.

Правовую основу обеспечения авиационной безопасности в Республике Казахстан составляет Закон Республики Казахстан от 15 июля 2010 года № 339-IV «Об использовании воздушного пространства Республики Казахстан и деятельности авиации». В статье 105 указанного Закона закреплено, что эксплуатанты аэродромов, вертодромов и воздушных судов обязаны принимать меры по защите гражданской авиации от актов незаконного вмешательства. При этом законодатель прямо относит к таким актам незаконный захват воздушного судна, разрушение воздушного судна, захват заложников, насильственное проникновение на борт воздушного судна или в аэропорт, размещение оружия или опасных устройств, использование воздушного судна для причинения вреда, а также сообщение ложной информации, создающей угрозу безопасности [3].

Следовательно, авиационная безопасность имеет комплексную природу: она включает административно-правовые, уголовно-правовые, организационные, технические и профилактические меры.

Одновременно обеспечение общественного порядка и безопасности граждан на объектах транспорта относится к сфере деятельности органов внутренних дел. Закон Республики Казахстан «Об органах внутренних дел» определяет органы внутренних дел как правоохранительный орган, основными целями которого являются защита жизни, здоровья, прав и свобод человека и гражданина, интересов общества и государства от противоправных посягательств, охрана общественного порядка и обеспечение общественной безопасности [4].

В этой связи полиция выступает самостоятельным субъектом правоприменительной деятельности на объектах воздушного транспорта, однако ее деятельность не может рассматриваться отдельно от служб авиационной безопасности, администрации аэропортов, авиакомпаний, пограничных, таможенных и иных государственных органов. Практика показывает, что недостатки взаимодействия чаще всего становятся причиной снижения эффективности реагирования на угрозы.

Проблема взаимодействия полиции и иных субъектов безопасности в научной литературе отчасти рассматривается через концепцию «управления безопасностью» как распределенной системы. Так, К. Ширинг развивает идею «узлового управления безопасностью», согласно которой обеспечение порядка в современном обществе осуществляется не только государственными органами, но и множеством негосударственных и специализированных институтов, действующих в едином пространстве безопасности [5]. Данный подход особенно применим к аэропорту, где одновременно функционируют полиция, службы авиационной безопасности, частные подрядчики, диспетчерские службы, пограничный и таможенный контроль, администрация аэропорта и авиаперевозчики.

Схожую позицию развивают И. Лодер и Н. Волкер, рассматривая безопасность как общественное благо, которое требует не только силового обеспечения, но и демократической легитимности, доверия и подотчетности [6].

В условиях трансформации правоохранительной системы Республики Казахстан особое значение приобретает развитие сервисно-ориентированной модели полицейской деятельности. По мнению Ж.Р. Дильбархановой, Э.М. Насыровой и С.К. Кан, сервисная модель полиции представляет собой современную форму организации правоохранительной деятельности, основанную на взаимодействии государства и общества, профилактике правонарушений, открытости полиции и укреплении доверия населения к правоохранительным органам [7]. Авторы подчеркивают, что эффективность полиции в современных условиях определяется не только количеством выявленных правонарушений, но и способностью обеспечивать безопасность посредством партнерства с населением и иными субъектами системы общественной безопасности [7]. Применительно к объектам воздушного транспорта указанная концепция представляется особенно актуальной, поскольку безопасность в аэропорту обеспечивается не одним субъектом, а совокупностью взаимосвязанных государственных и негосударственных институтов.

В зарубежной криминологической науке значительный вклад в развитие современных подходов к полицейской деятельности внес Г. Голдштейн, предложивший концепцию проблемно-ориентированной полиции. По его мнению, полиция должна концентрироваться не только на внутренних организационных процедурах, но и на конечном результате – решении конкретных проблем, вызывающих общественную небезопасность [8].

Применительно к объектам воздушного транспорта это означает необходимость анализа не отдельных эпизодов правонарушений, а устойчивых факторов риска: зон скопления пассажиров, конфликтов при посадке, повторяющихся случаев ложных сообщений, нарушений досмотрового режима, хищений багажа и грузов, а также уязвимостей цифровой инфраструктуры аэропорта.

Д. Бейли, исследуя перспективы развития полиции в демократических государствах, подчеркивал, что современная полиция должна быть ориентирована на предотвращение преступности и повышение доверия общества, а не только на реактивное реагирование после совершения правонарушения [9]. Эта идея непосредственно связана с реформой казахстанской полиции и переходом к сервисной модели, в рамках которой приоритетом становится партнерство полиции и общества, профилактика правонарушений, открытость и использование цифровых технологий.

В казахстанском контексте особое значение имеет профессиональная подготовка специалистов авиационной безопасности. Так, А. Бейсенбаева, А. Булатбаева, М. Богачева и Е. Сулейманова обосновывают необходимость специальной подготовки сотрудников служб авиационной безопасности аэропортов, в том числе по вопросам психологического профайлинга [10]. Данный вывод имеет практическое значение и для органов внутренних дел на

транспорте, поскольку полицейский в аэропорту должен обладать не только общими навыками охраны общественного порядка, но и пониманием специфики авиационной среды, режимных зон, процедур досмотра, поведения пассажиров, а также алгоритмов взаимодействия с авиационными службами.

Цифровизация существенно меняет содержание правоприменительной деятельности на объектах воздушного транспорта. Современный аэропорт является высокотехнологичной средой, где используются системы видеонаблюдения, биометрической идентификации, базы данных пассажиров, автоматизированные системы контроля доступа. Внедрение подобных решений способствует повышению уровня безопасности, однако одновременно создает новые риски, связанные с защитой персональных данных и устойчивостью информационной инфраструктуры.

По мнению Е.Укванду и соавторов, дальнейшая цифровизация гражданской авиации требует формирования эффективных механизмов защиты критической информационной инфраструктуры аэропортов и авиационных систем от киберугроз, поскольку именно IT-инфраструктура является одним из наиболее уязвимых элементов современной авиационной отрасли [11]

В этой связи цифровизация должна рассматриваться не как самостоятельная цель, а как инструмент повышения эффективности правоприменения при обязательном соблюдении законности, прав человека, режима персональных данных и процессуальной допустимости получаемой информации. Использование видеозаписей, цифровых следов, систем контроля доступа и иных электронных данных требует четкого правового режима: кто имеет доступ к информации, в каком порядке она передается полиции, как фиксируется ее происхождение, как обеспечивается неизменность данных и каким образом они могут быть использованы в административном или уголовном производстве.

Особое значение имеет межведомственное взаимодействие. В действующей модели аэропортовой безопасности полиция не может самостоятельно охватить весь объем угроз, поскольку значительная часть первичной информации находится у служб авиационной безопасности, авиакомпаний, операторов аэропорта, диспетчерских служб и иных субъектов. Поэтому необходимы устойчивые правовые и организационные механизмы обмена информацией, совместного реагирования, проведения тренировок, распределения зон ответственности и фиксации действий каждого субъекта. В противном случае взаимодействие будет зависеть преимущественно от личной инициативы должностных лиц, что снижает устойчивость всей системы безопасности.

Проведенный анализ позволяет сделать вывод о необходимости дальнейшего совершенствования механизмов обеспечения общественной безопасности на объектах воздушного транспорта по нескольким ключевым направлениям.

Во-первых, необходимо нормативно конкретизировать алгоритмы взаимодействия транспортной полиции со службами авиационной безопасности аэропортов и авиапредприятий.

Во-вторых, следует развивать специализированную подготовку сотрудников полиции, несущих службу в аэропортах, с учетом международных

стандартов ИКАО, специфики актов незаконного вмешательства, цифровых угроз и коммуникации с пассажирами.

В-третьих, требуется внедрение риск-ориентированного подхода, при котором профилактические меры строятся не формально, а на основе анализа пассажиропотока, криминогенных зон, повторяющихся инцидентов и оперативной информации.

В-четвертых, цифровые инструменты должны использоваться при наличии четких гарантий законности, защиты персональных данных и процессуальной пригодности полученной информации.

Таким образом, цифровизация и глобализация трансформируют традиционные подходы к обеспечению общественной безопасности на воздушном транспорте, переводя их от преимущественно ведомственной модели к модели комплексного управления рисками, основанной на межведомственном взаимодействии, использовании цифровых технологий и международных стандартах авиационной безопасности.

1. Конвенция о международной гражданской авиации 1944. Doc. ICAO 7300/9 [Электронный ресурс] – URL: //https://wipolex-res.wipo.int/edocs/lexdocs/treaties/ru/icao-ca/trt_icao_ca_002ru.pdf (дата обращения: 10.05.2026);
2. Приложение 17 к Конвенции о международной гражданской авиации «Авиационная безопасность. Защита международной гражданской авиации от актов незаконного вмешательства». Международные стандарты и рекомендуемая практика (действует с 18.11.2022 г.). - Издание 12. – 2022. ISBN 978-92-9265-808-3 (печатная копия);
3. Закон Республики Казахстан от 15.07.2010 № 339-IV «Об использовании воздушного пространства Республики Казахстан и деятельности авиации» (с изменениями и дополнениями по состоянию на 09.01.2026 г.) [Электронный ресурс] – URL: //https://adilet.zan.kz/rus/docs/Z100000339_ (дата обращения: 11.05.2026);
4. Закон Республики Казахстан от 23 апреля 2014 года № 199-V «Об органах внутренних дел Республики Казахстан» (с изменениями и дополнениями по состоянию на 09.01.2026) [Электронный ресурс] – URL: // https://adilet.zan.kz/rus/docs/Z1400000199 (дата обращения: 11.05.2026);
5. **Shearing C.D.** Nodal Security // Police Quarterly. 2005. Vol. 8(1). P. 57–63;
6. **Loader I., Walker N.** Civilizing Security. Cambridge: Cambridge University Press, 2007;
7. **Дильбарханова Ж.Р., Насырова Э.М., Кан С.К.** Сервисная модель полиции Казахстана: доверие и безопасность в современном обществе // Ученые труды Алматинской академии МВД Республики Казахстан имени Макана Есбулатова. – 2024. – №3(80). – С. 78–83;
8. **Goldstein H.** Improving Policing: A Problem-Oriented Approach // Crime & Delinquency. 1979. Vol. 25. Issue 2. P. 236–258;
9. **Bayley D.H.** Police for the Future. New York: Oxford University Press, 1994;
10. **Бейсенбаева А.К., Булатбаева А.А., Богачева М.А., Сулейманова Е.С.** Профессиональная подготовка специалистов служб авиационной безопасности аэропортов // Вестник Казахского национального университета имени аль-Фараби. Серия «Педагогические науки». – 2023. – Т. 75. – № 2. – С. 4–14. DOI: 10.26577/JES.2023.v75.i2.01.;
11. **Ukwandu E., Ben-Farah M.A., Hindy H., Bures M., Atkinson R., Tachtatzis C., Andonovic I., Bellekens X.** Cyber-Security Challenges in Aviation Industry: A Review of Current and Future Trends // Information. – 2022. – Vol. 13. – No. 3. – Article 146. – DOI: 10.3390/info13030146.

ПРИМЕНЕНИЕ ТЕХНОЛОГИЙ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА И DIGITAL TWIN ДЛЯ ПОВЫШЕНИЯ УРОВНЯ БЕЗОПАСНОСТИ СОТРУДНИКОВ ПОЛИЦИИ

ДЮСЕБЕКОВА Сабина Булатовна
Докторант 1 курса послевузовского образования Академии управления МВД Республики Казахстан, капитан полиции

Статье рассматривается проблема обеспечения личной безопасности сотрудников полиции Республики Казахстан в условиях фактической непрерывности исполнения служебных обязанностей. Актуальность исследования обусловлена ростом уровня агрессии в обществе, увеличением числа насильственных правонарушений в отношении представителей власти и недостаточной защищенностью сотрудников, особенно во внеслужебное время. На основе анализа судебной практики и конкретных кейсов выявлены ключевые факторы профессиональной виктимности, включая зависимость уровня угроз от времени суток, социальных условий и характера ситуации. Установлено, что основным риском является не только наличие угрозы, но и ограниченные возможности оперативного реагирования. В работе обоснована необходимость внедрения практико-ориентированных цифровых решений и предложена концепция носимого устройства экстренного реагирования (смарт-часов), функционирующего на основе технологии цифрового двойника. Данная система обеспечивает оперативную передачу сигнала тревоги, геолокации и данных об обстановке при сохранении прав сотрудника за счет добровольной активации и минимизации собираемой информации. Сделан вывод о необходимости комплексного подхода, включающего правовые, организационные и технологические меры.

Введение. Актуальность настоящего исследования обусловлена приоритетами государственной политики Республики Казахстан, направленной на укрепление принципа «Закон и Порядок» как фундаментальной основы устойчивого развития общества и государства. В рамках данной политики особое значение придается формированию нулевой терпимости к правонарушениям, насилию и иным проявлениям антисоциального поведения. [1]

Реализация указанного принципа предполагает консолидацию усилий государственных органов, выработку единого подхода к обеспечению правопорядка и системную поддержку соответствующих инициатив. В этих условиях возрастает значимость формирования устойчивого общественного иммунитета к противоправным проявлениям, включая агрессию, грубость и насилие, которые все чаще наблюдаются в повседневной жизни, в том числе в общественных местах.

Современная социальная среда характеризуется ростом агрессии, снижением правовой культуры отдельных категорий граждан и увеличением числа правонарушений, сопряженных с насилием в отношении представителей власти. Данная тенденция подтверждается как официальной статистикой органов внутренних дел Республики Казахстан, так и резонансными случаями, широко освещаемыми в средствах массовой информации.

Особое значение имеет специфика правового статуса сотрудников полиции, на которых возложена обязанность пресекать правонарушения независимо от

времени и места их совершения. Это фактически закрепляет непрерывный характер исполнения служебных обязанностей, повышает уровень профессиональных рисков и расширяет спектр потенциальных угроз, включая ситуации вне служебной деятельности.

Таким образом, формируется противоречие между обязанностью реагировать на правонарушения в любой ситуации, включая внеслужебное время, и недостаточным уровнем правовой, организационной и социальной защищенности. Указанное противоречие обусловливает необходимость комплексного научного осмысления проблемы и разработки эффективных механизмов обеспечения личной безопасности.

Объектом исследования выступают общественные отношения в сфере обеспечения безопасности сотрудников полиции.

Предметом исследования являются правовые, организационные и технологические механизмы защиты в условиях цифровой трансформации.

Цель исследования заключается в разработке научно обоснованных предложений по повышению уровня безопасности сотрудников полиции с использованием современных цифровых технологий. Для ее достижения решаются следующие задачи: анализ правового статуса сотрудника полиции; выявление факторов профессиональной виктимности; изучение зарубежного опыта; анализ цифровых решений; разработка концепции интеллектуальной системы экстренного реагирования.

Степень научной разработанности проблемы характеризуется наличием значительного числа исследований. В работах Рустемовой Г.Р., Лесовой Н.Н., Милюкова С.Ф. и Зуевой Ю.В. раскрыты теоретико - правовые и криминологические основы безопасности сотрудников полиции, исследования Роота В.В., Зайырбековой А.А. и Кузнецова Д.Ю. посвящены виктимологическим и психологическим аспектам, труды Ешанова А.Ш., Семиглазова А.Г., Абдулина А.Р. и Якушева В.А. систематизируют прикладные вопросы подготовки и защиты сотрудников, Молдабаев С.С., Сабирдинов Б.С., Сайтбеков А.М., Кулмуханбетова Б.А. и Аханов Б.Б. акцентируют внимание на социальной и правовой защищенности. Вместе с тем исследования носят фрагментарный характер и не формируют целостной модели обеспечения безопасности, особенно с учетом цифровых технологий, что указывает на наличие научного пробела.

Научная новизна исследования заключается в комплексном криминологическом и правовом анализе обеспечения личной безопасности сотрудников полиции в условиях непрерывности исполнения служебных обязанностей. На основе анализа судебной практики, а также реального кейса ситуации выявлены устойчивые факторы профессиональной виктимности и обосновано, что ключевым риском является ограниченность оперативного реагирования как вовремя так и вне служебной деятельности. Предложена концепция применения цифрового двойника с использованием смарт-часов, обеспечивающая экстренное оповещение, передачу геолокации и анализ обстановки в режиме реального времени.

Практическая значимость заключается в возможности применения результатов исследования в деятельности правоохранительных органов Республики Казахстан для повышения уровня личной безопасности сотрудников. Предложенная концепция может быть использована при разработке цифровых систем экстренного реагирования, а также при совершенствовании ведомственных инструкций и образовательных программ.

Методологическую основу исследования составляет комплекс взаимодополняющих методов. Системный подход позволил рассмотреть безопасность сотрудника как элемент общей системы общественной безопасности. Формально-юридический метод применялся при анализе законодательства Республики Казахстан. Криминологический метод использован для выявления факторов профессиональной виктимности. Сравнительно-правовой метод позволил изучить зарубежный опыт.

Эмпирическую базу составили приговоры судов Республики Казахстан по делам о применении насилия в отношении представителей власти. Разработана аналитическая модель, включающая параметры личности правонарушителей, мотивы, характер агрессии, обстоятельства дела и назначенные меры наказания, что позволило выявить типичные криминологические характеристики и условия совершения правонарушений.

Дополнительно применен метод кейс-стади для анализа инцидента, получившего распространение в социальных сетях, в котором сотрудник полиции подвергается агрессии в присутствии ребенка.

Сопоставление результатов показало, что ключевой уязвимостью является не только сам факт угрозы, но и отсутствие оперативных механизмов реагирования вне стандартной служебной обстановки. Полученные данные обосновывают необходимость внедрения технологических решений, направленных на сокращение времени реагирования в критических ситуациях.

Основная часть. Профессиональная виктимность сотрудников органов внутренних дел представляет собой социально–правовой феномен, обусловленный их статусом представителей государственной власти, осуществляющих правоохранительную деятельность. Она имеет объективный характер и напрямую связана с исполнением служебных обязанностей по защите правопорядка, что формирует повышенный риск противоправных посягательств [2, с. 53].

В научной литературе данное явление рассматривается как подверженность угрозам, нахождение в зоне повышенного риска либо состояние уязвимости, отражающие единую сущность – повышенную вероятность причинения вреда сотруднику в связи с его служебной деятельностью. Уязвимость проявляется в ограниченных возможностях своевременного обеспечения собственной безопасности и передачи сигнала о помощи, особенно при внезапном возникновении конфликтных ситуаций. Ее причины носят комплексный характер и обусловлены как условиями совершения правонарушений, так и спецификой службы.

Международные исследования подтверждают, что сотрудники правоохранительных органов значительно чаще подвергаются насильственным действиям по сравнению с представителями других профессий. [3]

В рамках исследования проведен анализ судебной практики по делам о применении насилия в отношении представителей власти. Эмпирическую базу составили десять приговоров судов Республики Казахстан, вынесенных по соответствующей категории дел и связанных с посягательствами на сотрудников полиции при исполнении ими служебных обязанностей. Отбор судебных актов осуществлялся по критериям релевантности предмету исследования, наличия описательной части, позволяющей установить обстоятельства совершения правонарушений, а также репрезентативности рассматриваемых ситуаций.

Проведенный анализ позволил выявить устойчивые криминологические закономерности. Установлено, что большинство инцидентов происходит в темное время суток, что обусловлено ограниченной видимостью, снижением общественного контроля и повышенной вероятностью агрессивного поведения правонарушителей. Значительная часть противоправных действий совершается в выходные дни, что связано с ростом социальной активности и употреблением алкоголя. Территориально рассматриваемые случаи носят повсеместный характер, что свидетельствует о системности проблемы и ее общенациональном масштабе.

Дополнительным фактором риска выступает режим служебной деятельности. Продолжительность рабочего времени для сотрудников устанавливается в соответствии с трудовым законодательством Республики Казахстан, однако в случае необходимости сотрудники могут привлекаться к выполнению служебных обязанностей сверх установленного времени, а также в ночное время, выходные и праздничные дни. [4]

Исходя из анализа приговоров ясно, что в большинстве случаев сотрудник подвергается агрессии в темное время суток. Нередки случаи, когда сотрудник может быть подвергнут насилию во внеслужебное время.

Вспомним случай, произошедший в марте 2026 года в городе Костанай, когда сотрудник полиции, сопровождая малолетнего ребенка, подвергся нападению. Несмотря на то, что обстоятельства произошедшего выходили за рамки формального исполнения служебных обязанностей, действия сотрудника были обусловлены необходимостью реагирования на правонарушение. Нападение было квалифицировано как применение насилия в отношении представителя власти. [5]

Специфика профессии связанна с круглосуточным реагированием. Даже находясь вне исполнения служебных обязанностей, сотрудник сохраняет статус представителя власти и обязан реагировать на правонарушения. Отсутствие специальных средств защиты, поддержки со стороны коллег и четкой координации действий существенно увеличивает уровень риска. В результате сотрудник оказывается в ситуации повышенной уязвимости, что требует разработки дополнительных механизмов защиты.

Выявленные закономерности свидетельствуют о том, что профессиональная виктимность сотрудников полиции носит устойчивый и ситуационно

обусловленный характер, при котором уровень риска существенно возрастает в условиях ночного времени, выходных дней, а также при исполнении обязанностей вне службы. При этом ключевым уязвимым элементом выступает ограниченность возможностей оперативного реагирования и передачи сигнала о помощи в момент возникновения угрозы. В совокупности это указывает на необходимость перехода от исключительно организационно-правовых мер защиты к применению технологических решений, обеспечивающих непрерывный мониторинг состояния сотрудника и мгновенное оповещение в случае опасности, что в международной практике реализуется посредством цифровых систем экстренного реагирования.

Зарубежные исследования показывают, что использование современных информационных систем и технологий искусственного интеллекта позволяет существенно повысить эффективность деятельности правоохранительных органов [6, с. 22]. В частности, внедрение технических средств мониторинга и фиксации способствует снижению уровня угроз и повышению результативности реагирования на правонарушения.

Особое значение приобретают системы оперативного реагирования, которые обеспечивают сокращение времени прибытия помощи и повышают координацию действий подразделений. Так, результаты рандомизированных экспериментов, проведенных в США, свидетельствуют о снижении случаев сопротивления более чем на 50% и количества жалоб на сотрудников – более чем на 60% [7].

Эффективность указанных решений во многом обусловлена применением алгоритмов машинного обучения, которые позволяют идентифицировать факторы риска, оценивать вероятность криминальных событий и формировать прогнозные оценки, используемые при принятии превентивных и тактических решений.

В более широком контексте следует отметить, что в настоящее время искусственный интеллект активно развивается во всех сферах общественной жизни: цифровые технологии проникают в экономику, государственное управление, сферу безопасности и повседневную деятельность человека. В этих условиях возрастает значение интеллектуальных систем анализа данных, способных обрабатывать большие массивы информации и выявлять скрытые закономерности.

Вместе с тем развитие аналитических и прогностических технологий дополняется необходимостью внедрения практических решений, обеспечивающих оперативное реагирование на уже возникшие угрозы. В этой связи особый интерес представляет зарубежный опыт использования носимых систем экстренного оповещения.

Наибольший уровень доверия пользователей обеспечивают системы с ручной активацией тревожного сигнала, поскольку они исключают элементы скрытого наблюдения и предоставляют сотруднику полный контроль над передачей информации. В работе «Comparing panic alarm systems for high-risk domestic abuse victims» отмечается, что такие устройства становятся значимым элементом систем безопасности, включая взаимодействие с

правоохранительными органами. [9] Это подтверждается и зарубежной практикой: в США применяются носимые устройства, интегрированные в служебные бейджи, позволяющие одним нажатием передавать сигнал тревоги с указанием точного местоположения, а также аналогичные решения в образовательных учреждениях, где персонал оснащается индивидуальными кнопками экстренного реагирования. Их эффективность подтверждается реальными инцидентами: например, в одном из учебных заведений штата Джорджия использование таких устройств позволило своевременно уведомить правоохранительные органы об угрозе и обеспечить её оперативную локализацию.[10] Такие решения рассматриваются как эффективный инструмент экстренного реагирования, позволяющий оперативно передавать сигнал о помощи.

Таким образом, зарубежный опыт демонстрирует высокую эффективность носимых устройств экстренного оповещения и подтверждает целесообразность их внедрения как элемента системы обеспечения безопасности сотрудников, что формирует основу для дальнейшего развития более комплексных решений, включая интеллектуальные носимые устройства с расширенным функционалом.

В настоящее время в Министерство внутренних дел Республики Казахстан в рамках концепции сервисной полиции реализованы ряд цифровых проектов, направленных на повышение уровня общественной безопасности и оперативности реагирования. В частности, на улицах населенных пунктов установлены кнопки экстренного вызова «SOS», позволяющие гражданам в кратчайшие сроки связаться с правоохранительными органами. Кроме того, функционируют мобильные приложения, обеспечивающие возможность обращения в полицию и получения государственных услуг в электронном формате.

Указанные инициативы, разработанные в рамках сервисной модели полиции, получили положительную оценку со стороны представительных органов и признаны перспективными, соответствующими современным требованиям. Они отличаются продуманностью, доступностью и простотой использования. Автоматизация государственных услуг способствует сокращению сроков их оказания и ориентирована на достижение конкретного результата. [11, с.243]

Вместе с тем в деятельности органов внутренних дел применяются и иные цифровые средства, в частности видеожетоны (нагрудные видеорегистраторы), предназначенные для фиксации правонарушений и документирования действий сотрудников. Однако их использование, как правило, ограничено отдельными категориями личного состава, прежде всего сотрудниками патрульно-постовой службы и участковыми инспекторами. Это свидетельствует о сохраняющемся технологическом разрыве в уровне оснащенности различных подразделений.

В этой связи представляется целесообразным развитие универсального технического инструмента, доступного каждому сотруднику полиции и являющегося неотъемлемым элементом форменного обмундирования. Перспективным направлением является использование носимых цифровых устройств, в частности смарт-часов, интегрированных с системой обеспечения

личной безопасности и функционирующих на основе цифрового двойника сотрудника. Такое решение обеспечит непрерывный мониторинг, оперативную передачу данных и возможность мгновенной подачи сигнала тревоги с автоматическим определением местоположения, что позволит повысить уровень защищенности сотрудников и эффективность реагирования.

Функционирование указанного устройства может быть основано на технологии так называемого «цифрового двойника». Цифровой двойник (Digital Twin) – это современная концепция информационных технологий, которая набирает популярность вместе с развитием Индустрии 4.0. Она становится все более значимой в промышленности и привлекает внимание многих отраслей. Технология может стать отличным инструментом для компаний, позволяющим повысить свою конкурентоспособность, производительность и эффективность. [12, с.36]

Технология цифровых двойников широко применяется в промышленности (Industry 4.0), здравоохранении, транспортных системах и управлении сложными инфраструктурами, обеспечивая мониторинг, прогнозирование и оперативное принятие решений.

Лю и соавторы говорят о том, что цифровой двойник на самом деле представляет собой живую модель физического актива или системы, которая постоянно адаптируется к операционным изменениям на основе собранных онлайн-данных и информации и может прогнозировать будущее соответствующего физического аналога. [13]

Ю. Чжэн и соавторы описывают цифровой двойник в рамках производственного процесса: «Цифровой двойник – это набор виртуальной информации, которая полностью описывает потенциальное или реальное физическое производство от микроатомного до макрогеометрического уровня». [14]

Я. Трауер и соавторы определяют в своей работе цифровой двойник как «виртуальное динамическое представление физической системы, которое подключено к ней на протяжении всего жизненного цикла для двунаправленного обмена данными». [15]

В работе говорится о том, что физический двойник автоматически передает, среди прочего, данные о своем поведении, своем статусе и информацию об окружающей среде из реального пространства в виртуальное пространство в течение всего жизненного цикла продукта, когда это необходимо. В то же время виртуальный двойник идентифицирует улучшения, ориентированные на продукт или процесс, контролирует требования, основанные на текущей ситуации или прогнозах ближайшего будущего, и отправляет их обратно в реальное пространство, чтобы физический продукт соответствующим образом адаптировался.

Как мы видим, разные ученые трактуют термин «цифровой двойник» по-разному, однако, исходя из всех определений, можно сделать вывод о том, что цифровой двойник – это некая виртуальная модель физического объекта, с которым происходит автоматический взаимообмен данными и информацией, способствующий нахождению проблем и поиску их решений.[16, с. 150]

В контексте правоохранительной деятельности использование цифрового двойника сотрудника может быть направлено исключительно на обеспечение его безопасности. В данном случае формируется не полный цифровой профиль личности, а ограниченная функциональная модель, включающая критически важные параметры – местоположение, факт активации тревожного сигнала и, при необходимости, отдельные показатели обстановки.

Практическая реализация данной модели предполагает функционирование цифрового двойника на базе носимого устройства, синхронизированного с информационной системой правоохранительных органов. В обычном режиме устройство не передаёт данные, исключая постоянный мониторинг, при этом выполняя базовые функции (отображение времени, контроль пульса и других показателей).

Активация системы возможна как вручную, так и с помощью голосовой команды. После этого запускается автоматический обмен данными: передаются геолокация, временные параметры и сигнал тревоги в дежурный центр. На основе поступающей информации формируется актуальная цифровая модель ситуации, позволяющая в режиме реального времени отслеживать местоположение сотрудника и координировать действия ближайших нарядов.

В частности, система может быть настроена на распознавание индивидуальной голосовой команды сотрудника, предварительно заданной и привязанной к его биометрическим характеристикам. Такая команда может представлять собой краткую кодовую фразу служебного характера (например, «тревога», «помощь» и т.п.), что исключает случайную активацию и обеспечивает надежность срабатывания.

Использование голосовой активации имеет принципиальное значение в ситуациях, когда сотрудник ограничен в движениях или не имеет возможности воспользоваться ручным управлением. При этом сохраняется возможность альтернативного запуска системы посредством нажатия кнопки, что обеспечивает дублирование каналов активации и повышает общую надежность функционирования устройства.

Также возможно подключение модулей анализа акустической обстановки, позволяющих распознавать звуковые признаки конфликтных ситуаций (крики, угрозы, шум борьбы). Наряду с этим система может предусматривать кратковременную активацию видеомодуля, встроенного в носимое устройство. Видеофиксация осуществляется исключительно в момент активации тревожного сигнала и направлена на передачу визуальной информации в дежурный центр для более точной оценки обстановки.

Получаемые аудио и видеоданные интегрируются в цифровую модель ситуации (цифровой двойник), обеспечивая более полное представление о происходящем и позволяя повысить эффективность координации сил реагирования. При этом принципиально важным является то, что видеозапись не осуществляется на постоянной основе и активируется только по инициативе сотрудника либо в момент срабатывания тревожного сигнала, что обеспечивает соблюдение его права на неприкосновенность частной жизни.

Важной особенностью является способность системы функционировать в условиях отсутствия стабильного интернет–соединения. Передача сигнала может осуществляться через альтернативные каналы связи, включая ведомственные радиосети, что обеспечивает устойчивость работы в различных оперативных условиях.

Таким образом, цифровой двойник в рассматриваемом контексте выступает не как инструмент контроля за сотрудником, а как механизм оперативного реагирования, обеспечивающий своевременное выявление угроз и координацию действий по их нейтрализации при одновременном соблюдении прав сотрудника.

Принципиальное значение имеет соблюдение конституционных прав сотрудника, в том числе права на неприкосновенность частной жизни. В связи с этим функционирование системы должно основываться на принципах: минимизации собираемых данных, отсутствия постоянного мониторинга, исключительно голосовой либо ручной активации устройства.

Следует отметить, что предлагаемые меры по внедрению носимых систем экстренного реагирования соответствуют современным направлениям государственной политики Республики Казахстан в сфере цифровизации и развития технологий искусственного интеллекта. Целями государственного регулирования общественных отношений в сфере искусственного интеллекта являются обеспечение его развития и стимулирование внедрения в различных сферах общественной жизни. [17] Указанные положения, закрепленные в Закон Республики Казахстан об искусственном интеллекте, формируют правовую основу для интеграции интеллектуальных технологий в деятельность правоохранительных органов, в том числе в целях повышения уровня безопасности сотрудников полиции.

В свою очередь, положения Цифровой кодекс Республики Казахстан ориентированы на развитие цифровых решений в системе государственного управления, включая внедрение инновационных инструментов обеспечения общественной и личной безопасности [18].

Таким образом, разработка и внедрение носимого устройства экстренного реагирования, функционирующего на основе технологии цифрового двойника, не только отвечает выявленным криминологическим рискам, но и полностью соответствует приоритетам государственной политики, направленной на цифровую трансформацию и повышение эффективности деятельности правоохранительных органов.

Заключение. Проведенное исследование позволяет сделать вывод о том, что проблема обеспечения личной безопасности сотрудников полиции Республики Казахстан носит комплексный и системный характер. Она обусловлена не только спецификой их правового статуса и фактической непрерывностью исполнения служебных обязанностей, но и трансформацией современной социальной среды, характеризующейся ростом агрессии, снижением правовой культуры и расширением цифрового пространства взаимодействия.

Выявленные в ходе анализа судебной практики и конкретного кейса закономерности подтверждают, что ключевым фактором профессиональной виктимности сотрудников полиции является не только наличие угрозы, но и ограниченность возможностей оперативного реагирования. Наиболее уязвимыми условиями выступают ночное время, выходные дни, а также ситуации, в которых сотрудник действует вне стандартной служебной обстановки и лишен поддержки коллег и технических средств.

Существующие организационные и правовые механизмы обеспечения безопасности сотрудников в полной мере не учитывают данные риски, что формирует необходимость их модернизации с учетом современных вызовов. При этом анализ зарубежного опыта показывает, что наибольшую эффективность демонстрируют решения, направленные не только на профилактику и прогнозирование преступности, но и на обеспечение оперативного реагирования в момент возникновения угрозы.

В этой связи одним из приоритетных направлений повышения уровня безопасности сотрудников полиции является внедрение практико-ориентированных цифровых решений. Предложенная в работе концепция использования носимого устройства экстренного реагирования, функционирующего на основе технологии цифрового двойника, позволяет существенно сократить время передачи сигнала о помощи, обеспечить точное определение местоположения сотрудника и повысить эффективность координации действий дежурных служб.

Таким образом, решение проблемы обеспечения личной безопасности сотрудников полиции требует комплексного подхода, сочетающего правовые, организационные и технологические меры. Внедрение интеллектуальных систем экстренного реагирования, основанных на современных цифровых технологиях, представляет собой перспективное направление, способное существенно повысить уровень защищенности сотрудников и эффективность деятельности правоохранительных органов в целом.

1.Казахстан в эпоху искусственного интеллекта: актуальные задачи и их решения через цифровую трансформацию: Послание Главы государства Касым–Жомарта Токаева народу Казахстана от 8 сентября 2025 года [Электронный ресурс] // Режим доступа: https://primeminister.kz/ru/addresses/08092025 (дата обращения: 15.04.2026)

2.**Шалагин А.Е.** Криминологическая характеристика и предупреждение преступлений, связанных с посягательством на жизнь и здоровье сотрудника органов внутренних дел: Дипломная Раб. … – Казань, 2025. – 72 с.

3.**Van Reemst L,** Fischer T and Weerman F Aggression Against Police Officers and Behavior Toward Citizens: Reciprocal Influence or Common Causes? // Frontiers in Psychology. – 2022. – Vol. 13. – P. 1–10

4.О правоохранительной службе: Закон Республики Казахстан от 6 января 2011 года № 380–IV [Электронный ресурс] // Информационно–правовая система нормативных правовых актов Республики Казахстан. – Режим доступа: https://adilet.zan.kz/rus/docs/Z2400000072 (дата обращения: 15.04.2026)

5.Полицейского жестоко избили в Костанае – момент попал на видео [Электронный ресурс] // Режим доступа: https://www.zakon.kz/proisshestviia/6512923–politseyskogo–zhestoko–izbili–v–kostanae—moment–popal–na–video.html (дата обращения: 15.04.2026)

6.**Шульц В.Л., Бочкарев С.А., Кульба В.В., Шелков А.Б., Чернов И.В., Тимошенко А.А.** Анализ проблем трансформации систем законодательного регулирования и правоприменения в условиях цифровизации и методов оценки эффективности принимаемых решений // Национальная безопасность. – 2019. – №4. – С. 20–74

7.**Wesley G. Jennings, Mathew D. Lynch, Lorie A.** Fridell Evaluating the impact of police officer body–worn cameras (BWCs) on response–to–resistance and serious external complaints: Evidence from the Orlando police department (OPD) experience utilizing a randomized controlled experiment // Journal of Criminal Justice. – 2015. – Vol. 43. – P. 480–486

8.AI AND POLICING, THE BENEFITS AND CHALLENGES OF ARTIFICIAL INTELLIGENCE FOR LAW ENFORCEMENT // An Observatory Report from the Europol Innovation Lab. European Union Agency for Law Enforcement Cooperation. – 2024 [Электронный ресурс] // Режим доступа: https://www.eerstekamer.nl/bijlage/20241106/ai_and_policing_the_benefits_and (дата обращения: 15.04.2026)

9.**Hodgkinson W., Ariel B. & Harinam V.** Comparing panic alarm systems for high–risk domestic abuse victims: a randomised controlled trial on prevention and criminal justice system outcomes // J Exp Criminol – 2023. – Vol. 19. – P. 595–613
10.Georgia teachers pressed new panic buttons during shooting, alerting police
[Электронный ресурс] // Режим доступа: https://www.reuters.com/world/us/georgia–teachers–pressed–new–panic–buttons–during–shooting–alerting–police–2024–09–05/ (дата обращения: 15.04.2026)
11.**Токсанова М.Б.** Переход на сервисную модель в системе органов внутренних дел Республики Казахстан //Актуальные проблемы полицейского права. – 2021. – С. 239–244
12.**Сосфенов Д.А.** ЦИФРОВОЙ ДВОЙНИК: ИСТОРИЯ ВОЗНИКНОВЕНИЯ И ПЕРСПЕКТИВЫ РАЗВИТИЯ // Интеллект. Инновации. Инвестиции. – 2023. – №4. – С. 35–43
13.**Zheng L., Norbert M., Nezih M.** The role of data fusion in predictive maintenance using digital twin // AIP Conf. Proc. – 2018. – Vol. 1949 (1)
14.**Fu Y., Zhu G., Zhu M.** Digital Twin for Integration of Design–Manufacturing–Maintenance: An Overview // Chin. J. Mech. Eng. – 2022. – Vol. 35 (80)
15.**Trauer J, Schweigert–Recksiek S, Engel C, Spreitzer K, Zimmermann M.** WHAT IS A DIGITAL TWIN? – DEFINITIONS AND INSIGHTS FROM AN INDUSTRIAL CASE STUDY IN TECHNICAL PRODUCT DEVELOPMENT. Proceedings of the Design Society: DESIGN Conference. – 2020. – Vol.1. – P. 757–766
16.**Сосфенов Д.А.** ЦИФРОВОЙ ДВОЙНИК КАК ИНСТРУМЕНТ ОПТИМИЗАЦИИ ПРОИЗВОДСТВЕННЫХ ПРОЦЕССОВ // Инновации и инвестиции. – 2023. – №5. – С.149–153
17.Об искусственном интеллекте: Закон Республики Казахстан от 17 ноября 2025 года № 230–VIII ЗРК [Электронный ресурс] // Режим доступа: https://adilet.zan.kz/rus/docs/Z2500000230 (дата обращения: 15.04.2026)
18.Цифровой кодекс Республики Казазхстан: Кодекс Республики Казахстан от 12 января 2026 года № 255–VIII ЗРК [Электронный ресурс] // Информационно–правовая система нормативных правовых актов Республики Казахстан. – Режим доступа: https://adilet.zan.kz/rus/docs/K2600000255

ПЕРСПЕКТИВЫ ИСПОЛЬЗОВАНИЯ СИСТЕМ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ОРГАНИЗАЦИИ РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ НА ВОЗДУШНОМ И ЖЕЛЕЗНОДОРОЖНОМ ТРАНСПОРТЕ

ЖАКИПБЕКОВ Е.Н.
Докторант 1 курса факультета послевузовского образования Академии управления МВД РК, магистр юридических наук, полковник полиции

ЖАРЫЛКАСЫНОВ К.Ә.
Докторант 1 курса факультета послевузовского образования Академии управления МВД РК, магистр юридических наук, полковник полиции

В статье рассмотрены перспективы использования систем искусственного интеллекта в организации расследования преступлений на воздушном и железнодорожном транспорте в Республике Казахстан. На фоне институциональной модернизации, включающей создание в 2026 году Центра по расследованию транспортных происшествий и инцидентов, и положительной динамики состояния безопасности (снижение числа инцидентов на воздушном и железнодорожном транспорте по итогам 2025 года) формируется благоприятная среда для цифровой трансформации. В работе обосновывается, что ручная обработка значительных массивов технических и статистических данных больше не отвечает современным вызовам. Ключевой акцент сделан на необходимости создания единой ИИ-платформы, способной автоматически инициировать фиксацию доказательств в первые часы после происшествия: от запуска беспилотников и цифрового моделирования места происшествия до сохранения телеметрии и переговоров экипажей. Автором рассматриваются правовые аспекты легитимизации сгенерированные системой искусственного интеллекта выводы в уголовном процессе в соответствии с законодательством Республики Казахстан, а также вопросы интеграции с Национальной системой видеомониторинга и геоинформационными системами. Делается вывод о необходимости перехода к целостной интеллектуальной модели транспортной криминалистики для повышения оперативности и качества расследований.

Развитие транспортной инфраструктуры и цифровых технологий в современных условиях обусловливает необходимость совершенствования механизмов обеспечения транспортной безопасности и повышения эффективности расследования преступлений, совершаемых на объектах воздушного и железнодорожного транспорта. Транспортная система РК представляет собой стратегически важный элемент национальной экономики и государственного управления, функционирование которого связано с постоянным перемещением значительных потоков пассажиров, грузов и информации. В связи с этим транспортная сфера становится объектом повышенного внимания со стороны преступных групп, террористических организаций и иных субъектов противоправной деятельности.

Современные преступления на транспорте отличаются высокой степенью технологичности, трансграничным характером, использованием цифровых коммуникаций и сложных схем сокрытия следов преступной деятельности. Особую опасность представляют преступления, связанные с незаконным

вмешательством в деятельность гражданской авиации, диверсиями на объектах железнодорожного транспорта, кибератаками на автоматизированные системы управления движением, незаконным оборотом наркотических средств, контрабандой, террористическими угрозами и преступлениями коррупционной направленности.

В данных условиях традиционные методы расследования постепенно утрачивают достаточную эффективность, поскольку объем информации, подлежащей анализу, значительно превышает возможности ручной обработки данных следователем. Именно поэтому в деятельности правоохранительных органов все более активно внедряются системы искусственного интеллекта, позволяющие автоматизировать аналитические процессы, ускорить обработку цифровых доказательств и повысить эффективность принятия организационно-тактических решений.

Правовую основу использования цифровых технологий и интеллектуальных систем в нашей стране составляют Конституция РК [1], УПК РК [2], Законы РК «Об информатизации» «Об искусственном интеллекте» [3; 4]. Особое значение приобретает формирование правовых механизмов, обеспечивающих допустимость использования интеллектуальных систем в уголовном судопроизводстве, защиту персональных данных и соблюдение конституционных прав граждан.

В настоящее время искусственный интеллект рассматривается как совокупность технологий, обеспечивающих моделирование когнитивных функций человека посредством автоматизированной обработки информации, самообучения алгоритмов и интеллектуального анализа данных. В сфере расследования преступлений на транспорте данные технологии способны выполнять широкий комплекс задач, связанных с поиском, обработкой, классификацией и интерпретацией информации.

Особенности расследования преступлений на воздушном и железнодорожном транспорте обусловлены спецификой функционирования транспортной инфраструктуры.

Во-первых, транспортные объекты характеризуются высокой концентрацией пассажиропотока и интенсивностью движения, что существенно осложняет процесс выявления преступников и фиксации следов преступления.

Во-вторых, деятельность транспортных систем сопровождается непрерывным формированием больших массивов цифровых данных: видеозаписей, данных систем контроля доступа, навигационной информации, электронных билетов, телекоммуникационных сведений, логов автоматизированных систем управления и иных цифровых следов.

В-третьих, значительная часть транспортных преступлений носит межрегиональный либо транснациональный характер, что требует оперативного обмена информацией между различными ведомствами и государствами.

В этих условиях искусственный интеллект становится важнейшим инструментом организации расследования.

На сегодняшний день в Казахстане идет активный процесс формирования организационной основы модернизации системы расследования транспортных

происшествий, что создает благоприятные условия для последующего внедрения технологий искусственного интеллекта в деятельность органов транспортной безопасности и расследования транспортных преступлений. Статистика также свидетельствуют о положительной динамике состояния транспортной безопасности.

Так, по итогам 2025 года количество транспортных происшествий и инцидентов, подлежащих расследованию Департаментом по расследованию происшествий и инцидентов на транспорте Министерства транспорта РК, по сравнению с 2024 годом сократилось на воздушном с 42 до 35 случаев, а на железнодорожном транспорте с 16 до 7. Вместе с тем на водном транспорте зафиксирован рост происшествий с 3 до 9 случаев [5].

Департаментом ежегодно проводится анализ характерных тенденций транспортных происшествий, включая причины и способствующие факторы завершенных расследований, что имеет принципиальное значение для понимания перспектив использования систем искусственного интеллекта в организации расследования транспортных преступлений и происшествий. Фактически уже сегодня деятельность уполномоченных органов связана с анализом значительных объемов информации, включающих технические данные транспортных систем, результаты расследований, статистические показатели, сведения о причинах происшествий и факторах риска.

В существующих условиях обработка подобных массивов данных преимущественно осуществляется вручную либо посредством разрозненных информационных систем. Использование интеллектуальных алгоритмов позволило бы обеспечить автоматизированный анализ причинно-следственных связей между происшествиями, выявление повторяющихся факторов риска и формирование прогнозных моделей транспортной безопасности.

При этом, как показывает практика, в ходе организации расследования преступлений на воздушном и железнодорожном транспорте особое значение имеют вопросы межведомственного взаимодействия с государственными органами РК, в частности, Главной транспортной прокуратурой, Министерствами внутренних дел, иностранных дел, по чрезвычайным ситуациям, здравоохранения, труда и социальной защиты населения, и их готовности к оперативному реагированию при транспортных происшествиях в труднодоступной местности (горные районы, акваторий и т.п.), а также оцепления места происшествия и сохранения вещественных доказательств, имеющих особое значения для установления причин происшествий.

Именно на данном этапе организация расследования наиболее остро нуждается во внедрении систем искусственного интеллекта. Зарубежная практика показывает, что значительная часть доказательственной информации утрачивается в первые часы после транспортного происшествия вследствие нарушения порядка фиксации следовой картины, отсутствия своевременного цифрового моделирования обстановки и недостаточной координации между ведомствами [6].

В связи с этим использование искусственного интеллекта в нашей стране должно быть ориентировано прежде всего на создание единой цифровой

системы фиксации и анализа транспортных происшествий. При поступлении информации о происшествии система должна автоматически инициировать: запуск беспилотных летательных аппаратов; создание трехмерной цифровой модели места происшествия; автоматизированную фиксацию расположения объектов; сохранение данных систем видеонаблюдения; резервное копирование переговоров диспетчеров и экипажей; выгрузку телеметрической информации транспортных средств.

Особую актуальность представляет разработанная по инициативе Главной транспортной прокуратуры при поддержке Министерства транспорта, Департамента полиции на транспорте и Министерства юстиции РК «Методика расследования авиакатастроф в сфере гражданской авиации: опыт, проблемы, решения». Данный документ направлен на формирование единой правоприменительной практики и координацию действий ответственных государственных органов, что позволит повысить эффективность расследований как со стороны правоохранительных органов, так и полномочного органа по расследованию в сфере гражданской авиации.

Фактически данная методика уже формирует основу для дальнейшей цифровизации расследования преступлений на воздушном транспорте. Однако эффективность подобной системы может быть существенно повышена за счет интеграции интеллектуальных аналитических комплексов, способных обеспечить: автоматизированный анализ параметров полета; сопоставление действий экипажа с требованиями авиационных регламентов; интеллектуальную обработку переговоров диспетчеров; выявление отклонений в работе навигационных систем; формирование цифровой хронологии происшествия.

Следует отметить, что в 2026 году запланировано начало работы АО «Центр по расследованию транспортных происшествий и инцидентов», предусматривающий внедрение нового подхода к формированию независимой и эффективной системы расследования в соответствии со стандартами и рекомендуемой практикой Международной организации гражданской авиации (ИКАО), включая производство независимой расшифровки бортовых регистраторов (черных ящиков), различные виды экспертиз, а также исследование в области микроэлектроники, в том числе их восстановление.

Данный этап представляет собой наиболее благоприятный момент для интеграции систем искусственного интеллекта непосредственно в организационную структуру расследования транспортных происшествий. Представляется целесообразным, чтобы в структуре нового Центра функционировало специализированное подразделение интеллектуальной транспортной криминалистики, обеспечивающее: анализ больших массивов транспортных данных; цифровое моделирование транспортных происшествий; интеллектуальную обработку видеоматериалов; автоматизированный анализ телеметрии; прогнозирование факторов транспортного риска; межведомственную интеграцию цифровой информации.

Особого внимания заслуживает международное сотрудничество в сфере расследования транспортных происшествий. В частности, в 2025 г. Департаментом по расследованию происшествий и инцидентов на транспорте

Министерства транспорта РК были подписаны Соглашения о взаимопонимании с полномочными органами по расследованию Сингапура и Объединенных Арабских Эмиратов. Данные государства являются одними из наиболее технологически развитых в области цифровизации транспортной безопасности и использования интеллектуальных систем анализа транспортных рисков.

Изучение международного опыта имеет принципиальное значение для формирования казахстанской модели интеллектуального сопровождения расследований. В частности, современные международные подходы предусматривают: обязательное цифровое моделирование мест транспортных происшествий; использование искусственного интеллекта для реконструкции событий; автоматизированный анализ систем управления транспортом; интеграцию цифровых доказательств в единые аналитические платформы; использование интеллектуальных систем прогнозирования угроз.

На основе соблюдения международных стандартов и изучения лучшей мировой практики Министерством транспорта в 2026 г. планируется внесения изменений и дополнений в нормативно-правовые акты РК в сфере расследования транспортных происшествий, которое должно сопровождаться закреплением правовых механизмов использования искусственного интеллекта в расследовании преступлений на транспорте. В частности, представляется необходимым нормативно определить: статус результатов интеллектуального анализа; порядок использования цифровых моделей места происшествия; требования к алгоритмам искусственного интеллекта; механизмы верификации результатов автоматизированного анализа; правила хранения и защиты цифровых доказательств.

Так, используемая система искусственного интеллекта должна быть сертифицирована согласно Закону РК «Об искусственном интеллекте» [Закон] как высокой степени риска и проходить регулярный независимый аудит на предмет отсутствия дискриминационных предубеждений в обучающих данных. Она должна быть интегрирована с Национальной системой видеомониторинга, базами данных правоохранительных органов (МВД, КНБ).

С железнодорожной инфраструктурой система должна быть напрямую интегрирована с геоинформационными системами АО «Қазақстан темір жолы», используя искусственный интеллект для анализа состояния путей, мостов и контактной сети, а также для мониторинга несанкционированной застройки в пределах полос отвода, что является частой причиной диверсий и хищений [7]. На воздушном транспорте в аэропортах следственные подразделения должны получить прямой канал доступа к очищенному потоку видеоархивов камер распознавания лиц (включая обсервацию зон duty-free и телетрапов) без возможности редактирования буфера, но с функцией автоматической маркировки временных меток, синхронизированных с бортовыми самописцами.

Все выводы, генерируемые системой, должны оформляться в виде структурированных процессуальных документов – «ИИ-аналитических заключений», которые прилагаются к материалам уголовного дела как письменные доказательства согласно ст. 120 УПК РК. Каждое такое заключение должно содержать полную информацию об использованной модели

искусственного интеллекта, версии программного обеспечения, исходных данных для анализа и параметрах запуска, что обеспечит возможность проверки и допустимость в суде. Доступ к системе должен быть строго ограничен для уполномоченных сотрудников органов досудебного расследования и осуществляться через защищенные облачные решения (SaaS), что повысит безопасность и масштабируемость интеллектуальной транспортной экосистемы [8].

Следовательно, эффективная организация расследования преступлений на воздушном и железнодорожном транспорте требует не просто внедрения отдельных технологий, а создания целостной, юридически легитимной и технически прозрачной ИИ-платформы, которая станет неотъемлемым инструментом в арсенале казахстанских правоохранительных органов.

Подводя итог, можно сделать вывод о формирующейся сегодня институциональной и нормативной базы для перехода к интеллектуальной модели транспортной безопасности. Внедрение систем искусственного интеллекта позволит существенно повысить оперативность расследования, обеспечить более качественное сохранение доказательственной информации, автоматизировать анализ больших массивов данных и сформировать единый межведомственный механизм реагирования на транспортные происшествия и преступления.

1. Конституция Республики Казахстан (принята 30 августа 1995 года) // https://adilet.zan.kz/rus/docs/K950001000_. Дата обращения 14.05.2026г.
2. Уголовно-процессуальный кодекс Республики Казахстан от 4 июля 2014 года № 231-V (с изменениями от 08.03.2026 г.) // https://prg.kz/document/?doc_id=31575852. Дата обращения 14.05.2026г.
3. Закон Республики Казахстан от 24 ноября 2015 года № 418-V «Об информатизации» (с изменениями от 18.01.2026 г.) // https://prg.kz/document/?doc_id=33885902. Дата обращения 14.05.2026г.
4. Закон Республики Казахстан от 17 ноября 2025 года № 230-VIII «Об искусственном интеллекте» // Ведомости Парламента Республики Казахстан. — 2025. — № 21-22 (2928).
5. В Министерстве транспорта Республики Казахстан подведены итоги 2025 года по вопросам расследования происшествий и инцидентов на воздушном, железнодорожном и водном транспорте // https://www.gov.kz/memleket/entities/transport/press/news/details/1159851?lang=ru. Дата обращения 14.05.2026г.
6. **Stavroulakis P.J., Prousaloglou P., Alexandraki N.** An AI-guided accident investigation protocol based on the 2023 Tempi train crash // NEXRES. — 2026. — № 8. — P. 1-16.
7. **Rybkina A.M., Korobitsyna E.S., Demidova P.M., Shobairi S.O.R.** Artificial intelligence to assess the prospects of developing sites within the boundaries of roadsides and railway security zones // AIP Conference Proceedings. — 2023. — № 2943. — P. 050038.
8. **Drozdova M., Benin A.** RETRACTED: Cloud solutions as a trend of safe intelligent transport ecosystem development // E3S Web of Conferences. — 2024. — № 549. — P. 08001.

ЖАҢА БУЫН АВТОМОБИЛЬДЕРІНІҢ ҚАУІПСІЗДІГІНЕ ҚАРСЫ ТРАНСШЕКАРАЛЫҚ ҚЫЛМЫСТАР: КИБЕР ОСАЛДЫҚТАР, ДӘЛЕЛДЕМЕЛЕРДІҢ КРИМИНАЛИСТИКАСЫ ЖӘНЕ ҚАЗАҚСТАН РЕСПУБЛИКАСЫНДАҒЫ ҚЫЛМЫСТЫҚ ЖАУАПТЫЛЫҚ МӘСЕЛЕЛЕРІ

ЗАЙНУЛДИН Ерасыл Серікұлы
Қазақстан Республикасы Бас прокуратурасының жанындағы Құқық қорғау органдары академиясы, Қосшы

Мақалада жаңа буын автомобильдерін басқарудың электрондық жүйелерін қашықтан бұзу арқылы жасалған трансшекаралық қылмыстық құқық бұзушылықтар зерттеледі. Шетелдік шолуларда жүйеленген техникалық осалдықтарды (RKE, PKES, Bluetooth, GPS, CAN-шина сымсыз хаттамалары) талдау негізінде құқықтық проблемалардың үш тобы анықталды: Қазақстан Республикасының Қылмыстық кодексінде киберфизикалық бұзуды қамтитын қылмыстың арнайы құрамының болмауы; таратылған шабуыл инфрақұрылымы кезіндегі трансшекаралық элементтің белгісіздігі; сандық іздерді алудың криминалистикалық әдістерінің тапшылығы (SDR-құрылғылар, CAN-логтар, Bluetooth-адаптерлер). ҚР ҚК 194-1-бабын енгізу, Көлік құралының электрондық жүйелеріне заңсыз қашықтан қол жеткізу бойынша ұсыныстар тұжырымдалған. Нәтижелер заң шығарушы мен тергеу тәжірибесіне бағытталған.

Қазіргі кезеңдегі қоғамдық даму цифрландыру үдерістерімен және жасанды интеллект технологияларының жедел таралуымен тығыз байланысты. Соңғы бірнеше жыл ішінде көлік саласы да дәстүрлі механикалық жүйеден күрделі цифрлық инфрақұрылымға айнала бастады. Әсіресе жаңа буын автомобильдері электрондық басқару модульдеріне, сымсыз байланыс арналарына және автоматтандырылған басқару элементтеріне тәуелді болып отыр. Мұндай өзгерістер көлік қауіпсіздігіне қатысты тәуекелдердің де сипатын өзгертті.

Қазақстанда цифрлық технологияларды дамыту мемлекеттік саясаттың маңызды бағыттарының біріне айналды. 2026 жылдың «Цифрландыру және жасанды интеллект жылы» болып жариялануы осы үрдістің маңызын көрсетеді [1]. Мемлекеттік деңгейде платформалық экономика, деректерді өңдеу, жасанды интеллект элементтерін енгізу және «ақылды» инфрақұрылымды қалыптастыру бағытында бірқатар бағдарламалар қабылданды [2]. Соның ішінде көлік саласын цифрландыруға ерекше назар аударылып келеді.

Қазіргі автомобильдер бұрынғыдай тек қозғалыс құралы ретінде қарастырылмайды. Олар GPS, Bluetooth, Wi-Fi, PKES, RKE және CAN-шина секілді технологиялар арқылы сыртқы ортамен тұрақты байланыста жұмыс істейтін күрделі киберфизикалық жүйеге айналды [3]. Мұндай жүйелер жүргізушіге ыңғайлылық береді, алайда бір мезгілде жаңа қылмыстық қауіптерді де қалыптастырады. Соңғы жылдары шетелдік тәжірибеде көліктерді қашықтан бұзу, сигналды ұстап қалу, relay attack шабуылдары және электрондық жүйелерге заңсыз араласу жағдайлары жиілеп отыр [3].

Р. Гестейра-Миньярро және бірлескен авторларының жүргізген талдау қазіргі автомобильдердің шабуылға ұшырау деңгейі жоғары екенін көрсетеді [3].

Әсіресе сымсыз байланыс арналары арқылы жасалатын шабуылдар көлік қауіпсіздігіне тікелей қатер туғызады. Кейбір жағдайларда шабуылдаушылар автомобильді ашып қана қоймай, қозғалтқышты іске қосып, көлікті толық басқаруға мүмкіндік алады. Мұндай әрекеттердің қауіптілігі қарапайым мүліктік қылмыстардан әлдеқайда жоғары.

Проблеманың тағы бір маңызды қыры оның трансшекаралық сипат алуында. Қылмыстық әрекетті ұйымдастырушы басқа мемлекет аумағында орналасуы мүмкін, ал шабуыл интернет немесе делдал серверлер арқылы іске асырылады. Көлік бір елде бұзылып, кейін басқа мемлекеттің аумағына шығарылуы ықтимал. Осындай жағдайда қылмыстың жасалу орны, юрисдикция мәселесі және дәлелдемелерді жинау тәртібі күрделене түседі.

Қазақстан Республикасының қолданыстағы қылмыстық заңнамасы мұндай қауіптерді толық көлемде қамтып отырған жоқ [4]. Компьютерлік ақпаратқа заңсыз қол жеткізуге қатысты нормалар бар болғанымен, автомобильдің электрондық жүйесіне қашықтан араласу ерекшеліктері нақты көрсетілмеген. Соның салдарынан киберфизикалық шабуылдарға құқықтық баға беру кезінде бірқатар қиындықтар туындайды.

Сондықтан жаңа буын автомобильдеріне қатысты кибершабуылдарды тек техникалық мәселе ретінде қарастыру жеткіліксіз. Бұл қылмыстық құқық, криминалистика және цифрлық қауіпсіздік салаларының түйіскен жерінде тұрған күрделі мәселе болып саналады. Қазіргі жағдайда мұндай құқықбұзушылықтарға қарсы тиімді құқықтық және криминалистикалық тетіктер қалыптастыру ерекше өзектілікке ие.

Шетелдік тәжірибе көрсеткендей, автомобильдердің электрондық жүйелеріне бағытталған кибершабуылдар жыл сайын күрделене түсуде. Бұрын мұндай әрекеттер жекелеген техникалық тәжірибелер деңгейінде қарастырылса, қазіргі жағдайда олар ұйымдасқан қылмыстық схемалардың бір бөлігіне айналып отыр. Әсіресе қашықтан басқару элементтері бар көліктер қылмыстық топтар үшін ыңғайлы нысанаға айналғаны байқалады.

Автомобильге заңсыз қол жеткізудің кең таралған тәсілдерінің бірі RKE және PKES жүйелеріне жасалатын шабуылдар болып саналады [3]. RKE жүйесі көлікті қашықтан ашуға арналған болса, PKES технологиясы жүргізуші кілтті қалтасынан шығармай-ақ қозғалтқышты іске қосуға мүмкіндік береді. Практикада дәл осы ыңғайлылық қауіпсіздік деңгейін әлсіретіп отыр. Relay attack әдісі кезінде шабуылдаушылар кілттен шығатын сигналды күшейтіп, оны автомобильге жеткізеді [3]. Соның нәтижесінде жүйе кілт иесі көліктің жанында тұр деп қабылдайды.

Мұндай шабуылдардың қауіптілігі олардың із қалдыру деңгейінің төмен болуымен де байланысты. Көп жағдайда көлік иесі жүйенің бұзылғанын бірден байқамайды. Кейбір жағдайларда көлік кәдімгі заңды кілт арқылы ашылғандай көрінеді. Тергеу барысында дәл осы ерекшелік үлкен қиындық туғызады, себебі классикалық автокөлік ұрлау белгілері анықталмайды.

CAN-шинаға қатысты шабуылдар одан да қауіпті саналады. CAN жүйесі автомобильдің негізгі электрондық модульдерін өзара байланыстырады. Тежеу жүйесі, қозғалтқыш, қауіпсіздік жастықтары және жарықтандыру элементтері

осы арна арқылы басқарылады. Егер шабуылдаушы CAN-шинаға қол жеткізсе, автомобильдің жекелеген функцияларын толық басқару мүмкіндігі пайда болады. Соңғы жылдары фаралар немесе мультимедиялық жүйелер арқылы CAN-инъекция жасау фактілері халықаралық сараптамаларда бірнеше рет көрсетілді [3].

Проблеманың күрделілігі техникалық қауіпсіздікпен ғана шектелмейді. Мұндай әрекеттердің құқықтық табиғаты да бірқатар даулы мәселелер туғызады. Қазақстан Республикасының Қылмыстық кодексінде компьютерлік ақпаратқа заңсыз қол жеткізуге қатысты баптар болғанымен, көліктің электрондық жүйесіне киберфизикалық араласу мәселесі нақты бөлінбеген. Соның салдарынан құқық қорғау органдары әрекетті саралау кезінде әртүрлі нормаларды қатар қолдануға мәжбүр болады.

Тағы бір маңызды мәселе қылмыстың трансшекаралық сипатымен байланысты. Қазіргі жағдайда шабуылды ұйымдастырушы бір мемлекетте орналасып, сервер екінші елде жұмыс істеуі мүмкін, ал көлік үшінші мемлекеттің аумағында бұзылады [5]. Мұндай схема халықаралық ынтымақтастық мәселесін алдыңғы қатарға шығарады. Әсіресе цифрлық дәлелдемелерді алу кезінде юрисдикциялық қайшылықтар жиі кездеседі.

Криминалистикалық тұрғыдан алғанда да қиындықтар аз емес. Қарапайым тергеу әдістері мұндай қылмыстарды толық ашуға жеткіліксіз болып отыр. SDR-құрылғылар, Bluetooth адаптерлері, CAN-логтар және радиожиілік құралдары арқылы алынатын цифрлық іздер арнайы техникалық дайындықты талап етеді. Сондықтан қазіргі жағдайда автомобиль киберқауіпсіздігі саласындағы мамандандырылған сараптамаларды дамыту қажеттілігі айқын байқалады.

Жаңа буын көліктеріне қатысты кибершабуылдар тек IT саласының мәселесі емес. Олар ұлттық қауіпсіздікке, көлік инфрақұрылымына және азаматтардың жеке қауіпсіздігіне тікелей әсер ететін күрделі құқықтық проблемаға айналып келеді.

Қазіргі кезеңде автомобильдерді қашықтан бұзу тек техникалық осалдықтарды пайдалану деңгейінде қалып отырған жоқ. Мұндай шабуылдар біртіндеп ұйымдасқан қылмыстық қызметтің жаңа бағытына айналып келеді. Әсіресе трансшекаралық сипаттағы қылмыстарда электрондық жүйелерге заңсыз араласу көлік ұрлау, бопсалау және диверсиялық әрекеттермен қатар қолданылуда.

Халықаралық тәжірибеде relay attack тәсілі ең жиі кездесетін әдістердің бірі ретінде қарастырылады. Бұл жағдайда шабуылдаушылардың бірі көлік иесіне жақындап, смарт-кілт сигналын ұстап алады, ал екінші тұлға сол сигналды автомобильге жеткізеді. Бір қарағанда қарапайым көрінетін бұл әдіс қазіргі қауіпсіздік жүйелерінің әлсіз тұстарын анық байқатады. Көптеген автомобиль өндірушілері соңғы жылдары дәл осы проблемаға байланысты бағдарламалық жаңартулар енгізуге мәжбүр болды.

Кейбір жағдайларда шабуыл бұдан да күрделі схема бойынша жүзеге асырылады. Мысалы, басқару сигналы VPN сервистері немесе жасырын серверлер арқылы бірнеше мемлекет аумағы арқылы берілуі мүмкін. Тергеу барысында мұндай цифрлық маршрутты анықтау айтарлықтай уақыт пен

техникалық ресурстарды талап етеді. Соның салдарынан құқық қорғау органдары үшін қылмыстың нақты ұйымдастырушысын анықтау қиынға соғады [6].

Қазақстан заңнамасында трансшекаралық киберқылмыстарға қатысты жалпы нормалар болғанымен, автомобильдердің электрондық жүйесіне қатысты арнайы құқықтық механизм қалыптаспаған. Қолданыстағы баптар көбіне компьютерлік ақпаратты қорғауға бағытталған. Алайда көлік құралы тек ақпараттық объект емес. Ол адамның өмірі мен денсаулығына тікелей қауіп төндіретін техникалық жүйе болып саналады.

Мәселен, CAN-шина арқылы тежегіш жүйесіне немесе рульдік басқаруға араласу жол-көлік оқиғасына әкелуі мүмкін. Мұндай жағдайда әрекет тек ақпараттық қауіпсіздік шеңберінде бағаланбауы тиіс. Себебі ықтимал салдар мүліктік зиянмен шектелмейді. Адам өлімі немесе ауыр дене жарақаты сияқты зардаптар да туындауы ықтимал.

Осыған байланысты жаңа құқықтық тәсіл қажет екені байқалады. Автомобильдің электрондық жүйесіне заңсыз қашықтан қол жеткізу әрекетін дербес қылмыстық құрам ретінде қарастыру мәселесі барған сайын өзекті болып отыр. Әсіресе шабуыл көлікті иелену мақсатында немесе қозғалыс қауіпсіздігіне қатер төндіру үшін жасалған жағдайда жауапкершілікті күшейту қажеттілігі анық сезіледі.

Шетелдік құқықтық тәжірибеде мұндай бағыттағы алғашқы қадамдар байқалады. Кейбір мемлекеттер көлік құралдарының компьютерлік жүйесіне заңсыз араласуды жеке құқықбұзушылық ретінде қарастыра бастады. Дегенмен көптеген елдерде бұл мәселе әлі де толық шешілген жоқ. Сондықтан Қазақстан үшін халықаралық тәжірибені механикалық көшіруден гөрі, ұлттық құқықтық жүйеге бейімделген модель қалыптастыру маңыздырақ.

Криминалистика саласында да жаңа тәсілдер қажет. Бұрын автокөлік ұрлау кезінде негізгі дәлел ретінде механикалық іздер қарастырылса, қазіргі жағдайда басты рөлді цифрлық ақпарат атқарады. Радиожиілік құрылғыларынан алынған деректер, лог-файлдар, телематикалық жүйелердегі жазбалар және Bluetooth байланыстары тергеу үшін маңызды дәлел көзіне айналып отыр.

Осындай өзгерістер құқық қорғау органдарының техникалық мүмкіндіктерін жаңартуды талап етеді. Автомобиль киберқауіпсіздігі саласындағы мамандарды даярлау, арнайы сараптамалық бөлімдерді дамыту және халықаралық деңгейдегі ақпарат алмасуды күшейту қазіргі кезеңдегі негізгі міндеттердің біріне айналып келеді.

Қазіргі жағдайда автомобильдердің электрондық жүйелеріне қарсы жасалатын шабуылдарды дәстүрлі автокөлік қылмыстарының қарапайым жалғасы ретінде бағалау жеткіліксіз. Мұндай әрекеттердің ерекшелігі олардың физикалық және цифрлық кеңістікті қатар қамтуында. Бір жағынан қылмыс нақты көлік құралына бағытталады, екінші жағынан шабуыл ақпараттық-телекоммуникациялық желілер арқылы жүзеге асырылады. Дәл осы аралас сипат құқықтық реттеуде көптеген қайшылықтардың пайда болуына әсер етеді.

Қазақстан Республикасының Қылмыстық кодексінде көлік ұрлау, ақпараттық жүйелерге заңсыз қол жеткізу және қозғалыс қауіпсіздігін бұзу

бойынша нормалар бар. Бірақ жаңа буын автомобильдеріне қатысты кибершабуылдар бұл құрамдардың ешқайсысына толық сәйкес келмейді. Мысалы, шабуылдаушы көлік жүйесіне заңсыз кіргенімен, автомобильді алып кетпеуі мүмкін. Кей жағдайда негізгі мақсат көлік жүйесін бақылауға алу немесе оның жұмысын уақытша бұзу болуы ықтимал.

Осындай жағдайларда құқықтық бағалау күрделене түседі. Егер шабуыл физикалық бұзусыз жүзеге асырылса, классикалық ұрлық белгілері толық байқалмайды. Ал компьютерлік ақпаратқа қатысты баптар автомобильдің киберфизикалық табиғатын толық ескермейді. Соның салдарынан құқық қолдану тәжірибесінде құқықтық вакуум қалыптасады.

Проблеманың тағы бір маңызды жағы дәлелдемелерді жинау мәселесімен байланысты. Дәстүрлі қылмыстарда заттай айғақтар басты рөл атқарса, автомобиль кибершабуылдарында цифрлық іздер негізгі дәлел көзіне айналады. Бұл жерде тергеушілер тек құқықтық біліммен шектелмейді. Радиожиілік талдау, телематика, бағдарламалық логтарды өңдеу және желілік белсенділікті анықтау сияқты техникалық бағыттар да қажет болады.

Практика көрсеткендей, көптеген құқық қорғау органдары мұндай істерге толық дайын емес. Тергеу барысында кейде SDR-құрылғылар немесе сигнал күшейткіштер тәркіленгенімен, олардың нақты қолданылу механизмі дәлелденбей қалады. Себебі арнайы сараптамалық әдістемелер әлі жеткілікті деңгейде қалыптаспаған. Әсіресе relay attack немесе CAN-инъекция жағдайларында шабуыл тізбегін толық қалпына келтіру күрделі процесс болып саналады.

Халықаралық деңгейде де бұл мәселе толық шешілген жоқ. БҰҰ-ның R155 және R156 стандарттары өндірушілерге киберқауіпсіздік жүйесін енгізу міндетін жүктейді [6]. Дегенмен аталған құжаттар негізінен техникалық қауіпсіздікке бағытталған. Қылмыстық жауапкершілік мәселесі онда нақты қарастырылмайды. Сондықтан мемлекеттердің көпшілігі ұлттық құқықтық механизмдерді өз бетінше қалыптастыруға мәжбүр.

Қазақстан үшін бұл бағыттың маңыздылығы бірнеше фактормен түсіндіріледі. Біріншіден, елде көлік инфрақұрылымының цифрлануы белсенді жүріп жатыр. Екіншіден, смарт-қала элементтері мен интеллектуалды көлік жүйелері кезең-кезеңімен енгізілуде. Үшіншіден, халықаралық көлік дәліздерінің дамуы трансшекаралық қауіптердің ықтималдығын арттырады.

Осыған байланысты қылмыстық заңнамаға арнайы норма енгізу қажеттілігі айқын көрінеді. Автомобильдің электрондық жүйесіне заңсыз қашықтан қол жеткізу әрекетін жеке құқықбұзушылық ретінде бекіту құқықтық анықтылықты күшейтер еді. Сонымен қатар мұндай норма тергеу тәжірибесін біріздендіруге және құқық қорғау органдарының жұмысын жеңілдетуге мүмкіндік береді.

Автомобиль киберқауіпсіздігі саласындағы қылмыстар алдағы жылдары одан әрі күрделене түсетіні байқалады. Сондықтан алдын алу шараларын, техникалық бақылауды және криминалистикалық әдістерді қатар дамыту қазіргі кезеңдегі басты бағыттардың біріне айналып отыр.

Жаңа буын автомобильдеріне қатысты кибершабуылдар мәселесі тек техникалық қауіпсіздік шеңберімен шектелмейтіні анық байқалады. Мұндай

әрекеттер қазіргі қылмыстылықтың трансформацияланып жатқанын көрсетеді. Бұрын көлік құралын заңсыз иелену көбіне физикалық бұзу немесе механикалық құралдарды қолдану арқылы жүзеге асырылса, қазіргі жағдайда шабуыл бағдарламалық және радиожиілік технологиялар арқылы іске асырылуда.

Жүргізілген талдау автомобильдердің электрондық жүйелері құқықтық тұрғыдан жеткілікті деңгейде қорғалмағанын көрсетті. Әсіресе қашықтан араласу, relay attack, CAN-инъекция және цифрлық басқару элементтеріне заңсыз қол жеткізу сияқты әрекеттерге қатысты нақты құқықтық тетік толық қалыптаспаған. Қолданыстағы нормалар жекелеген элементтерді ғана қамтиды, алайда киберфизикалық шабуылдардың кешенді табиғатын толық ашпайды.

Автомобильдерді қашықтан бұзудың қауіптілігі олардың ықтимал салдарымен де түсіндіріледі. Кей жағдайда шабуыл мүліктік зиянмен ғана шектеледі. Бірақ электрондық жүйеге араласу жол қозғалысы қауіпсіздігіне тікелей әсер етуі мүмкін. Тежеу жүйесінің істен шығуы, рульдік басқаруға ықпал ету немесе көлік қозғалысын қашықтан бақылау адам өміріне нақты қауіп төндіреді. Сондықтан мұндай әрекеттерді тек ақпараттық құқықбұзушылық ретінде бағалау жеткіліксіз.

Трансшекаралық сипат бұл мәселені одан әрі күрделендіреді. Қазіргі цифрлық ортада шабуыл бірнеше мемлекеттің аумағын қатар қамтуы мүмкін. Басқарушы сервер басқа елде орналасады, сигнал үшінші мемлекет арқылы беріледі, ал көлік Қазақстан аумағында бұзылады. Мұндай жағдай халықаралық құқықтық көмек, юрисдикция және цифрлық дәлелдемелерді алу мәселелерін алдыңғы қатарға шығарады.

Криминалистикалық тұрғыдан алғанда да жаңа тәсілдер қажет екені анықталды. Автомобиль кибершабуылдарын тергеу барысында классикалық әдістер жеткіліксіз болып отыр. SDR-құрылғылар, Bluetooth адаптерлері, телематикалық логтар және радиожиілік құралдары бойынша арнайы сараптамалар жүргізу қажеттілігі күшейіп келеді. Бұл бағытта техникалық мамандар мен құқық қорғау органдары арасындағы өзара байланысты нығайту маңызды рөл атқарады.

Осыған байланысты Қазақстан Республикасының қылмыстық заңнамасын одан әрі жетілдіру қажеттілігі байқалады. Атап айтқанда, көлік құралының электрондық жүйелеріне заңсыз қашықтан қол жеткізуге қатысты дербес қылмыстық-құқықтық норманы енгізу мәселесін қарастыру орынды болып көрінеді. Мұндай норма шартты түрде ҚР ҚК-нің 194-1-бабы ретінде «Көлік құралының электрондық жүйелеріне заңсыз қашықтан қол жеткізу» атауымен бекітілуі мүмкін.

Ұсынылатын бапта киберфизикалық араласудың әртүрлі нысандары ескерілуі тиіс. Атап айтқанда, құқықбұзушылықтың салдарсыз жасалған түрлері бөлек, ал көлік құралын заңсыз иеленуге, жол-көлік оқиғасына, адамның денсаулығына зиян келтіруге немесе өлімге әкеп соққан әрекеттер ауырлатылған құрам ретінде қарастырылғаны жөн.

Сонымен қатар трансшекаралық сипаттағы шабуылдарға қатысты біліктілік белгілерін нақтылау маңызды. Егер құқықбұзушылық ақпараттық-телекоммуникациялық желілерді, шетелдік серверлерді немесе халықаралық

байланыс инфрақұрылымын пайдалану арқылы жасалса, мұндай мән-жай қылмыстық жауаптылықты күшейтетін белгі ретінде бағалануы мүмкін.

Қазіргі жағдайда автомобильдердің электрондық жүйелеріне қатысты шабуылдарды тергеу үшін арнайы криминалистикалық әдістемелер де қажет. Осыған байланысты SDR-құрылғыларды, радиожиілік құралдарын, OBD-II адаптерлерін және телематикалық деректерді алу мен зерттеу тәртібін регламенттейтін әдістемелік ұсынымдарды әзірлеу тәжірибелік маңызға ие.

Мақаланы дайындау кезінде мәтіннің жеке бөліктерін тілдік және стилистикалық өңдеуге арналған жасанды интеллект құралдары қолданылды. Ғылыми талдауды, заңды қорытындыларды және қорытынды редакцияны автор өз бетінше орындады.

1. Қазақстан Республикасы Президентінің № 1151 «Цифрландыру және жасанды интеллект жылын жариялау туралы» 2026 жылғы 6 қаңтардағы Жарлығы // https://adilet.zan.kz/kaz/docs/U2600001151 (жүктелген күні 2026 ж.01.05.)
2. Мемлекет басшысы Қасым-Жомарт Тоқаевтың 2025 жылғы 8 қыркүйектегі «Жасанды интеллект дәуіріндегі Қазақстан: өзекті мәселелер және оны түбегейлі цифрлық өзгерістер арқылы шешу» Қазақстан халқына Жолдауы // https://adilet.zan.kz/kaz/docs/K25002025_1 (жүктелген күні 2026 ж.01.05.)
3. **Gesteira-Miñarro R., López G., Palacios R.** Revisiting Wireless Cyberattacks on Vehicles // Sensors. – 2025. – Vol. 25, No. 8. – P. 1-15. –2605 p. – DOI: 10.3390/s25082605.
4. Қазақстан Республикасының Қылмыстық кодексі 2014 жылғы 3 шілдедегі № 226-V ҚРЗ. // https://adilet.zan.kz/kaz/docs/K1400000226 (жүктелген күні 2026 ж.01.05.)
5. **UN Regulation No.** 155 – Cyber security and cyber security management system; UN Regulation No. 156 – Software update and software update management system. UNECE, 2021. // https://unece.org/transport/documents/2021/03/standards/un-regulation-no-155-cyber-security-and-cyber-security (жүктелген күні 2026 ж.01.05.)
6. **Checkoway S., McCoy D., Kantor B.,** et al. Comprehensive Experimental Analyses of Automotive Attack Surfaces // Proceedings of the 20th USENIX Security Symposium. San Francisco, 2011. –P. 6–12.

ЖАЛҒАН АҚПАРАТТЫ ТАРАТҚАНЫ ҮШІН ҚЫЛМЫСТЫҚ ЖАУАПТЫЛЫҚТЫҢ ШЕГІ

КАДРИН Тілеген Берекеұлы
«Bolashaq» Академиясы, Қазақстан, Қарағанды

Мақалада интернет кеңістігінде жалған және дәйексіз ақпарат таратқаны үшін қылмыстық жауаптылықтың құқықтық шектері жан-жақты қарастырылады. Ақпараттық технологиялардың қарқынды дамуы, әлеуметтік желілер мен мессенджерлердің кең таралуы қоғамда тексерілмеген, шындыққа сәйкес келмейтін мәліметтердің көбеюіне алып келді. Мұндай ақпараттар қоғамдық қауіпсіздікке, азаматтардың құқықтары мен бостандықтарына, сондай-ақ мемлекеттік институттарға деген сенімге елеулі қауіп төндіреді. Әсіресе төтенше жағдайлар, саяси оқиғалар немесе әлеуметтік мәселелер кезінде жалған ақпараттың таралуы қоғам арасында дүрбелең туғызып, әлеуметтік тұрақтылыққа кері әсер етеді.

Автор Қазақстан Республикасының Қылмыстық кодексінің 274-бабына құқықтық талдау жасап, қолданыстағы заңнаманың негізгі кемшіліктерін анықтайды. Атап айтқанда, «жалған ақпарат» ұғымының нақты құқықтық анықтамасының болмауы, қасақана және абайсызда жасалған әрекеттердің өзара ажыратылмауы, құқық қолдану тәжірибесінде түрлі түсінбеушіліктердің туындауына себеп болатыны көрсетіледі.

Сонымен қатар мақалада «жалған ақпарат» пен «дәйексіз ақпарат» ұғымдарына салыстырмалы құқықтық талдау жүргізіліп, олардың мазмұны мен құқықтық табиғатындағы айырмашылықтар айқындалады. Шетелдік мемлекеттердің заңнамалық тәжірибелері де қарастырылып, халықаралық құқықтық тәсілдермен салыстыру жасалады. Автор интернетте дәйексіз ақпарат таратқаны үшін жауаптылықты нақтылайтын ҚР ҚК-не 274-1 жаңа бабын енгізуді ұсынады. Ұсынылған норма жауапкершілікті әрекеттің ниеті мен салдарына қарай саралауға мүмкіндік беріп, сөз бостандығы мен қоғамдық қауіпсіздік арасындағы тепе-теңдікті сақтауға бағытталған.

Кіріспе

Цифрлық технологиялардың дамуы интернет желісінде таралатын ақпарат көлемінің едәуір артуына алып келді. Сонымен қатар, жекелеген азаматтарға да, жалпы қоғамға да зиян келтіруі мүмкін жалған мәліметтер мәселесі туындады. Қазіргі жағдайда жалған немесе шындыққа сәйкес келмейтін ақпарат таратқаны үшін қылмыстық жауапкершіліктің шекарасын нақты айқындап, азаматтардың құқықтарын қорғауды және құқықтық тәртіпті сақтауды қамтамасыз ететін заңнамалық тетіктерді әзірлеу қажет.

Мемлекет басшысы Қасым-Жомарт Тоқаев ақпараттың аса қуатты құрал екенін, сондықтан оның таралуы жан-жақты талданып, тексеріліп, сенімді болуы тиіс екенін атап өткен [1]. Азаматтарды жаңылыстыруға жол берілмеуі керек, сонымен қатар сөз бостандығы елде болып жатқан барлық жағдайды негізсіз сынау құқығын білдірмейді; бұқаралық ақпарат құралдары қоғам бірлігін нығайтуға ықпал етуі тиіс.

Жұмыстың мақсаты: интернетте жалған ақпарат таратқаны үшін қылмыстық жауапкершіліктің нақты шекараларын белгілеуге бағытталған заңнамалық бастама әзірлеу.

Мәселе және оны шешу жолдары

Қазіргі уақытта Қазақстан Республикасы заңнамасы жалған ақпарат таратқаны үшін жауапкершілікті ҚР Қылмыстық кодексінің 274-бабы арқылы реттейді, алайда келесі кемшіліктер байқалады:

- «Жалған ақпарат» дегеннің нақты анықтамасы жоқ.
- Қасақана және абайсызда жасалған әрекеттердің ара жігі ажыратылмаған.
- Әлеуметтік желілер мен мессенджерлер арқылы жалған ақпарат таратуға қатысты жауапкершілік жеткілікті деңгейде реттелмеген.

Шешу жолдары:

- Интернеттегі анық емес (дұрыс емес) ақпаратты анықтаудың нақты критерийлерін енгізу.
- Салдарына байланысты әкімшілік және қылмыстық жауапкершілікті ажырату.
- Интернет-платформалар мен медиа қолданушыларының әрекеттерін реттейтін арнайы нормалар енгізу.
- Онлайн түрде жалған ақпарат таратқаны үшін жауапкершілікті нақтылайтын жаңа бап енгізу арқылы ҚР Қылмыстық кодексіне өзгерістер әзірлеу.

Заңнамалық реттеу бойынша ұсыныстар

Интернетте жалған ақпарат тарату әлеуметтік қақтығыстарға әкелуі мүмкін, мемлекеттік институттарға деген сенімді әлсіретеді және азаматтарға материалдық немесе моральдық зиян келтіреді [2]; [3]. Халықаралық тәжірибе (БҰҰ, Еуропа Кеңесі) жауапкершілікті ниет (қасақаналық) дәрежесі мен салдардың ауырлығына қарай саралау реттеудің тиімділігін арттырып, адам құқықтарын қорғауға мүмкіндік беретінін көрсетеді [4]; [5]. Дұрыс емес ақпаратты анықтаудың ашық әрі нақты критерийлері сөз бостандығы мен қоғамды қорғау арасындағы тепе-теңдікті сақтауға ықпал етеді [6]; [7].

Қазіргі қоғамда ақпарат әл-ауқат пен саяси биліктің негізгі ресурсы болып табылады. М.Кастельстің пікірінше, желілік қоғамдағы билік — коммуникациялық билік [8, 72], бұл ақпарат таратқаны үшін жауапкершілікті саралап қараудың маңыздылығын көрсетеді. Абсолютті тыйым сөз бостандығын шамадан тыс шектеуге және қоғамдық игілікке зиян келтіруге әкелуі мүмкін. Сондықтан заңнамада ниет пен ақпараттың шынайылық деңгейі ескерілуі тиіс, бұл ұсынылып отырған 274-1-баптың балама нұсқасында қарастырылғандай, қоғамды қорғау мен азаматтардың құқықтары арасындағы тепе-теңдікті қамтамасыз етеді.

Осыған байланысты ақпарат таратуды абсолютті түрде тыйым салу сөз бостандығын шамадан тыс шектеп, қоғамдық игілікке нұқсан келтіруі мүмкін. Сондықтан заңнама ақпарат таратқаны үшін жауапкершілікті ниет пен ақпараттың шынайылық деңгейін ескере отырып саралауы тиіс. Бұл азаматтардың құқықтары мен қоғам мүддесін қорғауды қамтамасыз етіп, пікір білдіру еркіндігін бұзбауға мүмкіндік береді.

Заңнаманы өзгерту жобасы

Қазақстан Республикасының Қылмыстық кодексіне жаңа бап енгізу ұсынылады:

274-1-бап. Интернетте дәйексіз ақпарат тарату

Қоғамдық қауіпсіздікке, азаматтардың немесе ұйымдардың құқықтары мен заңды мүдделеріне қауіп төндіруі мүмкін, шындыққа әдейі сәйкес келмейтін мәліметтерді (дәйексіз ақпаратты) қасақана немесе өрескел абайсыздық салдарынан тарату ғана қылмыстық жауаптылыққа жатады.

1. Дәйексіз ақпаратты абайсызда таратқаны үшін кінәлі тұлға:

•ескерту;

• ең төменгі мөлшердегі айыппұл салуға;

• таратылған ақпаратты түзету немесе оны теріске шығару міндетіне тартылады.

2.Егер әрекет елеулі салдарға әкелсе (жаппай тәртіп бұзушылық, ірі экономикалық шығын, денсаулыққа зиян), жаза 3 жылға дейін бас бостандығынан айыруға дейін күшейтілуі мүмкін.

Ұсынылып отырған **274-1-бап** қолданыстағы **ҚР ҚК 274-бабынан** («жалған ақпарат тарату») түбегейлі ерекшеленеді. Іс жүзінде интернетте ақпарат тарату кейде әдейі жалған мәлімет түрінде де, дәйексіз ақпарат түрінде де болуы мүмкін, ал көбінесе заңмен қорғалатын мүдделерге зиян келтіру ниеті болмайды. Жаңа норма қасақана және абайсызда тарату әрекеттерін ажыратуға бағытталған, бұл қылмыстық-құқықтық жауапкершілікті неғұрлым әділ әрі гумандық етуге мүмкіндік береді.

Ұсынылып отырған норманың негізгі айырмашылығы — «жалған ақпарат» терминінің орнына «дәйексіз ақпарат» ұғымын енгізу, бұл қасақана және абайсызда тарату жағдайларын нақты ажыратуға мүмкіндік береді.

Жалған ақпарат — бұл алушыны алдау немесе жаңылыстыру мақсатында әдейі жасалатын немесе таратылатын мәліметтер. Яғни мұнда негізгі элемент — автордың қасақаналығы (ниеті).

Сипаттамалық белгілері:

•Мақсаттылық: ақпарат алдау мақсатымен таратылады.

Фактілерді бұрмалау: деректер толығымен ойдан шығарылуы немесе қатты бұрмалануы мүмкін.

Мысалдар: фейк жаңалықтар, әдейі таралатын өсек-аяңдар, манипуляциялық мемдер.

Мысал: «Вакцина жазылмайтын ауру тудырады» деген хабарлама, ал медициналық зерттеулер мұны жоққа шығарады және бұл ақпарат әдейі дүрбелең тудыру мақсатында таратылады.

Дәйексіз ақпарат - бұл шындыққа сәйкес келмейтін мәліметтер, бірақ олар міндетті түрде алдау мақсатында таратылмайды. Ақпарат көзі құзыретсіз болуы мүмкін, мәлімет ескірген болуы мүмкін немесе қате түсіндірілген болуы ықтимал.

Сипаттамалық белгілері:

•Ниеттің болмауы: адам оған өзі сеніп, қателесіп таратуы мүмкін.

Қателер немесе дәлсіздіктер: деректер ішінара дұрыс болуы мүмкін, бірақ жалпы мазмұны қате.

Мысалдар: ескірген статистикалық деректер, ғылыми нәтижелерді қате түсіндіру, қателік салдарынан пайда болған өсек-аяңдар.

Мысал: журналист жаңартылмаған ескі есепке сүйеніп, науқастар саны туралы мәлімет жариялады — бұл дәйексіз, бірақ әдейі жалған емес ақпарат.

«Жалған және дәйексіз ақпарат» терминдеріне салыстырмалы талдау

Жалған ақпарат — бұл алдау немесе жаңылыстыру мақсатында әдейі жасалатын немесе таратылатын мәліметтер. Оның негізгі белгілері — мақсаттылық және фактілерді бұрмалау. Мысалдар: фейк жаңалықтар, үгіт-насихат материалдары.

Дәйексіз ақпарат — шындыққа сәйкес келмейтін, бірақ міндетті түрде алдау ниетінсіз таратылатын мәліметтер. Ол қателіктер, ескірген деректер немесе дұрыс емес түсіндіру салдарынан пайда болуы мүмкін. Мысалдар: ескірген статистикалық деректер, ғылыми нәтижелерді қате түсіндіру.

Салыстырмалы талдау:

Сипаттамасы	Жалған ақпарат	Дәйексіз ақпарат
Автордың ойы	Бар (әдейі алдау)	Жоқ (қате, надандық)
Фактілерге сәйкестік	Сәйкес емес	Сәйкес емес
Мысалдар	Жалған жаңалықтар, насихат	Қате Статистика
Салдары	Жалған ақпарат, манипуляция	Олар адастыруы мүмкін, бірақ жаман ниетсіз
Жауапкершілік	Жоғары құқықтық және этикалық	Жағдайларға байланысты аз болуы мүмкін

Ниет: жалған ақпаратта болады, дәйексіз ақпаратта болмайды.

Фактілерге сәйкестігі: екеуі де шындыққа сәйкес келмейді.

Салдары: жалған ақпарат дезинформация мен манипуляцияға әкеледі; дәйексіз ақпарат зиянды ниетсіз жаңылыстыруға себеп болады.

Жауапкершілік: жалған ақпарат үшін құқықтық және этикалық жауапкершілік жоғары.

Қорытынды: жалған ақпарат әрқашан дәйексіз болады, бірақ дәйексіз ақпарат әрқашан жалған бола бермейді.

Жобаның ғылыми негіздемесі:

Айта кету керек, ұсынылып отырған бап ниет пен салдарды ескереді, бұл негізсіз жазалау қаупін азайтады. Норманың қолданылу аясын тек интернет кеңістігімен шектейді. Сондай-ақ құқықтық реттеудің тиімділігін арттырып, азаматтардың құқықтарын қорғайды.

Бастаманы практикалық іске асыру

Осылайша, ұсынылып отырған бап келесі қажеттіліктерді қарастырады:

-Ақпаратты мониторинг жүргізетін органдар үшін әдістемелік ұсынымдар әзірлеу.

-ҚР ҚК-нің жаңа нормалары туралы азаматтар мен БАҚ арасында ақпараттық-түсіндіру жұмыстарын жүргізу.

-Ақпараттың дәйектілігін бағалау бойынша заңгерлер мен құқық қорғау органдары қызметкерлеріне арналған оқыту бағдарламаларын енгізу.

Ғылыми жоба бойынша қорытындылар

Заңнамалық бастама интернетте дәйексіз ақпарат таратқаны үшін жауапкершілікті нақтылайды және ҚР Қылмыстық кодексін 274-1-баппен толықтырады.

Ниет пен салдарға қарай жауапкершілікті саралау қылмыстық жазаны әрекеттің ауырлығы мен кінә дәрежесіне сәйкес қолдануға мүмкіндік береді.

Нақтылай түскен нормалар әлеуметтік қақтығыстардың азаюына, мемлекеттік институттарға деген сенімнің артуына және азаматтардың құқықтарын қорғауға ықпал етеді.

Ұсынылатын өзгерістер:

- ҚР ҚК-не 274-1 жаңа бапты енгізу;
- дәйексіз ақпаратты анықтау критерийлерін бекіту;
- әкімшілік және қылмыстық жауапкершілікті ажырату;
- ауырлататын мән-жайларды және жаппай тарату үшін жауапкершілікті нақтылау.

1. **Тоқаев Қ.Ж.** Ақпарат – қуатты құрал… [Мәтін] / Қ.Ж. Тоқаев. – Қазақстан Республикасы Президентінің ресми сайты, 2022. – Қолжетімділік режимі: https://www.akorda.kz/…Қаралған күні: 13.05.2026.
2. Қазақстан Республикасының Қылмыстық кодексі. – Алматы: Norma, 2023. [Электрондық ресурс]. – Қолжетімділік режимі:https://adilet.zan.kz [Қаралған күні: 12.05.2026].
3. **Қонышева М.А**. Интернеттегі жалған мәліметтер үшін ақпараттық қауіпсіздік және қылмыстық жауапкершілік. – Алматы: ЭКЦ, 2022.
4. OECD Digital Economy Papers. Online Misinformation and Policy Responses. – Paris, 2021.
5. UNESCO. Freedom of Expression and Digital Platforms. – Paris, 2020.
6. Совет Европы. Recommendations on the Regulation of Online Content. – Strasbourg, 2021.
7. Закон Республики Казахстан «ОСМИ и массовой информации». – Алматы, 2021. [Электронный ресурс]. – Режим доступа: https://adilet.zan.kz [Дата обращения: 12.05.2026].
8. **Кастельс М.** Власть коммуникации / пер. с англ. Н. М. Тылевич ; под науч. ред. А. И. Черных. М.: Изд. дом Высшей школы экономики, 2016. 564 с.

ОТВЕТСТВЕННОСТЬ ЗА СБЫТ И ПОТРЕБЛЕНИЕ НАРКОТИЧЕСКИХ СРЕДСТВ: ПРОБЛЕМЫ И ПУТИ РЕШЕНИЯ

ПРИМКУЛОВА Алмагуль Алматовна
Костанайская академия МВД РК имени Шракбека Кабылбаева
РК, г.Костанай

В статье обосновывается необходимость декриминализации деяний, связанных с незаконным приобретением и хранением наркотических средств без цели сбыта, в контексте трансформации уголовной политики Казахстана. Анализ действующей редакции статьи 296 УК РК выявляет ее неэффективность: размывание границы между потребителем и сбытчиком, высокая социальная стоимость судимости для лиц с зависимостью, перегрузка правоохранительной системы и правоприменительные проблемы при доказывании «общественного места». С опорой на статистические данные (высокий процент прекращения дел и фактическое неприменение части 1 ст. 296 УК) и международные практики (опыт Грузии, стран Балтии и постсоветского пространства) доказывается, что репрессивная модель не достигает цели снижения наркотизации. Предлагается вернуться к исторически апробированной административной модели ответственности, что позволит сфокусировать ресурсы на борьбе с организованным наркотрафиком и развитии системы медицинской и социальной реабилитации.

Современная уголовно-правовая политика в сфере противодействия незаконному обороту наркотических средств и психотропных веществ находится в состоянии глубокого переосмысления. Модель, десятилетиями строившаяся на жесткой репрессии и последовательной криминализации конечного потребителя, сегодня демонстрирует свою неэффективность. Стратегические цели - снижение уровня наркотизации населения, минимизация социального ущерба, рациональное распределение бюджетных средств - оказываются недостижимыми в рамках карательного подхода. В связи с этим ключевое значение приобретает вопрос о принципиальном разграничении ответственности за коммерческий сбыт и за немедицинское потребление наркотиков. Речь идет не о смягчении «ради смягчения», а о назревшей необходимости трансформации самого подхода: выведение потребителя из сферы уголовного преследования с переводом соответствующих деяний в разряд административных правонарушений. Это направление уже стало общемировым трендом, и Казахстан здесь не исключение.

Действующая редакция статьи 296 Уголовного кодекса Республики Казахстан объединяет в себе два разнородных деяния - сбыт и приобретение либо хранение для личного употребления, устанавливая за них единую уголовную ответственность [1]. Такая конструкция порождает целый ряд системных проблем, которые невозможно разрешить точечными изменениями.

Прежде всего, уголовный закон в равной степени охраняет два разных объекта: общественную безопасность - когда речь идет о сбыте, и здоровье населения - когда речь идет о потреблении. В правовом государстве, признающем высокую степень автономии личности, защита человека от него

самого едва ли может рассматриваться как оправданное основание для применения уголовной репрессии. Криминализация саморазрушительного поведения, не создающего прямой угрозы третьим лицам, представляет собой избыточное вторжение государства в частную жизнь и входит в противоречие с принципом «ultimaratio» - использованием уголовного права лишь в качестве крайней меры [2].

Далее, «Лицо» - осужденное по частям первой или второй статьи 296 УК РК, даже если наказание не связано с лишением свободы, приобретает статус судимого. Формально судимость считается инструментом исправления, по факту же она становится пожизненным социальным клеймом. Непреодолимые барьеры при трудоустройстве, невозможность получить образовательный кредит, ограничения в реализации избирательных и иных гражданских прав - всё это не способствует ресоциализации, а напротив, консервирует маргинальный статус личности. Государство, декларирующее цель исправления, на деле производит социальную эксклюзию, провоцируя дальнейшую девиантную и нередко криминальную карьеру.

Не менее значим и организационно - управленческий аспект. Расследование и судебное рассмотрение дел о хранении без цели сбыта поглощает колоссальный объем ресурсов следственного аппарата, прокуратуры и судов. Вместо того чтобы сконцентрировать усилия на противодействии организованным формам наркопреступности - сбыте, транзите, подпольном производстве, представляющих реальную угрозу национальной безопасности, - правоохранительная система вынуждена перерабатывать массивы дел, общественная опасность которых минимальна либо вовсе отсутствует.

Наконец, самый тревожный эффект существующей модели заключается в том, что угроза уголовного преследования формирует у потребителей устойчивое избегание контактов с медицинскими и социальными службами. Раннее выявление зависимости становится невозможным, программы профилактики и снижения вреда остаются невостребованными, а в макромасштабе это оборачивается ростом заболеваемости ВИЧ, вирусными гепатитами и иными социально значимыми инфекциями. Общественные издержки в таком сценарии многократно превышают гипотетический эффект от репрессивных мер.

В этой связи чрезвычайно показателен опыт государств постсоветского пространства, которые уже прошли или проходят схожий этап переосмысления уголовной политики.

Российская Федерация сохраняет уголовную ответственность за хранение без цели сбыта, однако Федеральным законом № 420-ФЗ была введена возможность освобождения от ответственности при добровольной выдаче наркотических средств и активном содействии раскрытию преступлений. Кроме того, ключевую роль в дифференциации играет институт значительного, крупного и особо крупного размера. Это модель частичной, условной декриминализации, построенной на процессуальном компромиссе.

Украина также исходит из уголовной наказуемости хранения для личного употребления, однако судебная практика последних лет, в том числе позиция

Верховного Суда, выраженная в 2018 году, фактически выводит из-под удара незначительные количества, хранимые без цели сбыта. Сформирован судебный механизм, позволяющий не признавать такие действия преступлением при отсутствии общественно опасных последствий.

Республика Беларусь традиционно демонстрирует жесткий подход, однако и здесь правоприменительная практика активно использует условное осуждение и меры, не связанные с изоляцией от общества. Уголовный кодекс формально сохраняет запрет, но индивидуализация наказания позволяет избегать наиболее репрессивных санкций.

Армения и Кыргызстан при сохранении уголовной ответственности за хранение предусматривают возможность освобождения от наказания либо смягчения мер при незначительных размерах. Одновременно усиливается роль лечебных и реабилитационных программ.

Молдова формально относит хранение к уголовно наказуемым деяниям, однако при малозначительности содеянного активно применяются административные санкции либо освобождение от уголовной ответственности.

Литва, Латвия и Эстония последовательно реализуют модель двойного регулирования: незначительные количества для личного употребления влекут административную ответственность, превышение установленных порогов либо наличие цели сбыта - уголовную.

Наиболее радикальная и последовательная реформа проведена **в Грузии**. Решениями Конституционного Суда в 2015 - 2018 годах уголовная ответственность за потребление наркотических средств была признана неконституционной. Сегодня потребление и хранение для личного использования квалифицируются как административные правонарушения и влекут штраф либо общественные работы. Борьба со сбытом и организованным наркобизнесом при этом не ослаблена, а напротив, выведена на принципиально иной уровень за счет перераспределения ресурсов [3].

Таким образом, прослеживается отчетливая конвергентная тенденция. Государства, объединенные общим правовым прошлым, двигаются в одном направлении: уголовная репрессия сохраняется как инструмент противодействия коммерческому обороту и организованной преступности, в то время как потребление и сопутствующее ему хранение без цели сбыта либо полностью декриминализируются, либо смягчаются до административных составов, либо обрастают механизмами, позволяющими избегать судимости и реального лишения свободы.

С позиции правовой доктрины происходящее имеет под собой фундаментальное обоснование. Современное понимание уголовного права исходит из презумпции личной автономии и ответственности дееспособного индивида. Государственное принуждение в его наиболее жесткой, уголовно-правовой форме допустимо лишь тогда, когда поведение лица причиняет вред другим субъектам либо создает реальную угрозу причинения такого вреда. Этот принцип, восходящий еще к идеям **Джона Стюарта Милля,** остается актуальным и сегодня [2].

Приобретение и хранение наркотических средств для личного употребления при отсутствии цели сбыта относится к поведению, затрагивающему преимущественно самого субъекта. Оно асоциально, оно не одобряется, оно может и должно влечь негативную правовую оценку. Но применение за него именно уголовного наказания, влекущего судимость и весь сопутствующий комплекс ограничений, представляется чрезмерным, несоразмерным и этически уязвимым вмешательством. По своему характеру и степени общественной опасности такое деяние сопоставимо с административными правонарушениями, а не с преступлениями. Более того, аналогия с потреблением алкоголя или табака здесь вполне уместна: саморазрушительное поведение само по себе никогда не рассматривалось законодателем как основание для криминализации.

Перевод рассматриваемых деяний в разряд административных правонарушений позволяет сохранить официальную отрицательную оценку со стороны государства, но исключает наиболее тяжелые социальные последствия в виде судимости и маргинализации личности. Одновременно соблюдается принцип соразмерности: санкция должна соответствовать реальной опасности деяния.

Наряду с доктринальными аргументами существуют и сугубо прагматические, управленческие.

Выведение дел о потреблении наркотиков из уголовного производства в административное способно кардинально разгрузить органы дознания, следствия, прокуратуру и суды. Освобождающиеся кадровые, временные и финансовые ресурсы могут и должны быть перенаправлены на противодействие транснациональномунаркотрафику, ликвидацию подпольных лабораторий, пресечение деятельности организованных сбытовых сетей. Именно эти направления представляют действительную угрозу национальной безопасности, именно здесь уголовная репрессия оправдана и необходима.

Кроме того, декриминализация потребления - действенный механизм оптимизации пенитенциарной системы. Сокращение числа лиц, направляемых в учреждения уголовно-исполнительной системы за деяния, не связанные со сбытом, уменьшит бюджетные расходы на их содержание, позволит улучшить условия отбывания наказания осужденными за тяжкие и особо тяжкие преступления, повысит эффективность ресоциализационных программ. Ресурсы колоний и тюрем перестанут расходоваться на тех, кто не представляет общественной опасности.

Нельзя обойти вниманием и антикоррупционный потенциал такой реформы. Сужение уголовно-правового запрета, его четкая формализация, ориентация исключительно на коммерческий оборот наркотиков объективно сокращают объем дискреционных полномочий правоприменителя. Это, в свою очередь, уменьшает пространство для злоупотреблений, связанных с провокациями преступлений, фабрикацией доказательств, искусственным переквалификацией деяний. Чем меньше размытость границ между преступным и непреступным, тем ниже коррупционные риски.

И наконец, самое важное - стратегическое измерение.

Ключевым результатом реформы должен стать переход от преимущественно карательной модели реагирования к политике, ориентированной на предупреждение, лечение и восстановление. Освободившиеся финансовые средства и организационные ресурсы целесообразно реинвестировать в развитие наркологической службы, развертывание амбулаторных и стационарных программ помощи зависимым, расширение программ заместительной терапии и снижения вреда, реализацию масштабных профилактических проектов среди уязвимых групп населения.

Устранение угрозы уголовного преследования разрушает тот самый барьер, который сегодня отделяет потребителя от системы здравоохранения. Перестав быть фигурой, скрывающейся от правосудия, человек получает возможность легально и безопасно обращаться за медицинской помощью. Раннее выявление зависимости становится реальным, эффективность лечебно-реабилитационных мероприятий возрастает многократно.

Тем самым фокус государственной политики смещается с преследования жертвы на противодействие преступному бизнесу. Долгосрочная эффективность борьбы с наркопреступностью определяется не количеством осужденных потребителей, а способностью государства воздействовать на финансовые потоки, логистические цепочки, организационные структуры преступных сообществ. Перенастройка оперативно-розыскной и следственной деятельности на решение этих стратегических задач позволяет сформировать принципиально иную, более рациональную и социально ориентированную модель уголовной политики.

В ходе подготовки исследования проведён анализ официальных статистических данных, который показал следующее [4].

1 Динамика регистрации и прекращения дел

год	Зарегистрировано	Прекращено по реабилит	Доля прекращенных
2020	4602	2322	50,5%
2022	3241	2250	69,4%
2023	3194	2050	64,2%
2024	3372	1650	48,9%
2025	2993	1348	45,0%
1 кв. 2026	818	198	24,2%

Значительная часть зарегистрированных дел (до 70 % в отдельные годы) прекращается по реабилитирующим основаниям, что указывает на отсутствие достаточных доказательств или малозначительность деяний. Уголовное преследование в таких случаях является избыточным [4].

2 Осуждённые по частям 1 и 2 ст. 296 УК РК

год	Осужд. по ч.1	Осужд. по ч.2	Всего осуждено
2020	539	2588	3 127
2021	157	2131	2 288
2022	59	1652	1 711
2023	33	1717	1 750
2024	7	1852	1 859

2025	11	1862	1 873
1 кв. 2026	1	545	546

По части 1 статьи 296 УК РК – осуждение сократилось с 539 (2020) до единичных случаев (1–11) в 2024–2026 гг. Норма фактически **не применяется** и является «**недействующей**» с точки зрения уголовного правосудия.

По части 2 статьи 296 УК РК – ежегодно осуждается стабильно более 1 500 лиц. При этом данные деяния связаны, как правило, с потреблением или хранением без цели сбыта и не представляют высокой общественной опасности.

Таким образом, криминологические данные за последние пять лет неумолимо свидетельствуют: уголовное преследование по частям 1 и 2 статьи 296 УК РК не решает задачи снижения наркотизации, но при этом ежегодно криминализирует тысячи граждан, перегружает правоохранительную систему и размывает грань между реальной угрозой обществу (сбытом) и социальным недугом (потреблением).

Изложенное позволяет утверждать, что декриминализация приобретения и хранения наркотических средств для личного употребления с одновременным сохранением и даже усилением уголовной ответственности за сбыт и организованные формы наркопреступности - не уступка либеральным веяниям, а прагматичный, научно обоснованный и подтвержденный опытом зарубежных государств подход. Это путь к снижению уровня криминализации населения, оздоровлению социальной атмосферы, рациональному использованию ресурсов государства и, в конечном счете, к более эффективной защите, как общественной безопасности, так и здоровья граждан.

Представляется целесообразным исключить из Уголовного кодекса Республики Казахстан ответственность за незаконные приобретение, хранение, перевозку, изготовление, переработку наркотических средств или психотропных веществ без цели сбыта, то есть полностью вывести составы, предусмотренные частями 1 и 2 статьи 296 УК РК, из сферы уголовного преследования.

Одновременно с этим указанные деяния должны быть перенесены в Кодекс Республики Казахстан об административных правонарушениях с сохранением негативной правовой оценки, но в более мягком, соразмерном режиме юридической ответственности.

Важно подчеркнуть, что предлагаемая мера не является разрывом с отечественной правовой традицией. Напротив, она восстанавливает исторически оправданный подход, уже апробированный в казахстанском законодательстве.

В период действия Кодекса Республики Казахстан об административных правонарушениях от 30 января 2001 года статья 320 устанавливала административную ответственность за незаконные приобретение, хранение, потребление наркотических средств или психотропных веществ без назначения врача [5]. Указанная норма действовала на протяжении ряда лет, и практика ее применения не свидетельствовала о росте наркопотребления либо об ослаблении антинаркотической политики. Напротив, именно в этот период была выстроена действенная система профилактики, а правоприменительные органы имели возможность концентрировать усилия на борьбе со сбытом.

Таким образом, возвращение к административно-правовой модели реагирования на немедицинское потребление и сопутствующее хранение является не революционным нововведением, а восстановлением ранее существовавшего, доказавшего свою работоспособность правового механизма.

1. Уголовный кодекс Республики Казахстан: Закон Республики Казахстан от 3 июля 2014 года № 226-V (с изм. и доп. по состоянию на 2026 год).
2. Милль Дж. С. О свободе / Дж. С. Милль; пер. с англ. – London, 1859. – Гл. 1 (О границах власти общества над личностью).
3. Информация о решении Конституционного суда Грузии от июня 2020 года по иску НПО «Белый шум» и «Ассоциации молодых юристов Грузии» // Sputnik Грузия, 06.06.2020. – URL: https://sputnik-georgia.ru (дата обращения: 18.05.2026).
4. Комитет по правовой статистике и специальным учетам Генеральной прокуратуры Республики Казахстан. Официальные статистические данные о состоянии преступности за 2020–2026 годы. – URL: http://pravstat.prokuror.kz (дата обращения: 18.05.2026).
5. Кодекс Республики Казахстан об административных правонарушениях: Закон Республики Казахстан от 30 января 2001 года № 155-II (утратил силу).

ЦИФРОВИЗАЦИЯ В УСЛОВИЯХ РАЗВИТИЯ КИБЕРПРЕСТУПНОСТИ: УГОЛОВНО-ПРАВОВЫЕ И КРИМИНОЛОГИЧЕСКИЕ АСПЕКТЫ

САГИМБАЕВА Мөлдір Қадырбекқызы
Костанайская академия МВД РК имени Шракбека Кабылбаева, г.Костанай

В данной статье исследуются современные процессы цифровизации общества и их влияние на развитие киберпреступности как одной из наиболее опасных форм транснациональной преступности. Рассматриваются уголовно-правовые и криминологические аспекты преступлений, совершаемых с использованием информационно-коммуникационных технологий. Особое внимание уделяется причинам увеличения количества киберпреступлений, характеристике личности киберпреступника, а также проблемам квалификации противоправных деяний в цифровой среде. Кроме того, анализируются современные угрозы, возникающие в результате развития искусственного интеллекта, цифровых платформ, электронных платежных систем и интернет-коммуникаций. В статье отмечается, что стремительное развитие цифровых технологий значительно опережает совершенствование законодательства и практики правоохранительных органов, вследствие чего возникают дополнительные сложности в предупреждении, раскрытии и расследовании киберпреступлений. Автор приходит к выводу о необходимости комплексного подхода к противодействию преступности в цифровой сфере, включающего международное сотрудничество, повышение цифровой грамотности населения и совершенствование механизмов кибербезопасности.

На современном этапе развития общества цифровизация затрагивает практически все сферы жизнедеятельности человека. Следует отметить, что внедрение цифровых технологий способствует ускорению экономических процессов, совершенствованию государственного управления, а также развитию образования, медицины и финансовой системы. Вместе с тем наряду с положительными изменениями цифровая трансформация общества порождает и определенные негативные последствия, связанные прежде всего с ростом преступности в информационном пространстве [1].

В настоящее время киберпреступность по праву считается одной из наиболее быстро развивающихся форм преступной деятельности. Прежде всего это связано с тем, что использование современных цифровых технологий позволяет преступникам совершать противоправные деяния дистанционно, анонимно и нередко за пределами одного государства. Более того, активное распространение сети Интернет, электронных платежных систем, социальных сетей и технологий искусственного интеллекта значительно расширяет возможности преступной деятельности [2].

Необходимо подчеркнуть, что проблема противодействия киберпреступности приобретает особую актуальность именно в условиях глобальной цифровизации. Это объясняется тем, что традиционные механизмы

уголовно-правового регулирования не всегда способны эффективно противостоять преступлениям нового поколения.

Следует обратить внимание на то, что в современной научной литературе отсутствует единый подход к определению понятия «киберпреступность». Однако большинство исследователей рассматривают киберпреступность как совокупность преступлений, совершаемых с использованием компьютерных технологий, информационных систем и сети Интернет [3].

Киберпреступность обладает рядом характерных признаков. В частности, к ним относятся использование информационно-коммуникационных технологий, высокая степень латентности, транснациональный характер, сложность установления личности преступника, а также возможность дистанционного совершения преступления. Кроме того, одной из особенностей киберпреступности является постоянная адаптация преступников к новым технологическим условиям. Так, развитие искусственного интеллекта, технологий deepfake, криптовалют и облачных сервисов способствует возникновению новых форм преступной деятельности [4].

В современных условиях киберпреступления условно можно разделить на несколько основных категорий. К ним относятся преступления против компьютерной информации, мошенничество с использованием цифровых технологий, кража персональных данных, кибертерроризм, распространение вредоносного программного обеспечения, незаконный доступ к информационным системам, а также финансовые преступления в цифровой среде.

Как показывает криминологический анализ, цифровизация существенно изменила структуру современной преступности. Иными словами, виртуальное пространство фактически стало новой средой совершения преступлений, а интернет — инструментом реализации преступных намерений [5].

По мнению исследователей, основными детерминантами киберпреступности являются массовая цифровизация общества, недостаточный уровень цифровой грамотности населения, слабая защищенность информационных систем, высокий уровень анонимности в сети Интернет, экономическая выгода киберпреступлений и несовершенство международного сотрудничества.

Особое внимание в криминологической науке уделяется личности киберпреступника. В отличие от традиционной преступности субъектами киберпреступлений зачастую становятся лица с высоким уровнем интеллектуального развития, обладающие специальными техническими знаниями. При этом преступления могут совершаться как индивидуально, так и организованными преступными группами [6].

Следует также отметить, что значительная часть киберпреступлений носит транснациональный характер. Иначе говоря, преступник может находиться на территории одного государства, использовать серверы другого государства и причинять вред гражданам третьих стран. Безусловно, это существенно осложняет расследование и привлечение виновных лиц к уголовной ответственности.

Кроме того, одной из наиболее серьезных проблем остается высокая латентность киберпреступности. На практике многие потерпевшие не обращаются в правоохранительные органы вследствие недоверия к эффективности расследования либо невозможности установить преступника.

Развитие цифровых технологий, безусловно, требует постоянного совершенствования уголовного законодательства. Вместе с тем традиционные нормы уголовного права зачастую не учитывают специфику преступлений, совершаемых в киберпространстве [7].

На сегодняшний день уголовное законодательство большинства государств предусматривает ответственность за неправомерный доступ к компьютерной информации, создание и распространение вредоносных программ, нарушение функционирования информационных систем, мошенничество с использованием электронных средств и незаконный оборот персональных данных.

Однако, как показывает практика, преступники достаточно быстро адаптируются к новым условиям, используя современные технологии для обхода существующих механизмов правового контроля.

Серьезные трудности вызывает и процесс сбора цифровых доказательств. Дело в том, что электронная информация может быть быстро уничтожена, изменена либо скрыта при помощи специальных программ. В связи с этим возрастает значение цифровой криминалистики и специальных методов расследования.

Важно подчеркнуть, что одним из ключевых направлений совершенствования уголовного законодательства является международное сотрудничество. Поскольку киберпреступность не ограничивается государственными границами, эффективная борьба с ней возможна исключительно при взаимодействии правоохранительных органов различных государств.

В современных условиях наблюдается устойчивая тенденция к увеличению количества преступлений, совершаемых с использованием цифровых технологий. Следует отметить, что киберпреступность развивается значительно быстрее по сравнению с традиционными формами преступной деятельности. Это обусловлено высокой скоростью распространения цифровых технологий, доступностью сети Интернет и возможностью анонимного взаимодействия пользователей в виртуальном пространстве [4].

Особую опасность представляет тот факт, что современные киберпреступления отличаются высоким уровнем организованности и технической подготовки преступников. В настоящее время злоумышленники активно используют вредоносное программное обеспечение, фишинговые сайты, технологии подмены данных, а также средства скрытия цифровых следов. Кроме того, распространение криптовалют значительно осложняет контроль за незаконными финансовыми операциями и способствует легализации преступных доходов.

В последние годы наблюдается увеличение количества преступлений, связанных с незаконным использованием персональных данных граждан. Утечка конфиденциальной информации может повлечь серьезные последствия как для

отдельных лиц, так и для государственных и коммерческих организаций. Использование похищенных данных позволяет преступникам осуществлять мошеннические действия, получать незаконный доступ к банковским счетам и совершать иные противоправные деяния [6].

Следует также обратить внимание на рост преступлений, совершаемых в отношении несовершеннолетних в цифровой среде. Социальные сети, мессенджеры и игровые платформы нередко используются злоумышленниками для вовлечения подростков в противоправную деятельность, распространения запрещенной информации и психологического воздействия. В связи с этим особую актуальность приобретает проблема обеспечения безопасности несовершеннолетних пользователей сети Интернет.

Расследование преступлений, совершаемых в цифровом пространстве, представляет собой сложный и многоэтапный процесс. Одной из основных проблем является сложность установления личности преступника. Использование анонимных сетей, VPN-сервисов, поддельных IP-адресов и специальных программ позволяет злоумышленникам скрывать свое местонахождение и затрудняет деятельность правоохранительных органов [5].

Кроме того, расследование киберпреступлений осложняется высокой скоростью уничтожения цифровых следов. Электронные данные могут быть удалены либо изменены за короткий промежуток времени, вследствие чего правоохранительные органы должны оперативно реагировать на поступающую информацию о преступлении.

Существенную проблему представляет и недостаточный уровень технического оснащения отдельных правоохранительных подразделений. В условиях постоянного развития цифровых технологий возникает необходимость использования современного программного обеспечения, специализированного оборудования и методов анализа цифровой информации. При этом эффективность расследования напрямую зависит от уровня профессиональной подготовки сотрудников, осуществляющих борьбу с киберпреступностью [7].

Следует подчеркнуть, что значительная часть цифровых преступлений совершается с использованием зарубежных интернет-ресурсов и серверов, расположенных за пределами государства. В результате этого получение необходимой информации требует длительных международных запросов, что существенно замедляет процесс расследования.

В современных условиях стремительное развитие искусственного интеллекта оказывает существенное влияние на характер киберпреступности. С одной стороны, технологии искусственного интеллекта активно используются для обеспечения информационной безопасности, выявления подозрительной активности и предотвращения кибератак. С другой стороны, данные технологии могут применяться преступниками для автоматизации противоправной деятельности [8].

Одной из наиболее опасных тенденций является использование технологий deepfake. Создание поддельных видеозаписей, аудиоматериалов и изображений позволяет злоумышленникам осуществлять мошенничество, дискредитацию личности, распространение ложной информации и шантаж. При этом развитие

нейросетевых технологий делает подобные материалы все более реалистичными, что существенно осложняет их выявление.

Кроме того, искусственный интеллект может использоваться для автоматизированного подбора паролей, анализа больших объемов персональных данных и создания вредоносного программного обеспечения. Вследствие этого возникает необходимость совершенствования механизмов правового регулирования использования технологий искусственного интеллекта и разработки дополнительных мер защиты информационной безопасности [10].

Одним из наиболее эффективных направлений противодействия киберпреступности является ее предупреждение. Криминологическая профилактика включает систему мер, направленных на выявление и устранение причин и условий, способствующих совершению преступлений в цифровой среде [9].

Прежде всего важную роль играет повышение уровня цифровой грамотности населения. Многие пользователи сети Интернет недостаточно осведомлены о правилах информационной безопасности, вследствие чего становятся жертвами мошенников и иных злоумышленников. В связи с этим особое значение приобретают образовательные программы, направленные на формирование навыков безопасного использования цифровых технологий.

Не менее важным направлением профилактики является совершенствование технической защиты информационных систем. Использование современных антивирусных программ, систем шифрования данных, двухфакторной аутентификации и средств мониторинга киберугроз позволяет значительно снизить риск совершения преступлений.

Кроме того, важное значение имеет взаимодействие государства, правоохранительных органов, образовательных учреждений и частного сектора. Только комплексный подход к обеспечению цифровой безопасности способен обеспечить эффективное противодействие современным киберугрозам [1].

Таким образом, можно сделать вывод о том, что цифровизация общества оказывает существенное влияние как на современную преступность, так и на правовую систему в целом. Развитие информационных технологий способствует возникновению новых форм преступной деятельности, что, в свою очередь, требует адаптации уголовного законодательства и дальнейшего развития криминологической науки.

Следовательно, киберпреступность характеризуется высокой латентностью, транснациональностью и технологической сложностью, что существенно затрудняет деятельность правоохранительных органов. В условиях стремительного развития цифровых технологий особую актуальность приобретают вопросы совершенствования уголовно-правовых механизмов противодействия киберпреступности и разработки эффективных профилактических мер.

Подводя итог, необходимо отметить, что в условиях стремительного развития цифровых технологий проблема противодействия киберпреступности приобретает особую значимость для обеспечения стабильности правовой системы и общественной безопасности. Современная преступность активно

адаптируется к цифровой среде, используя новые технологические возможности для совершения противоправных деяний, что требует формирования принципиально новых механизмов защиты общества и государства [7].

Важным условием эффективного противодействия киберугрозам является формирование устойчивой государственной политики в сфере цифровой безопасности. Такая политика должна быть направлена не только на реагирование на уже совершенные преступления, но и на предупреждение потенциальных угроз в информационном пространстве. В современных условиях особую актуальность приобретает создание единой системы мониторинга цифровых рисков, позволяющей своевременно выявлять уязвимости информационных систем и предотвращать возможные кибератаки [5].

Необходимо учитывать, что цифровая среда постоянно изменяется, вследствие чего появляются новые способы совершения преступлений. Распространение облачных технологий, электронных сервисов, виртуальных платформ и автоматизированных систем обработки информации существенно расширяет возможности злоумышленников. В связи с этим государственным органам требуется постоянное совершенствование механизмов защиты информации и адаптация правоприменительной практики к современным цифровым условиям [8].

Особую роль в обеспечении кибербезопасности играет кадровое обеспечение данной сферы. Для эффективной борьбы с преступностью в цифровом пространстве необходимы высококвалифицированные специалисты, обладающие знаниями как в области права, так и в сфере информационных технологий. Подготовка таких специалистов должна осуществляться на системной основе с учетом современных тенденций развития цифровой преступности. Кроме того, важное значение имеет регулярное повышение квалификации сотрудников правоохранительных органов, поскольку технологии, используемые преступниками, постоянно совершенствуются [6].

Следует также подчеркнуть значение взаимодействия государства с частным сектором. Крупные технологические компании, банковские организации, операторы связи и владельцы цифровых платформ обладают значительными объемами информации о потенциальных угрозах и техническими возможностями для выявления противоправной активности. Эффективное сотрудничество между государственными структурами и частными организациями способствует повышению уровня защиты информационной инфраструктуры и более оперативному реагированию на киберинциденты [3].

Кроме того, в современных условиях возрастает значение международной координации в сфере борьбы с киберпреступностью. Глобальный характер цифровой среды приводит к тому, что преступные действия могут одновременно затрагивать интересы нескольких государств. Вследствие этого особую важность приобретает разработка единых международных стандартов информационной безопасности, унификация правовых механизмов

расследования киберпреступлений и развитие совместных программ по противодействию цифровым угрозам [2].

Таким образом, обеспечение безопасности в цифровом пространстве представляет собой одну из ключевых задач современного государства. Эффективное противодействие киберпреступности возможно только при условии комплексного сочетания правовых, технических, организационных и профилактических мер, направленных на защиту личности, общества и государства от угроз, возникающих в условиях глобальной цифровизации [1].

1. **Майоров М.А., Кузнецова Л.А.** Киберпреступность: понятие, признаки и виды // Социальное управление. 2024.
2. **Апухтина А.О.** Киберпреступность: правовые проблемы в условиях цифровизации // Молодой ученый. 2024. № 43.
3. **Атакулов Б.** Понятие киберпреступлений и необходимость их расследования // Общество и инновации. 2024.
4. **Иманмадиев Д.М., Раймбекова Ж.Е.** Уголовно-правовые механизмы обеспечения кибербезопасности в Республике Казахстан // Вестник Alikhan Bokeikhan University. 2025.
5. **Кувшинов А.Н.** О некоторых криминологических и уголовно-правовых аспектах противодействия киберпреступности // Евразийская адвокатура. 2025.
6. **Кудайбергенов Д.С.** и др. Киберпреступность: понятие, виды и способы противодействия // Theoretical Hypotheses and Empirical Results. 2025.
7. **Жанибеков А.К., Ермухамедов А.Б.** Ответственность за преступления, совершенные с применением цифровых технологий // Universal Science Perspectives. 2025.
8. **Волков С.С.** Проблемы квалификации экономических преступлений, совершаемых в киберпространстве // Police Activities. 2026.
9. **Серебренникова А.В.** Противодействие киберпреступности: актуальные вопросы // Пробелы в российском законодательстве. 2023.
10. **Перина А.С.** «Цифровые преступления»: понятие, типология, признаки // Юридический вестник Самарского университета. 2024.

ЗАҢДЫЛЫҚ ПЕН ҚҰҚЫҚТЫҚ ТӘРТІПТІ ҚАМТАМАСЫЗ ЕТУ САЛАСЫНДА ЖАСАНДЫ ИНТЕЛЛЕКТТІҢ ТЕХНОЛОГИЯЛЫҚ ЖҮЙЕЛЕРІН ПАЙДАЛАНУДЫҢ ӨЗЕКТІ МӘСЕЛЕЛЕРІ

САГИНБАЕВА Аружан Уайсқызы
Қазақстан Республикасы ІІМ М.Бөкенбаев атындағы Ақтөбе заң институты кәсіби даярлық факультетінің оқытушы – әдіскері, полиция аға лейтенанты, Ақтөбе қ-сы

Мақалада заңдылық пен құқықтық тәртіпті қамтамасыз ету саласында жасанды интеллекттің технологиялық жүйелерін қолданудың өзекті мүмкіндіктері қарастырылған. Автор халықаралық деңгейде ақпараттық-іздестіру, анықтамалық жүйелерді, сондай-ақ құқық қорғау органдары қызметкерлерінің уақытша және еңбек ресурстарын оңтайландыратын мәліметтер базасы мен криминалистикалық алгоритмдерді кеңінен құру және пайдалану қажеттілігі туралы қорытындыға келді. Ғылыми мақалада жасанды интеллекттің коммуникативтік жүйелерінің тиімділігі, сенімділігі және болжамдылығы критерийлері егжей-тегжейлі талданды, сондай-ақ отандық және шетелдік заңнаманы жетілдіру бойынша ұсыныстар айтылды.

Қазіргі уақытта отандық құқықтық ғылым мен құқық қорғау органдары қызметінің айрықша ерекшелігі цифрландыру мәселелеріне жан-жақты қызығушылық таныту және қазіргі заманғы қылмысқа қарсы іс-қимыл мақсатында динамикалық өзгеріп отыратын жасанды интеллект мүмкіндіктерінің кең спектрін қолдану болып табылады. Біз көрсеткен жағдай мемлекет жүргізіп жатқан ішкі және сыртқы саясат саласындағы реформалық өзгерістерге тікелей байланысты. Жоғарыда аталған оқиғалар дағдарыстық күйлердің көріністерінің және қоғамдық өмірдің белгілі бір салаларында жекелеген геосаяси қауіптердің туындауының тікелей катализаторы болды, бұл өз кезегінде стратегиялық маңызды мемлекеттік бағыттарды қорғауды қамтамасыз етудің, оның ішінде жасанды интеллект жүйелерін қолданумен қамтамасыз етудің ең жаңа жоғары тиімді тетіктерін әзірлеудің шұғыл қажеттілігін көрсете алмайды. *Қазақстан Республикасының президенті Қ.К.Тоқаев қоғамдық кеңістіктегі жасанды интеллекттің рөліне бірнеше рет назар аударды, «азаматтар үшін жасанды интеллектті енгізу - бұл өмірдің жаңа сапасы және кәсіби қызмет үшін жаңа мүмкіндіктер, оның дамуындағы барлық адамзаттың алға жылжуының негізі» деп атап өтті.*

Қазіргі уақытта Біріккен Ұлттар Ұйымының Бас Ассамблеясы «тұрақты даму үшін қауіпсіз, қорғалған және сенімді жасанды интеллект жүйелерінің мүмкіндіктерін пайдалану» атты қарар қабылдады. Біз көрсеткен нормативтік құқықтық құжат ұлттық қауіпсіздікті қамтамасыз ету мақсатында қоғам тарапынан сенімді қарым-қатынасқа лайық жоғары тиімді, адамға және қоршаған ортаға зиян келтірмейтін, жасанды интеллект технологияларын белсенді қолдану мүмкіндіктерін заңнамалық тұрғыдан бекітудің инновациялық тәжірибесінің жарқын мысалы болып табылады.

Қабылданған шешімді коммуникативтік диалогқа, сондай-ақ демократиялық елдердің бүкіл әлемдік қауымдастықты қамтитын цифрлық кеңістікті өзгертуге қатысуын кеңейтуге шақыру ретінде қарастыруға болады. В.М. Баранов пен П.В. Ремизов құқықтық қатынастардағы мұндай қарым-қатынасты тек белгілі бір тілдік механизм тұрғысынан ғана емес, сонымен қатар құқықтық формализмге негізделген [1, 430] құқықтық өріс шеңберіндегі субъектілер арасындағы өзара әрекеттесудің ерекше тәртібі ретінде қарастыру қажеттілігіне назар аударатынын атап өткен жөн. Әрине, Қазақстан Республикасының құқықтық жүйесі қазіргі әлемнің шындықтарында қарқынды дамып келеді, бірақ мұнда бірқатар жаңа заңнамалық бастамалар мен романдар қажет, нәтижесінде жасанды интеллект жүйелерін пайдалану саласындағы үлкен олқылықты жабатын түбегейлі өзгерістер қажет.

Біздің ойымызша, серпінді технологиялармен жоғары тиімді коммуникативтік қатынастарды құру өзара байланысты ауқымды отандық заңнаманы қабылдаудан басталуы керек. Сонымен бірге, Т.Н.Рахманинаның «Нақты заң жобасын әзірлеу туралы шешім қабылдау үшін заңнамалық қызмет стратегиясы және оның дұрыс таңдалған басымдықтары маңызды мәнге ие» деген пікірімен келіспеуге болмайды [2, 165].

Сондай-ақ, отандық құқықтық кеңістікте зияткерлік меншік құқықтарын, азаматтық құқықтардың құпиялылығын, атап айтқанда, жасанды интеллект жүйелерін пайдалану кезінде жеке деректерді сақтауға бағытталған қорғаныс құқықтық тетіктері жоқ екенін еске түсірейік. Сонымен қатар, автоматтандырылған машиналар қабылдаған шешімдерге адамның толық бақылауын қамтамасыз ететін заңды кепілдіктер жоқ, бұл өз кезегінде сенімділік пен болжамдылық критерийлеріне жауап бере алмайды. Бұл жағдай осындай инновацияларды қолданудың барлық жағымсыз салдарын болжауда маңызды рөл атқарады. Жасанды интеллектті пайдалану перспективаларын ашу, сондай-ақ жекелеген заңнамалық түзетулер мен жаңа бастамаларды енгізу үшін оны қоғамдық кеңістікте пайдалану нәтижелері туралы өзекті ақпаратты жүйелі түрде жинау және талдау қажет екенін атап өтуге болмайды.

Сонымен қатар, ұлттық мақсаттарға жету үшін халықтың құқықтық мәдениеті мен құқықтық санасы саласында белсенді жұмыс қажет, әрі қарастырып отырған технологиялар криминогендік фактор бола алатындығын ұмытпауымыз керек. Шабуылдаушылардың қолына түсіп, олар құқық бұзушылықтың мүлдем жаңа түрлерінің пайда болуына түрткі бола алады, осылайша қоғам мен мемлекеттің мүдделеріне нақты қауіп төндіреді [3, 95].

Қазіргі әлемде жасанды интеллекттің табиғи интеллектпен өзара әрекеттесу тақырыбы өзекті бола түсуде, осыған байланысты осы өзара әрекеттесудің ерекшелігін анықтау қажеттілігі туындайды. Қазіргі уақытта «жасанды интеллект» ұғымының анықтамасы деректерді жинауға, талдауға, сондай-ақ адамның танымдық функциясын имитациялауға қабілетті жеке ақпараттық технологиялар жиынтығын сипаттауға дейін азаятынын атап өткен жөн.

Жоғарыда аталған кемшілік қарастырылып отырған құбылыстың категориялық аппаратын адам мен қоғам өмірінің әртүрлі салаларында қолданудың барлық ерекшеліктерін ескере отырып кеңейту қажеттілігін

көрсетеді. Біз Б.М. Кедровтың Тұжырымдаманың анықтамасы пәннің мәнін түсінудің кілті деп санайтын ұстанымымен бөлісеміз [4, 48].

Жасанды интеллект отандық және шетелдік құқық қорғау органдары үшін қылмысқа қарсы күресте керемет күшті құралға айналғанын атап өтейік. Осылайша, машиналар өз қызметі барысында жұмыс істейтін схемалар ақпараттың үлкен массивін өңдеуге және талдауға бағытталған, бұл өз кезегінде халық арасында заңсыз мінез-құлық көріністерінің сипатын көрсететін себеп-салдарлық байланыстарды уақтылы анықтауға көмектеседі және іс жүзінде әртүрлі алдын алу шараларын жүзеге асырады.

Қылмыстық портретті жасау, портреттік сараптама жүргізу кезінде, сондай-ақ құқық бұзушының ықтимал орналасқан жерін анықтау мақсатында Карталарды жобалау кезінде ЖИ қолдану тәжірибесін көрсету керек. Бейнебақылау құрылғыларынан сәйкестендіру процесін, сондай-ақ дерекқорда бұрыннан бар ақпаратты жүзеге асыру кезінде тұлғаны автоматты түрде тануға бағытталған бағдарламалық жасақтама отандық және шетелдік құқық қорғау органдары арасында кеңінен таралды. Бетті тану кезінде жоғары дәлдікке адамның бетінің биометриялық нүктелері бойынша арнайы индекстерді қолдану арқылы қол жеткізіледі. Мұндай бағдарламаны пайдалану кезінде қателік алу ықтималдығы барынша азайтылады, бұл жазықсыз адамды заңсыз жауапқа тарту мүмкіндігін болдырмайды.

Жоғарыда қарастырылған технология қоғамдық іс-шараларды өткізу кезінде, әуежайларда, көлікте және басқа да қоғамдық орындарда кеңінен қолданылды. Күш құрылымдарының техникалық жабдықталуы қылмыстарды сапалы ашу және тергеу процесін айтарлықтай оңтайландырады. Сондай-ақ, жасанды интеллект алаяқтық пен ақшаны жылыстатуға, заңсыз көші-қон мен адам саудасына байланысты қылмыстарды анықтауда қолданылады. Жасанды интеллекттің айрықша ерекшелігі-әртүрлі көздерден алынған жиналған ақпарат негізінде жауаптар жасау мүмкіндігі. Біз қарастыратын автоматты жүйелер іске қатысты көптеген факторларды ескере отырып, белгілі бір құқық бұзушылық оқиғасын егжей-тегжейлі жаңғыртуға бағытталған. Біздің ойымызша, мұндай әлеуметтік-құқықтық құбылыс заңдылық пен құқықтық тәртіп саласында оң нәтиже бере алатындығын атап өтпей, жасанды интеллект жүйелерінің осы коммуникативті ерекшелігіне назар аудармауға болмайды.

Айта кетейік, жасанды интеллект құқық қорғау органдарының қызметкерлерін оқыту үшін белсенді қолданылады. Машиналық оқыту жүйелері нақты жағдайларды имитациялайтын тиімді оқу бағдарламаларын жасауға мүмкіндік береді. Мұндай тренажерлер қызметкерлерге тәжірибе жинауға, стресстік жағдайларда дұрыс шешім қабылдауға көмектеседі, бұл құқық қорғау органдарының кәсібилігі мен дайындық деңгейін арттырады [5, 271-283].

Ақпараттық технологиялардың үнемі дамуы және соның салдарынан құқық бұзушылықтардың жаңа тәсілдерінің пайда болуы жағдайында көптеген елдер қылмыспен күресу үшін нейрондық желілер жүйесін енгізуде.

Танымал құралдардың бірі-predpol (PredictivePolicing) - жасалған деректерді талдау негізінде белгілі бір жерлерде және уақыт аралықтарында құқық бұзушылықтардың ықтималдығын болжайтын американдық жүйе. Бұл құрал

құқық қорғау органдарына ықтимал қылмыстарға алдын-ала дайындалуға мүмкіндік береді.

Сонымен қатар, compas (Alternative Sanctions үшін Correctional Offender Management Profiling) алгоритмі сотталғандар мен сотталушыларда қайталану қаупін бағалауға қабілетті. Жүйе сондай-ақ бастапқыда сот органдары мен жазаларды орындау қызметтеріне құқық бұзушылар тарапынан теріс әрекеттердің ықтимал тәуекелдері мен салдарын тиімдірек басқаруға, жаза тағайындау кезінде неғұрлым негізделген шешімдер қабылдауға мүмкіндік береді. Құқық қорғау қызметінде нейрондық желілерді пайдалану қоғамда бірқатар оң және теріс реакцияларды тудырады. Жеке сыншылар мұндай жүйелер әділеттілік пен кемсітушіліктің негізгі принциптерін бұзуы мүмкін деп санайды, өйткені алгоритмдер біржақты немесе күмәнді деректерге негізделуі мүмкін. Дегенмен, қолдаушылар нейрондық желілерді пайдалану құқық қорғау органдарының тиімділігін арттырып, көптеген құқық бұзушылықтардың алдын алуға көмектесетінін атап көрсетеді [6, 36-55].

Заманауи технологиялар халықаралық деңгейде қолданылатын қауіпсіздік жүйелерін жетілдіруде шешуші рөл атқарады. Инновациялық шешім-бұл куәгерлерден сенімді ақпарат болмаса да, атыс қаруының дыбысы шыққан жерді дәл анықтайтын shotspotter динамик жүйесі.

Айта кетейік, акустикалық жүйелермен қатар басқа да инновациялық технологиялар қолданылады. Мысалы, таңбаларды оптикалық тану технологиясы (OCR) құжаттарды тиімді өңдеуге және ақпаратты талдау процестерін жеделдетуге мүмкіндік береді, бұл өз кезегінде заңдылық пен тәртіп жағдайына әсер етуі мүмкін әртүрлі жағдайларға дәл және жедел жауап беруді қамтамасыз етеді. Жасанды интеллекттің жағымсыз жақтарына қатысты алаңдаушылық пен пікірталастарға қарамастан, осы саладағы әзірлемелер оң нәтиже көрсетеді. Маңызды мысал-Дубай әмірлігінің полиция күштерінің жұмысында қолданылатын «ақылды» GoogleGlass көзілдірігі. Олардың көмегімен құқық қорғау органдары автокөлік жүргізушілерінің бұзушылықтарын тиімдірек қадағалап, іздеудегі көлік құралдары туралы жедел ақпарат ала алады.

Израильде әзірленген қызықты шешімдердің бірі – «Cortica» компаниясының қалалық қауіпсіздік жүйелері. Бұл жүйелер жол трафигін тиімді басқаруға, қала қауіпсіздігін қамтамасыз етуге, қоғамдық орындарды қорғауға және тіпті белгілі бір нысандарды іздеуге мүмкіндік беретін бақылау камералары мен ұшқышсыз ұшу аппараттарының деректерін талдауға негізделген. Қауіпсіздікті қамтамасыз етуде жасанды интеллектті кешенді пайдалану технологияның қазіргі құқық қорғау тәжірибесінде маңызды рөл атқаратынын көрсетеді.

Бүгінгі таңда кең таралған және заманауи технологиялардың ажырамас бөлігіне айналған ұшқышсыз ұшу аппараттары браконьерлерді анықтап, заңсыз тау-кен өндірісін тіркеп қана қоймай, сонымен қатар жоғалған адамдарды іздеуден бастап жол жағдайын бақылауға дейінгі әртүрлі салаларда көмек көрсете алады. Сонымен, ұшқышсыз ұшу аппараттары технологияларын әртүрлі елдердегі ішкі істер органдары белсенді қолданады.

Қазіргі заманғы дрондар жоғары дәлдіктегі камералармен және сенсорлық датчиктермен жабдықталған, бұл оларға әр түрлі тапсырмаларды орындай отырып, әр түрлі жағдайда өз қызметін жүзеге асыруға мүмкіндік береді. Бейнебақылау технологияларымен біріктірілген зияткерлік қауіпсіздік жүйелерінің арқасында құқыққа қайшы әрекеттерді тиімді бақылау және алдын алу қамтамасыз етіледі. Бұл құрылғылар қоршаған ортаға зиян келтірмей, құқық қорғау органдарының жұмысын жеңілдетіп қана қоймай, азаматтардың қауіпсіздігін қамтамасыз етуге ықпал етеді. Жол құқық бұзушылықтары туралы деректерді автоматты түрде тіркеу кешендерін пайдалану кезінде фото және бейнежазба функциялары бар арнайы техникалық құралдар негізгі құралға айналады. Бұл жол қозғалысы саласындағы әкімшілік құқық бұзушылықтарға қатысты фактілерді автоматты түрде анықтауға және тіркеуге мүмкіндік береді. Стационарлық техникалық құралдарды орнату-жолдардағы барлық қауіпсіздікті қамтамасыз етудің маңызды кезеңі. Мамандар авариялық-қауіпті орындарға және жол-көлік оқиғаларының шоғырлану орындарына назар аударады, онда мұндай құралдарды орнату авариялардың алдын алу және көліктің тегіс қозғалысын қамтамасыз ету үшін қажет [7, 436].

Техникалық құралдарды орнату үшін орындарды таңдау кезінде жолдардың апаттылығы мен жүру мүмкіндігі ғана емес, сонымен қатар тиісті уәкілетті органның және оның лауазымды адамдарының пікірі ескерілетіні назар аудартады. Жол қозғалысы қауіпсіздігі жүйелеріне заманауи технологияларды біріктіру апаттар қаупін азайтып қана қоймай, жолдардағы қауіпсіздіктің жалпы деңгейін арттыруға мүмкіндік беретіні сөзсіз. Жалпы, жол қозғалысының барлық қатысушылары үшін қолайлы және қауіпсіз жағдай жасау жолында стационарлық техникалық құралдарды орнату басым мемлекеттік бағыттарға жатады. Қылмыстарды неғұрлым тиімді тергеу үшін мүмкіндіктер ашатын геоақпараттық жүйелерді қолдану тәжірибесі өте кең. Аталған жүйелерді пайдаланудың арқасында күдіктілердің оқиға орны мен орналасқан жерін геокеңістіктік анықтау, нақты уақыт режимінде азаматтар мен көлік құралдарының орын ауыстыруына бақылау жүргізу мүмкін болады. Бір қызығы, бұл үшін әртүрлі әдістер қолданылады, соның ішінде телефон қоңырауларын бақылау және әлеуметтік медиа қызметі. Қозғалыс деректерін сауатты пайдалану қылмыстардың, мысалы, террористік актілердің жолын кесу мен алдын алуда маңызды рөл атқарады.

Бір қызығы, жасанды интеллект үшін құқық бұзушылықтар мен құқық бұзушылар туралы ақпарат алудың маңызды көздері Виртуалды кеңістіктегі қызығушылық тудыратын объектіні немесе субъектіні анықтауға мүмкіндік беретін көптеген мәліметтерді жинақтайтын әлеуметтік желілер мен медиа ресурстар болып қала береді. Пікірлерді, пікірлерді талдау AI жүйесіне ықтимал қауіптерді анықтауға және алдын алуға мүмкіндік береді. Киберқауіпсіздік сияқты бағыт ерекше назар аударуға тұрарлық. Бұл технологиялар желілік трафиктегі ауытқуларды анықтауға, қауіптер мен вирустарды анықтауға, деректерді қорғауға, кибершабуылдардың алдын алуға, биометриялық параметрлер бойынша бетті лезде тануға, сондай-ақ саусақтардың папиллярлық үлгілерінің іздеріне қабілетті. Зиянды бағдарламалық жасақтаманың белгілерін

анықтауға үйретілген нейрондық желілер дәстүрлі түрде қолданылатын антивирустар тапсырманы орындамаған кезде де компьютерлік қауіптерді анықтауға жоғары сезімталдыққа ие.

Қорытынды

Жоғарыда айтылғандар жасанды интеллектті қоғам мен мемлекеттің коммуникативті қарым-қатынас құралы ретінде қарастыруға мүмкіндік береді, ол өзі дайындаған, жасаған немесе жасаған құқыққа қайшы әрекет туралы әр түрлі ақпарат жиынтығын, сондай-ақ тиісті шаралар қабылдау мақсатында оны уәкілетті органдар мен ұйымдарға және олардың лауазымды адамдарына уақтылы жеткізу мүмкіндігін тудырады.

Нәтижесінде біз жаңа жүйелердің толық қауіпсіздігін қамтамасыз етуге қабілетті, мемлекеттік деңгейде ЖИ мәселелерімен айналысатын бірыңғай бақылау жүйесі мен реттеуші органдарды құрудың орындылығы туралы мәселені егжей-тегжейлі пысықтауды талап ететін қорытындыға келдік. Құқық қорғау қызметінде жасанды интеллект құралдарын пайдаланудың құқықтық мәртебесін анықтау және стандарттау да маңызды қадам болып табылады. Құқық қорғау органдарының қызметінде ЖИ пайдалану процесінде қауіп төндіруі мүмкін адамның іргелі құқықтарын қорғауға ерекше назар аудару керек.

Сонымен қатар, қылмыстық-құқыққа қарсы мақсаттарда ЖИ теріс пайдалануға қарсы іс-қимыл стратегияларын әзірлеу қажет. Қылмыстық заңнамада бекітілетін арнайы мәртебені анықтау маңызды. Сондай-ақ, жоғарыда аталған міндеттерді табысты іске асыру үшін құқық қорғау органдары қызметкерлерінің цифрлық сауаттылық деңгейін арттыру қажет. Қызметкерлерді жасанды интеллектпен жұмыс істеудің заманауи технологиялары мен принциптеріне үйрету оларға өз жұмысында жаңа әдістемелерді тиімді қолдануға көмектеседі және барлық азаматтар үшін қауіпсіз ортаны қамтамасыз етеді. Бұдан басқа, заңдылық пен құқықтық тәртіпті нығайту мақсатында жасанды интеллект технологиялары мен робототехника саласындағы қатынастарды реттеуді дамытудың тұжырымдамасын құқық қорғау органдары қызметкерлерінің өздерінің практикалық қызметінде ЖИ пайдалануының әдіснамалық және криминологиялық негіздерін қамтитын әдістемелік ұсынымдармен толықтыруды ұсынамыз.

Қойылған міндетті шешудегі басты мәселе құқық қорғау органдарының жұмысында жасанды интеллект алгоритмдерін пайдаланудың халықаралық тәжірибесін талдау болып табылады деп санаймыз. Бұл тәжірибеде сыналған жасанды интелекттің ең пайдалы түрлерін анықтауға және оларды тиісті органдардың қызметінде тиімділікті арттыру үшін қолдануға мүмкіндік береді.

---

1. **Баранов В.М. Ремизов П.В**. Критика законодательства как особая разновидность правовой коммуникации // Коммуникативная теория права и современные проблемы юриспруденции: к 60-летию Андрея Васильевича Полякова: коллективная монография: в 2 т. / под ред. **М.В. Антонова, И.Л. Чест-нова**. СПб., 2014. Т. 2. Актуальные проблемы философии права и юридической науки в связи с коммуникативной теорией права. С. 429-444.
2. Рахманина Т. Н. Организация и методика подготовки законопроектов // Законотворчество в Российской Федерации / под ред. **А.С. Пиголкина.** М., 2000. С. 177-224.
3. **Кузнецова А. В.** Искусственный интеллект и информационная безопасность общества / **А.В. Кузнецова, С.И. Самыгин, М.В. Радионов.** М.: Русайнс, 2017. С. 109-117.
4. **Кедров Б.М.** Оперирование понятиями в диалектической и формальной логике // Диалектика и логика. Формы мышления. Москва: Академия наук СССР, 1962. С. 42-141.

5.**Ястребов О.А.** Искусственный интеллект в правовом пространстве: концептуальные и теоретические подходы // Правосубъектность: общетеоретический, отраслевой и международно-правовой анализ: сборник материалов к XII ежегодным научным чтениям памяти проф. С. Н. Братуся. М., 2017. С. 271-283.
6.**Ястребов О.А.** Правосубъектность электронного лица: теоретико-методологические подходы // Труды Института государства и права Российской академии наук. 2018. Т. 13. № 2. С. 36-55.
7. **Кубасов И.А., Лекарь Л.А., Кондрущенков О.М.** Перспективные направления применения методов анализа больших данных в информационно-аналитическом обеспечении оперативно-розыскной деятельности // Стратегическое развитие системы МВД России: состояние, тенденции, перспективы: сборник статей международной научно-практической конференции / под общ. ред. **И.Г. Чистобородо-ва, А.Л. Ситковского, В.О. Лапина.** М., 2020. С. 436-442.

К ВОПРОСАМ МОРАЛЬНО-ПСИХОЛОГИЧЕСКОГО ОБЕСПЕЧЕНИЯ СЛУЖЕБНО-БОЕВОЙ ДЕЯТЕЛЬНОСТИ НАЦИОНАЛЬНОЙ ГВАРДИИ РЕСПУБЛИКИ КАЗАХСТАН

САУТБАЕВ Данияр Бауржанович
Национальный университет обороны Республики Казахстан, Астана

Актуальность исследования вопроса морально-психологического обеспечения служебно-боевой деятельности в Национальной гвардии Республики Казахстан обусловлена современными угрозами, которые неразрывно связаны с разрешением конфликтов, связанных с возникновением чрезвычайных ситуаций различного характера. Проведенный анализ нормативно-правовых актов и руководящих документов позволяет проследить взаимосвязь с проходившими на территории Республики Казахстан событиями, которые повлекли за собой проведение специальных операций с участием Национальной гвардии Республики Казахстан. Привлечение войск правопорядка к проведению специальных операций как совместно, так и самостоятельно в период выполнения служебно-боевых задач ставят вопрос о морально-психологическом обеспечении данных действий. Обозначенная в статье проблема ставит перед авторами задачи по раскрытию сущности и содержания морально-психологического обеспечения служебно-боевой деятельности Национальной гвардии Республики Казахстан, а также определении необходимости дальнейшего исследования проблем морально-психологического обеспечения служебно-боевой деятельности Национальной гвардии Республики Казахстан.

Введение

Глава государства Токаев К.К., выступая с докладом «Уроки «трагического января»: единство общества — гарантия независимости» на заседании Мажилиса Парламента Республики Казахстан, поручил укрепить количественно и качественно Национальную гвардию Республики Казахстан [1].

С обретением независимости Республики Казахстан, 10 января 1992 года были образованы Внутренние войска МВД Республики Казахстан [2]. В целях оперативного реагирования и расширения функций в решении задач общественной и военной безопасности государства 21 апреля 2014 года Внутренние войска МВД Республики Казахстан преобразованы в Национальную гвардию Республики Казахстан [3].

Постановка проблемы. На сегодняшний день войска Национальной гвардии Республики Казахстан (далее — НГ РК) могут выполнять задачи различного характера и направленности, как внутри страны, так и, в некоторых случаях, за ее пределами. В Республике Казахстан НГ РК входит в единую систему органов внутренних дел Республики Казахстан и предназначены для обеспечения безопасности личности, общества и государства, защиты прав и свобод человека и гражданина от преступных и иных противоправных посягательств.

Принятый 10 января 2015 года Закон «О Национальной гвардии Республики Казахстан» определяет ряд задач для военнослужащих войск правопорядка. Одной из важных задач является как, участие совместно с органами внутренних дел в охране общественного порядка, пресечении массовых беспорядков,

обеспечении общественной безопасности и правовых режимов чрезвычайного и военного положения [4].

При этом, выполнение этой задачи сопряжено, в некоторых случаях, с выполнением специальных операций. В данном случае, под специальной операцией понимается комплекс оперативных, режимных, войсковых и других мероприятий, проводимых комплексными силами и средствами на ограниченной территории в установленные сроки, по общему замыслу и под единым руководством, согласно утвержденному специальному оперативному плану [5, с. 7].

Вместе с тем, морально-психологическая готовность личного состава к выполнению поставленных задач — одно из важных условий боеспособности и эффективности действий в ходе выполнения служебно-боевых задач. Однако, недостаточная организация морально-психологического обеспечения специальных операций, увеличивает риск ошибок, снижает оперативность принятия решений, что может привести к росту числа психосоматических и посттравматических расстройств среди военнослужащих, где морально-психологическое обеспечение служебно-боевой деятельности Национальной гвардии Республики Казахстан - это комплекс мероприятий, согласованных по целям и задачам, последовательности, привлекаемым и проводимыми силами и используемыми средствами, совместно с взаимодействующими органами, по созданию, поддержанию и восстановлению морально-психологического состояния личного состава войск, в целях своевременного и полного выполнения служебно-боевых задач по обеспечению режима чрезвычайного и военного положения. [6, с. 4].

В этих условиях разработка систематической, научно обоснованной организации морально-психологического обеспечения в ходе выполнения задач служебно-боевой деятельности, адаптированной под специфику задач НГ РК, является насущной задачей командиров и начальников, так и для офицеров воспитателей и требует глубокого научного исследования.

Цель:

Рассмотреть роль и место морально-психологического обеспечения служебно-боевой деятельности Национальной гвардии Республики Казахстан.

Задачи:

1) раскрыть сущность и содержание морально-психологического обеспечения служебно-боевой деятельности в Национальной гвардии Республики Казахстан;

2) определить необходимость дальнейшего исследования проблем морально-психологического обеспечения служебно-боевой деятельности в Национальной гвардии Республики Казахстан.

Материалы и методы исследования: Источниковедческую базу исследования составили научная и специальная литература, а также приказы по рассматриваемой проблеме. Использовались методы анализа, синтеза, обобщения и научной интерпретации.

Результаты исследования:

Современная оперативно-тактическая обстановка, возможность возникновения массовых беспорядков повышают требования к готовности сил быстрого реагирования. Национальная гвардия Республики Казахстан как структура, выполняющая задачи по обеспечению общественной безопасности и охране правопорядка в чрезвычайных ситуациях, сталкивается с необходимостью быстрой мобилизации личного состава в условиях повышенной неопределённости и угроз.

Важно отметить, что успешное выполнение этих задач невозможно без высокого уровня морально-психологической устойчивости личного состава. Морально-психологическое состояние военнослужащих напрямую влияет на боеспособность, дисциплину и эффективность работы подразделений. В этой связи морально-психологическое обеспечение в НГ РК имеет следующие особенности при действиях подразделений по пресечению групповых (массовых) нарушений общественного порядка в населенном пункте, где уделяется внимание:

- **разъяснению** личному составу социальной опасности групповых (массовых) нарушений общественного порядка, необходимости смелых и решительных действий по их пресечению;
- **ознакомлению** военнослужащих с обычаями и традициями местного населения, убеждению их в необходимости строго соблюдать законность и не поддаваться на возможные провокации;
- **мобилизации** военнослужащих на обеспечение надежной охраны и обороны порученных объектов, государственного имущества. [6, с.80].

Уровень морально-психологического состояния военнослужащих оказывает прямое влияние на способность выполнять поставленные задачи. События в г. Жанаозен 2011 года, в Кордайском районе 2020 года, в Январе 2022 года, когда личный состав столкнулся с напряженными и опасными ситуациями, качество организации морально-психологического обеспечения личного состава сыграло ключевую роль в способности к выполнению служебно-боевых задач. В этом случае, при низкой морально-психологической устойчивости личного состава, в ходе выполнения служебно-боевых задач, могут возникнуть случаи стресса, тревожности и эмоционального истощения, что скажется на эффективности работы подразделений и на снижении общей боеспособности. Отсутствие должной морально-психологической поддержки, а также отсутствие четкой системы психологической диагностики и профилактики, может привести к ухудшению морально-психологического состояния личного состава, снижению воинской дисциплины и даже проявлению агрессии, и это, авторы считают серьезной проблемой, которая на сегодняшний день требует дальнейшего глубокого научного исследования.

Научная работа должна затронуть такие аспекты как, планирование и качественная организация морально-психологического обеспечения на всех этапах выполнения служебно-боевых задач, разработки и внедрения комплексных программ психологической подготовки и поддержки, а также ряда рекомендаций и предложений для внесения изменений и дополнений в

существующие нормативно-правовые акты, что существенно повысит эффективность выполнения задач НГ РК и позволит личному составу добиться отличных результатов в сложных условиях повышенного стресса.

Заключение

Национальная гвардия Республики Казахстан выполняет ряд ключевых задач, таких как обеспечение общественного порядка, борьба с терроризмом, защита важных государственных объектов, поддержание гражданского мира и участие в ликвидации чрезвычайных ситуаций. Важно отметить, что успешное выполнение этих задач невозможно без высокого уровня морально-психологической устойчивости личного состава. Психологическое состояние военнослужащих напрямую влияет на боеспособность, дисциплину и эффективность работы подразделений.

Таким образом, морально-психологическое обеспечение служебно-боевой деятельности является важнейшей составляющей эффективного функционирования НГ РК, от которой зависит не только боеспособность подразделений, но и стабильность внутреннего климата в войсках.

1. Выступление Главы государства К.-Ж.К. Токаева на заседании Мажилиса парламента Республики Казахстан. Уроки «трагического января»: единство общества — гарантия независимости URL: https://akorda.kz/ru/ (дата обращения 02.03.2026).
2. О Внутренних войсках Республики Казахстан / Указ Президента Республики Казахстан от 10 января 1992 года №575.
3. О мерах по дальнейшему совершенствованию системы государственного управления Республики Казахстан / Указ Президента Республики Казахстан от 21 апреля 2014 года №807.
4. О Национальной гвардии Республики Казахстан / Закон Республики Казахстан от 10 января 2015 года 274-V. - Астана, 2015. — 31 с.
5. **Акыжанов Р.Ж.** Оперативно-служебная (боевая) готовность соединений и частей Национальной гвардии, учебное пособие: Астана, 2025 - 181 с.
6. Руководство по организации воспитательной и социально-правовой работы с личным составом Национальной гвардии Республики Казахстан часть III «Организация воспитательной, социально-правовой, психологической и идеологической работы с личным составом взвода, роты, батальона Национальной гвардии» / Приказ Заместителя Министра внутренних дел Республики Казахстан - Главнокомандующего Национальной гвардией от 25 сентября 2025 года № 400. — 146 с.

О ПРОВОДИМОЙ РАБОТЕ ПО ВНЕДРЕНИЮ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

ТЕМІРЖАНОВ Асхат Төлешұлы
Начальник Управления Следственного департамента МВД Республики Казахстан, полковник полиции

В целях эффективного решения задач уголовного судопроизводства 6 февраля 2025 года Следственный департамент **инициировал внедрение искусственного** интеллекта в Информационную систему Единый реестр досудебных расследований.

Под председательством заместителя министра проведена рабочая встреча с руководством служб МВД *(СД, ВСД, ДСБ, ДИиС),* КПСиСУ и IT-компаниями по обсуждению данного вопроса.

Учитывая, что ЕРДР-ом пользуются все правоохранительные органы и его техническое обслуживание осуществляет Комитет по правовой статистике и специальным учетам Генеральной прокуратуры, решено рабочим органам определить **КПСиСУ.**

По нашей инициативе 20 марта т.г. Распоряжением первого заместителя Генерального Прокурора создана межведомственная рабочая группа из числа руководителей и сотрудников МВД, ГП, КПСиСУ и МЮ.

Свои услуги по разработке системы предоставляют IT-компании, специализирующие на создании цифровых решений с использованием микросервисной архитектуры.

Цель внедрения искусственного интеллекта - **создание помощника следователя**, способного помогать в расследовании уголовных дел, автоматизировать следственную работу и снизить трудозатраты.

В системе созданы следующие **модули:**

1. Планирование расследования;
2. Обработка показаний;
3. Формирование процессуальных документов;
4. Аналитика и прогнозирование.

Остановлюсь на каждом **функционале отдельно.**

Так, модуль **планирование расследования.**

В целом, расследование преступлений – это сложная, разносторонняя деятельность, осуществляемая в определенные, установленные законом сроки.

Следователь должен выявить все существенные обстоятельства имевшего место преступления и установить лиц, его совершивших.

В целях выполнения указанных задач необходимо умелое построение следственных версий, производство различных следственных действий, например допросов, обысков, осмотров, проведения экспертиз.

Без организующего начала, без целенаправленности вся эта сложная деятельность не обеспечит успеха. Именно это и обеспечивается планированием расследования.

В чем же выражается планирование?

Определяя его в общих чертах, можно сказать, что планирование состоит в такой организации следствия, которая обеспечивает быстрое и полное раскрытие преступления.

Для успешного выполнения этой сложной задачи, предлагаем ИИ помочь следователю. Он систематизирует имеющуюся информацию и сформирует версии происшествия.

В итоге ИИ составит план расследования с пошаговым алгоритмом следственных действий.

Ключевые функции модуля включают:

-анализ информации по делу;

-определение квалификации преступления;

-формирование нескольких версий расследования с обоснованиями и приоритетами.

Система создает детальный план следственных действий и предоставляет тактические рекомендации для их проведения.

Следующий модуль – **обработка показаний *(транскрибации)*.**

ИИ автоматизирует процесс преобразования аудио- и видеозаписей допросов в текстовый формат, анализирует содержание показаний, выявляет детали и противоречия.

Функциональные возможности модуля:

• Преобразование речи в текст с поддержкой языков, шумоподавлением и разделением реплик;

• Создание краткого резюме показаний;

• Анализ последовательности изложения;

• Сравнительный анализ нескольких показаний;

• Выявление противоречий;

• Генерация уточняющих вопросов;

• Подготовка к очным ставкам;

• Проставление временных меток;

• Экспорт в различные форматы.

Это значительно ускорит процесс обработки следственных материалов и поможет выявить важные детали и противоречия в показаниях, которые могут быть пропущены при ручной обработке.

Функционально модуль обеспечивает высококачественное преобразование речи в текст с поддержкой различных языков, шумоподавлением и разделением реплик разных говорящих.

Система автоматически создает краткое резюме показаний, проводит анализ ее последовательности изложения.

При наличии нескольких показаний модуль выполняет их сравнительный анализ, выявляет противоречия и генерирует **уточняющие вопросы для**

последующих допросов, в т.ч. для последующего проведения очных ставок между участниками процесса.

Все результаты проставляются временными метками для быстрой навигации и будут распечатываться в различных форматах для приобщения к материалам дела.

В перспективе ИИ поможет нам устанавливать правдивость и искренность показаний. Сегодня существует несколько методик распознания лжи, и они уже изучаются для внедрения в практическую деятельность.

Следующий модуль – это **формирование процессуальных документов.** Он предназначен для автоматизации процесса создания необходимых документов.

ИИ сам будет составлять постановления о назначении экспертиз с перечнем рекомендуемых вопросов экспертам.

Автоматизируется составление ходатайств, запросов и других документов на основе имеющихся данных.

Все процессуальные документы будут соответствовать требованиям законодательства с обеспечением полноты.

В настоящее время система на основе материалов уголовного дела формирует проекты постановления о квалификации деяния подозреваемого и обвинительный акт.

Система будет в автоматическом режиме готовить уголовное дело на 90%.

Формировать фабулу дела, составлять хронологию событий, данные о подозреваемом.

Систематизирует имеющиеся доказательства, и сама определит квалификацию преступления.

Функция редактирования позволяет следователю вносить корректировки в любую часть документа.

Далее - модуль **аналитики и прогнозирования.**

Он включает в себя широкие функции для профилактики преступлений.

В соответствии с частью 4 статьи 113 УПК, по уголовному делу подлежат выявлению обстоятельства, способствовавшие совершению уголовного правонарушения.

Статьей 200 УПК предусмотрено право следователя, после установления обстоятельств, способствовавших совершению уголовного правонарушения, вносить в соответствующие государственные органы, организации представление о принятии мер по устранению этих обстоятельств или других нарушений закона.

ИИ поможет следователю выявить все нарушения законов, условия, способствующие совершению преступлений и составить шаблон представления с определением адресата внесения.

Также предложит следователю рекомендации, которые необходимо включить в представление.

На наш взгляд, ИИ поможет продвижению идеологии закона и порядка в повышении правосознания граждан и укреплении доверия к государственным институтам.

Кроме того, в модуле предусмотрены аналитические функции для руководителей с целью принятия управленческих решений, которые организуют практическую деятельность по борьбе с преступностью.

Это данные о совершенных преступлениях, что позволяет создать полное представление о криминогенной обстановке.

В июле 2025 года пилотный проект по внедрению ИИ запущен в трех подразделениях: УП района «Есиль» и УП района «Алматы» ДП г.Астана и ОП г.Косши ДП Акмолинской области.

Руководством МВД проведен ряд рабочих встреч с акимами г.Астана и Акмолинской области. По итогам проведенных переговоров местными исполнительными органами выделены финансовые средства на приобретение серверного оборудования и программного обеспечения *(135,7 млн. и 40 млн соответственно).*

В декабре 2025г. ДП г.Астаны завершена закупка серверного оборудования.

С начала 2026 года к пилотному проекту дополнительно подключены сотрудники других территориальных подразделений ДП г.Астаны *(УП района «Байконур», «Сарыарка», «Сарайшик», «Нура»).*

Буквально на днях завершена интеграция ИИ с информационной системой ЕРДР.

Кроме того, МИИЦР выделены мощности суперкомпьютера для КПСиСУ ГП в целях реализации пилотного проекта.

В целях качественного составления документов программой, разработана инструкция для формирования фабул уголовных правонарушений и рекомендации по подготовке документов.

Вопрос о масштабировании пилота планируется рассмотреть по итогам первого полугодия т.г.

Мы сегодня не говорим, что внедрение искусственного интеллекта полностью заменит следователя.

Он лишь будет ему помогать расследовать уголовные дела более качественно, подсказывать ошибки и направлять, что полностью согласуется с задачами уголовно-процессуального законодательства – статье 8 УПК быстрое и полное раскрытие, расследование преступлений, изобличение и привлечение к уголовной ответственности лиц, их совершивших.

КӘМЕЛЕТКЕ ТОЛМАҒАНДАРДЫ ҰСТАУДЫҢ ПРОЦЕСТІК ШЕКТЕРІ: ҚҰҚЫҚТЫҚ АЙҚЫНДЫҚ ПЕН КОНСТИТУЦИЯЛЫҚ КЕПІЛДІКТЕР ТЕҢГЕРІМІНІҢ МӘСЕЛЕЛЕРІ

ТУЛЕУОВА Мулдир Ерлановна
Қазақстан Республикасы Бас прокуратурасының жанындағы Құқық қорғау органдары академиясы, Қосшы қ-сы

Мақала кәмелетке толмағандарға қатысты ұстау мерзімдерін қолдану барысында туындайтын қылмыстық-процестік мәселелерді зерттеуге арналған. Автор Қазақстан Республикасының Қылмыстық-процестік кодексі, конституциялық кепілдіктер және халықаралық құқық талаптары негізінде 24 сағаттық және 72 сағаттық ұстау мерзімдерінің өзара арақатынасын талдайды. Құқық қолдану тәжірибесінде қалыптасқан тәсілдер сараланып, құқықтық реттеудегі айқын еместіктің тергеу қызметіне, дәлелдемелердің жарамдылығына және азаматтардың бостандығын шектеудің заңдылығына әсері қарастырылады. Сонымен қатар кәмелетке толмағандарға қатысты процестік мәжбүрлеу шараларын қолдану кезінде пропорционалдық қағидатын сақтау қажеттілігі негізделіп, заңнаманы жетілдіруге бағытталған ұсыныстар беріледі.

Бүгінде кәмелетке толмағандар жасаған құқық бұзушылықтар мәселесі тек құқық қорғау органдарының қызметімен шектелмейді. Бұл тақырып мемлекеттік құқықтық саясат аясында да маңызды бағыттардың біріне айналды. Соңғы жылдары қоғамдағы әлеуметтік жағдайдың өзгеруі, цифрлық ортаның кеңеюі, интернеттің ықпалы мен жастар арасындағы мінез-құлық ерекшеліктерінің күрделене түсуі аталған мәселенің өзектілігін сақтап отыр.

Кәмелетке толмағандарға қатысты қылмыстық процесте арнайы кепілдіктердің белгіленуі олардың ерекше құқықтық мәртебесімен байланысты. Сонымен қатар мұндай тәсіл халықаралық құқық талаптарына да сәйкес келеді. Осы себепті мемлекет кәмелетке толмағандарға процестік мәжбүрлеу шараларын қолдану кезінде олардың құқықтары мен заңды мүдделерін қорғауға ерекше назар аударуға тиіс.

Қазақстан Республикасының Қылмыстық-процестік кодексінде кәмелетке толмағандарға арналған бірқатар арнайы кепілдіктер бекітілген. Солардың бірі – ұстау мерзіміне қатысты ерекше тәртіптің белгіленуі. Дегенмен құқық қолдану тәжірибесінде дәл осы норма әртүрлі түсіндіріледі. Соның салдарынан құқықтық даулар туындап, тәжірибеде біркелкі емес тәсілдер қалыптасып отыр.

Әсіресе ауыр және аса ауыр қылмыстар бойынша көзделген 72 сағаттық ұстау мерзімін кәмелетке толмағандарға қолдану мәселесі ерекше назар аударуды қажет етеді [1]. Мұндай жағдайда қылмысты тергеудің тиімділігі мен баланың конституциялық құқықтарын сақтау арасындағы тепе-теңдікті қамтамасыз ету мәселесі алдыңғы қатарға шығады.

Қазақстан Республикасы Қылмыстық-процестік кодексінің 131-бабы 4-бөлігінің талаптарына сәйкес күдіктіні ұстаудың жалпы мерзімі 48 сағаттан аспауға тиіс. Ал кәмелетке толмағандарға қатысты заң шығарушы неғұрлым қысқартылған – 24 сағаттық мерзімді белгілеген [1]. Мұндай құқықтық шектеу кәмелетке толмағандардың жас ерекшелігін, психикалық тұрақтылығының

толық қалыптаспағанын және олардың құқықтық қорғалуға көбірек мұқтаж екенін ескеруден туындайды.

Осы тұрғыдан алғанда, аталған норма кәмелетке толмағандарға берілген қосымша процестік кепілдіктердің бірі болып саналады. Себебі ересек адамдарға қарағанда, жасөспірімдер үшін еркіндікті уақытша шектеудің өзі едәуір күрделі психологиялық әсер етуі және әлеуметтік бейімделуіне кері ықпал жасауы ықтимал.

Сонымен қатар қолданыстағы қылмыстық-процестік заңнамада жекелеген санаттағы қылмыстар бойынша ұстау мерзімін 72 сағатқа дейін ұзартуға мүмкіндік беретін ережелер де бар. Мұндай істер қатарына терроризм мен экстремизмге байланысты құқық бұзушылықтар, ұйымдасқан қылмыстық топ құрамында жасалған әрекеттер, есірткі заттарының заңсыз айналымына қатысты қылмыстар, сондай-ақ адам өліміне алып келген қасақана іс-әрекеттер енгізілген.

Осы тұста құқық қолдану тәжірибесінде елеулі пікірталас тудыратын мәселе байқалады. Қолданыстағы заңнамада кәмелетке толмағандарға арналған 24 сағаттық шектеудің ерекше кепілдік ретінде барлық жағдайда сақталатыны нақты көрсетілмеген. Сонымен қатар ҚПК-де көзделген ерекше жағдайларда белгіленген 72 сағаттық мерзімнің кәмелетке толмағандарға таралатыны не таралмайтыны да тікелей айқындалмаған.

Практикада бұл нормаларды түсіндірудің екі бағыты қалыптасқан. Бірқатар құқық қолданушылар кәмелетке толмағандарға қатысты 24 сағаттық мерзімді өзгертілмейтін арнайы кепілдік ретінде қабылдайды. Олардың пайымдауынша, заң шығарушы бұл норманы балалардың құқықтарын қосымша қорғау мақсатында енгізген, сондықтан ол қылмыстың санатына қарамастан сақталуға тиіс.

Ал екінші көзқарас заң мәтінін тікелей түсіндіруге сүйенеді. Осы тәсілді ұстанатындар ҚПК-де көзделген ерекше жағдайлар барлық күдіктілерге ортақ қолданылады деп есептейді. Соның нәтижесінде 72 сағаттық ұстау мерзімі кәмелетке толмағандарға да қолданылып келеді.

Талдау көрсеткендей, тергеу тәжірибесінде, әсіресе ауыр және аса ауыр қылмыстар бойынша, көбіне осы соңғы тәсіл басымдыққа ие.

Кәмелетке толмаған адамды 72 сағатқа дейін ұстау мәселесін тек қылмыстық процестегі техникалық мәселе ретінде қарастыруға болмайды. Бұл, ең алдымен, адамның конституциялық құқықтары мен бостандығын шектеудің шегімен байланысты құқықтық мәселе болып табылады.

Ересек тұлғаларға қатысты ұстау мерзімі 48 сағаттан 72 сағатқа дейін ұзартылған кезде қосымша шектеу уақыты 24 сағатты құрайды. Ал кәмелетке толмағандарға қатысты бастапқы мерзім 24 сағат болғандықтан, оны 72 сағатқа дейін ұзарту қосымша 48 сағатқа тең болады.

Яғни іс жүзінде кәмелетке толмаған адамның бостандығын шектеу көлемі едәуір ұлғаяды. Осы тұста құқықтық қайшылық туындайды: заң кәмелетке толмағандардың құқықтарын қосымша қорғауды көздегенімен, тәжірибеде бұл кепілдік олардың бостандығын ұзағырақ шектеуге негіз болып кетуі мүмкін.

Құқықтық мемлекетте кез келген процестік мәжбүрлеу шарасы заң талаптарына ғана емес, оның қажеттілігі мен мөлшерлестігіне де сәйкес келуге

тиіс. Пропорционалдық қағидаты бойынша адамның құқықтарын шектеу қолданылып отырған мақсаттан артық болмауы қажет.

Кәмелетке толмағандар жасына, психологиялық ерекшеліктеріне және қоғамға бейімделу деңгейіне байланысты құқықтық қорғаудың күшейтілген түрін қажет етеді. Сол себепті оларға қатысты қандай да бір бостандықты шектеу шарасы қолданылған жағдайда, оның мерзімі мүмкіндігінше қысқа болуы тиіс.

Құқықтық реттеудегі нақты айқындықтың жеткіліксіздігі тәжірибеде әртүрлі құқық қолдану тәсілдерінің пайда болуына әсер етеді. Мұндай жағдай нәтижесінде азаматтардың конституциялық құқықтарын шектеу мәселесінде біркелкі емес практика қалыптасуы ықтимал.

Қазақстан Республикасы Конституциясының 18-бабында әр адамның бостандығына және жеке басына қол сұғылмауына кепілдік берілген [2]. Осыған байланысты адам бостандығын шектеу тек заңда тікелей көзделген жағдайларда және белгіленген рәсімдерді сақтай отырып жүзеге асырылуы қажет.

Ұлттық заңнамада бекітілген бұл қағидалар халықаралық құқық талаптарымен де сәйкес келеді. Атап айтқанда, Қазақстан қосылған Бала құқықтары туралы конвенцияда кәмелетке толмағанды ұстау немесе қамауда ұстау ерекше жағдайларда ғана және ең қысқа мерзімге қолданылуы керектігі белгіленген [3].

Кәмелетке толмағандарға қатысты сот төрелігін жүзеге асыру саласындағы халықаралық актілердің бірі – БҰҰ-ның Пекин қағидалары. Бұл құжатта да кәмелетке толмағандарға қатысты шектеу сипатындағы шараларды қолдану ерекше жағдай ретінде қарастырылатыны көрсетілген [4]. Яғни, баланың бостандығын шектеуге байланысты кез келген процестік шешім барынша сақтықпен қабылдануға тиіс.

Халықаралық құқықтық құжаттардың мазмұнына қарағанда, олардың негізгі мақсаты – кәмелетке толмағандарға қатысты репрессивтік ықпалды азайту және ең алдымен баланың мүддесін қорғауды қамтамасыз ету. Осыған байланысты бостандықты шектеу шаралары тек қажетті болған жағдайда ғана қолданылуы керек деген ұстаным басым.

Сол себепті ұлттық қылмыстық-процестік нормаларды қолдану және түсіндіру барысында халықаралық құқықта бекітілген «мүмкіндігінше қысқа мерзім» қағидаты назардан тыс қалмауы қажет.

Ұстау мерзімдеріне қатысты нормаларды әртүрлі түсіндіру құқық қолдану тәжірибесінде бірқатар күрделі мәселелер туындатады.

Ең алдымен, мұндай жағдай дәлелдемелердің заңдылығына байланысты дауларға әкелуі мүмкін. Егер қорғау тарапы ұстау заңда көрсетілген мерзімнен асып кеткенін немесе талаптардың сақталмағанын көрсетсе, жүргізілген процестік әрекеттердің заңдылығы күмән тудыруы ықтимал.

Сонымен қатар құқықтық нормалардың нақты айқындалмауы тергеуші мен прокурордың жұмысына да әсер етеді. Тәжірибеде бір норманы әртүрлі түсіндіру кездесетіндіктен, құқық қолданушы шешім қабылдау кезінде тәуекелге барады.

Бұл мәселе қоғамның құқық қорғау органдарына деген сеніміне де ықпал етеді. Азаматтар заң талаптарының барлық жағдайда бірдей және тұрақты

қолданылуын күтеді. Егер тәжірибеде әртүрлі тәсілдер орын алса, құқықтық кепілдіктердің тиімділігіне күмән пайда болады.

Бұдан бөлек, кәмелетке толмаған адамды ұзақ уақыт ұстау оның психологиялық жағдайына теріс әсер етуі мүмкін. Мұндай жағдай кейіннен оның әлеуметтік ортаға бейімделуіне де ықпал етеді.

2021–2024 жылдар аралығындағы Қазақстан Республикасы Бас прокуратурасы Құқықтық статистика және арнайы есепке алу комитетінің статистикалық деректерін талдау кәмелетке толмағандарға қатысты 72 сағатқа дейінгі ұстауды қолдану тәжірибесінің тұрақты түрде сақталып отырғанын көрсетеді. Аталған мәліметтер қылмыстық қудалау органдарының процестік мәжбүрлеу шараларын қолдану көрсеткіштерінде көрініс тапқан.

Статистикалық деректерге сәйкес, 2021 жылы барлығы 91 кәмелетке толмаған ұсталған, олардың 49-ына қатысты 72 сағатқа дейінгі ұстау қолданылған. 2022 жылы мұндай жағдайлар саны 69-ға жеткен. 2023 жылы 52 жағдай тіркелсе, 2024 жылы бұл көрсеткіш 98-ге дейін өскен.

Сонымен қатар жалпы ұсталған кәмелетке толмағандардың саны да жыл сайын өсіп отырған:

— 2021 жыл - 91 адам;
— 2022 жыл - 147 адам;
— 2023 жыл - 230 адам;
— 2024 жыл - 353 адам.

Бұл көрсеткіштер 72 сағаттық ұстауды қолдану тәжірибесінің кездейсоқ немесе ерекше сипатта емес, жүйелі түрде қалыптасқан құқық қолдану тәсіліне айналып отырғанын көрсетеді.

Сонымен бірге заң шығарушы арнайы процестік кепілдік ретінде белгілеген 24 сағаттық ұстау мерзімін қолдану тәжірибесі салыстырмалы түрде шектеулі болып отыр. Атап айтқанда, 24 сағаттан аспайтын мерзімге ұсталған кәмелетке толмағандардың саны:

— 2021 жыл - 24 адам;
— 2022 жыл - 39 адам;
— 2023 жыл - 76 адам;
— 2024 жыл - 124 адам.

Қысқартылған мерзімді қолдану көрсеткіштерінің өсуі байқалғанымен, 72 сағаттық ұстау тәжірибесі кәмелетке толмағандарға қатысты процестік мәжбүрлеу құрылымында елеулі үлесті сақтап отыр.

Әсіресе 2024 жылғы статистика назар аудартады. Аталған кезеңде 72 сағатқа дейін ұсталған кәмелетке толмағандардың саны 98 адамды құраса, 24 сағат шегінде ұсталғандар саны 124 адам болған. Бұл құқық қолдану практикасында ҚПК-нің 131-бабы төртінші бөлігін кеңейтілген түрде түсіндіру сақталып отырғанын көрсетеді.

Сонымен қатар статистикада ұстаудың заңды негіздерінің болмауына немесе процестік мерзімдердің бұзылуына байланысты босатылған кәмелетке толмағандар туралы мәліметтер де тіркелген. Атап айтқанда, заңды негіздердің болмауына байланысты:

— 2021 жылы - 1 адам;

— 2022 жылы - 6 адам;
— 2023 жылы - 15 адам;
— 2024 жылы - 26 адам босатылған.

Бұдан бөлек, ұстау мерзімдерінің өтіп кетуіне байланысты босату жағдайлары да орын алған:

— 2023 жылы - 3 адам;
— 2024 жылы - 1 адам [5].

Берілген мәліметтер кәмелетке толмағандарды ұстау мерзімдерін қолдану барысында құқық қолдану тәжірибесінде әлі де бірқатар проблемалардың бар екенін аңғартады. Әсіресе, қолданыстағы құқықтық нормаларды әртүрлі түсіндіру мүмкіндігі құқықтық реттеудің жеткілікті дәрежеде нақтыланбағанын көрсетеді.

Жүргізілген талдау нәтижелері кәмелетке толмағандарға қатысты 72 сағатқа дейін ұстауды қолдану тәжірибесі сирек кездесетін ерекше шара сипатынан біртіндеп алыстап, тәжірибеде жиі пайдаланылатын процестік мәжбүрлеу құралдарының біріне айналғанын байқатады. Мұндай жағдай Қазақстан Республикасы Конституциясының 18-бабында бекітілген бостандық кепілдіктерін, Бала құқықтары туралы конвенция талаптарын және Пекин қағидаларын ескере отырып, қылмыстық-процестік нормаларды нақтылау қажеттігін күшейтеді. Сонымен қатар сот практикасы үшін бірыңғай құқықтық түсіндіру қалыптастыру мәселесі де маңызды болып отыр.

Сондықтан бұл мәселені тек қылмыстық процесс шеңберіндегі техникалық немесе рәсімдік мәселе ретінде бағалау жеткіліксіз. Оның мазмұны құқықтық саясатпен, адам құқықтарын қорғау деңгейімен және құқық қолдану мәдениетімен тікелей байланысты.

Қазақстанда соңғы кезеңде «Заң және Тәртіп» қағидаты құқықтық саясаттың негізгі басымдықтарының бірі ретінде қарастырылып келеді. Дегенмен құқықтық мемлекетте қоғамдық тәртіпті қамтамасыз ету тек қатаң жазалау шараларымен немесе процестік шектеулермен ғана байланысты болмауы қажет. Бұл, ең алдымен, азаматтардың құқықтарының сақталу деңгейімен, заң нормаларының түсініктілігімен және оларды қолданудың тұрақты тәжірибесімен айқындалады.

Осыған байланысты кәмелетке толмағандарды ұстау мерзімдерін құқықтық реттеу мәселесі ерекше назар аударуды талап етеді. Қолданыстағы заңнамада 72 сағаттық ұстау мерзімін кәмелетке толмағандарға қолдану тәртібі нақты әрі бірмәнді көрсетілмеген. Сондықтан бұл мәселені заң деңгейінде нақтылау қажеттілігі туындайды.

Сонымен қатар кәмелетке толмағандарға қатысты 24 сағаттық ұстау мерзімін өзгертілмейтін процестік кепілдік ретінде бекіту орынды болып көрінеді. Мұндай тәсіл баланың құқықтарын қорғаудың халықаралық стандарттарына да сәйкес келеді.

Бұдан бөлек, құқық қолдану практикасында бірыңғай ұстаным қалыптастыру мақсатында Қазақстан Республикасы Жоғарғы Сотының 2020 жылғы 24 қаңтардағы №1 «Бұлтартпау шараларын санкциялаудың кейбір

мәселелері туралы» нормативтік қаулысына [6] тиісті толықтырулар енгізу ұсынылады:

«14-1. Соттар кәмелетке толмаған күдіктіге қатысты ҚР ҚПК-нің 131-бабы төртінші бөлігінде көзделген жиырма төрт сағаттық ұстау мерзімі оның бостандығына және жеке басына қол сұғылмаушылық құқығын қамтамасыз етуге бағытталған арнайы процестік кепілдік болып табылатынын ескеруге тиіс.

Осыған байланысты кәмелетке толмағандарға қатысты жиырма төрт сағаттан асатын ұстау мерзімін қолдануға, оның ішінде 131-бабы төртінші бөлігінде 1)-6) көрсетілген қылмыстар бойынша да, жол берілмейді.

Соттар бұл мәселені шешу кезінде Қазақстан Республикасы Конституциясының 18-бабының ережелерін, Бала құқықтары туралы конвенцияны, сондай-ақ кәмелетке толмағандарға қатысты сот төрелігін жүзеге асыруға байланысты Біріккен Ұлттар Ұйымының ең төменгі стандарттық қағидаларын (Пекин қағидалары) басшылыққа алуға тиіс.»

Құқық қорғау органдары қызметкерлерінің кәсіби құқықтық дайындығы мен құқықтық мәдениеті де бұл мәселеде шешуші рөл атқарады. Өйткені заңда көзделген кепілдіктердің іс жүзінде тиімді жұмыс істеуі тек нормативтік ережелердің мазмұнына емес, оларды қолданатын лауазымды тұлғалардың құқықты түсіну деңгейіне де тәуелді.

Бүгінде кәмелетке толмағандарды ұстау мерзімдерін құқықтық реттеу құқық қолдану саласындағы өзекті мәселелердің бірі ретінде қалып отыр.

ҚР ҚПК-де белгіленген 24 сағаттық және 72 сағаттық мерзімдердің арақатынасына қатысты нақты әрі бірізді құқықтық түсіндірудің болмауы тәжірибеде әртүрлі тәсілдердің қолданылуына алып келуде.

Бұл мәселе тек ғылыми пікірталас деңгейінде ғана емес. Оның салдары азаматтардың конституциялық құқықтарын шектеудің заңдылығына, жиналған дәлелдемелердің кейінгі бағалануына, сондай-ақ құқық қорғау органдарына деген қоғамдық сенім деңгейіне әсер етеді. Сонымен қатар халықаралық құқық талаптарын сақтау мәселесі де тікелей осыған байланысты.

Құқықтық мемлекет жағдайында кәмелетке толмағандарға қатысты кез келген процестік мәжбүрлеу шарасы барынша мұқият және негізді түрде қолданылуы қажет.

Сондықтан заңнаманы одан әрі жетілдіру барысында тергеу тиімділігі мен тұлғаның процестік құқықтарын қамтамасыз ету арасындағы тепе-теңдікті сақтау негізгі бағдарлардың бірі болуға тиіс.

Нәтижесінде құқықтық тәртіптің тиімділігі азаматтардың құқықтары мен бостандықтарын нақты қорғауға мүмкіндік беретін құқықтық тетіктердің сапасымен айқындалады.

---

1. Қазақстан Республикасының Конституциясы 2026 жылы 15 наурызда республикалық референдумда қабылданды // https://adilet.zan.kz/kaz/docs/K2600000000 Қарау уақыты 2026 жылғы 12 мамыр.
2. Қазақстан Республикасының Қылмыстық-процестік кодексі 2014 жылғы 4 шілдедегі № 231-V ҚРЗ (2026 жылғы 8 наурыздағы өзгерістермен) // https://adilet.zan.kz/kaz/docs/K1400000231 Қарау уақыты 2026 жылғы 12 мамыр.
3. Нью-Йоркте 1994 жылғы 16 ақпанда қол қойылған 1989 жылғы 20 қарашадағы Бала құқықтары туралы Конвенция. Қазақстан Республикасының Жоғарғы Кеңесінің 1994 жылғы 8 маусымдағы қаулысымен ратификацияланған. // https://zakon.uchet.kz/kaz/history/B940001400_/08.06.1994 Қарау уақыты 2026 жылғы 12 мамыр.

4. Біріккен Ұлттар Ұйымының Кәмелетке толмағантарға сот төрелігін орындауға қатысты минималды стандартты ережелер («Пекин ережелері») БҰҰ-ның Бас Ассамблея Бұрыштамасымен 1985 ж. 10 желтоқсан айында қабылданған // https://zakon.uchet.kz/kaz/docs/O8500000002 Қарау уақыты 2026 жылғы 12 мамыр.
5. Қазақстан Республикасы Бас прокуратурасы Құқықтық статистика және арнайы есепке алу комитетінің статистикалық деректері // https://www.gov.kz/memleket/entities/pravstat?utm_source=chatgpt.com
6. Қазақстан Республикасы Жоғарғы Сотының «Бұлтартпау шараларын санкциялаудың кейбір мәселелері туралы» 2020 жылғы 24 қаңтардағы № 1 нормативтік қаулысы (2024 жылғы 17 желтоқсандағы өзгерістермен) // https://adilet.zan.kz/kaz/docs/P200000001S Қарау уақыты 2026 жылғы 12 мамыр.

ПРОБЛЕМЫ УГОЛОВНО-ПРАВОВОЙ ЗАЩИТЫ НЕСОВЕРШЕННОЛЕТНИХ ЖЕРТВ СЕМЕЙНО-БЫТОВОГО НАСИЛИЯ В УСЛОВИЯХ ЦИФРОВИЗАЦИИ: СИСТЕМЫ ВЫЯВЛЕНИЯ И ОКАЗАНИЯ ПОМОЩИ

УТЕГЕНОВА Гульзат Амандыковна
Кыргызский Национальный университет имени Ж. Баласагына, Кыргызская Республика, г.Бишкек

В статье рассматриваются актуальные проблемы уголовно-правовой защиты несовершеннолетних жертв семейно-бытового насилия в условиях цифровизации системы выявления и оказания помощи. Исследуются криминологические и виктимологические особенности насилия в отношении несовершеннолетних, причины высокой латентности подобных преступлений, а также факторы, препятствующие своевременному обращению детей за помощью. Особое внимание уделено современным цифровым механизмам выявления насилия, включая мобильные приложения, анонимные платформы обращения и системы дистанционного взаимодействия с уполномоченными органами. Проанализированы отдельные зарубежные подходы к использованию цифровых технологий в сфере защиты детей от семейно-бытового насилия. Сделан вывод о необходимости совершенствования уголовно-правовых, организационных и цифровых механизмов предупреждения насильственных преступлений в семейно-бытовой сфере, а также формирования безопасной цифровой среды для несовершеннолетних потерпевших.

Проблема семейно-бытового насилия в отношении несовершеннолетних в последние годы приобретает все более острый характер, поскольку затрагивает не только сферу охраны личности, но и вопросы общественной безопасности, устойчивости института семьи и профилактики насильственной преступности. Особую тревогу вызывает высокая латентность подобных деяний. Значительная часть несовершеннолетних жертв не обращается за помощью из-за психологической зависимости от агрессора, страха, недоверия к государственным институтам и отсутствия безопасных каналов коммуникации. Вследствие этого реальные масштабы насилия существенно превышают официальные статистические показатели, что осложняет деятельность правоохранительных органов и снижает эффективность уголовно-правовой защиты детей [1].

Современные процессы цифровизации постепенно изменяют подходы к выявлению и предупреждению насильственных преступлений в семейно-бытовой сфере. Развитие цифровых платформ, мобильных приложений, систем анонимного обращения и технологий дистанционного взаимодействия создает новые механизмы оказания помощи несовершеннолетним жертвам насилия. Особое значение подобные инструменты приобретают в условиях, когда ребенок фактически лишен возможности лично обратиться в правоохранительные органы либо сообщить о совершаемом насилии ближайшему окружению. Международная практика показывает, что цифровые технологии рассматриваются как дополнительный элемент системы раннего выявления виктимизации несовершеннолетних и профилактики повторного насилия. В шведской практике, например, активно развиваются цифровые сервисы

поддержки детей, подвергающихся домашнему насилию, ориентированные на обеспечение анонимности, безопасности и оперативного взаимодействия со службами помощи [2].

Дополнительную актуальность теме придают современные государственные программы цифровой трансформации. В Республике Казахстан вопросам цифровизации и внедрения технологий искусственного интеллекта в деятельность государственных институтов уделяется повышенное внимание. Указом Президента Республики Казахстан 2026 год объявлен Годом цифровизации и искусственного интеллекта, что подчеркивает стратегическую значимость внедрения цифровых решений в различные сферы общественной жизни, включая обеспечение безопасности граждан и совершенствование механизмов противодействия преступности [3]. В послании Главы государства отдельно подчеркивается необходимость формирования интеллектуальных систем противодействия современным угрозам и модернизации государственного управления на основе цифровых технологий [4]. Подобные тенденции позволяют рассматривать цифровые механизмы помощи несовершеннолетним жертвам семейно-бытового насилия не как вспомогательный элемент, а как перспективное направление развития уголовно-правовой и виктимологической политики государства.

Научный интерес к рассматриваемой проблематике обусловлен также междисциплинарным характером темы [5]. Вопросы уголовно-правовой защиты несовершеннолетних тесно связаны с положениями криминологии, виктимологии, цифрового права и проблемами обеспечения информационной безопасности личности. Особое значение приобретает анализ возможностей цифровых технологий в сфере раннего выявления латентного насилия, фиксации противоправных действий, оперативного реагирования уполномоченных органов и формирования безопасной среды для обращения несовершеннолетних за помощью. При этом внедрение цифровых инструментов порождает и новые риски, связанные с защитой персональных данных детей, конфиденциальностью обращений и пределами вмешательства государства в семейную сферу [6].

Цель статьи заключается в анализе проблем уголовно-правовой защиты несовершеннолетних жертв семейно-бытового насилия в условиях цифровизации системы выявления и оказания помощи.

Для достижения поставленной цели были определены следующие задачи:

1.Рассмотреть особенности уголовно-правовой и виктимологической характеристики семейно-бытового насилия в отношении несовершеннолетних.

2.Проанализировать современные цифровые механизмы выявления и оказания помощи несовершеннолетним жертвам насилия, а также проблемы их правового регулирования.

Объектом статьи выступают общественные отношения, возникающие в сфере уголовно-правовой защиты несовершеннолетних жертв семейно-бытового насилия.

Предмет статьи составляют нормы уголовного законодательства, материалы правоприменительной практики, положения криминологии и

виктимологии, а также цифровые механизмы выявления и оказания помощи несовершеннолетним жертвам насилия.

Уголовно-правовая и виктимологическая характеристика семейно-бытового насилия в отношении несовершеннолетних

Семейно-бытовое насилие в отношении несовершеннолетних представляет собой одну из наиболее сложных и социально опасных форм насильственной преступности, поскольку затрагивает базовые механизмы физической и психологической безопасности ребенка. Особенность подобных деяний заключается не только в причинении непосредственного вреда личности несовершеннолетнего, но и в разрушении доверительных внутрисемейных связей, формировании устойчивых психотравмирующих последствий и высокой вероятности последующей социальной дезадаптации жертвы. В отличие от иных категорий потерпевших несовершеннолетние зачастую находятся в полной материальной, эмоциональной и психологической зависимости от лица, совершающего насильственные действия, вследствие чего возможность самостоятельного обращения за защитой оказывается существенно ограниченной [7].

Уголовно-правовая охрана несовершеннолетних в государствах постсоветского пространства строится на признании повышенной общественной опасности преступлений, совершаемых против детей. В уголовном законодательстве предусматриваются специальные квалифицирующие признаки, связанные с возрастом потерпевшего, зависимым положением ребенка и использованием беспомощного состояния несовершеннолетнего [8]. Вместе с тем практическая реализация данных норм сталкивается с рядом серьезных проблем. Одной из ключевых остается высокая латентность семейно-бытового насилия. Значительная часть преступлений длительное время остается вне поля зрения правоохранительных органов, поскольку насильственные действия совершаются в закрытой семейной среде, а несовершеннолетние боятся сообщать о происходящем из-за страха наказания, чувства вины либо эмоциональной привязанности к агрессору [1].

Криминологический анализ показывает, что семейно-бытовое насилие в отношении детей обладает устойчивым циклическим характером. Во многих случаях противоправное поведение носит систематический характер и постепенно усиливается. Первоначальные формы психологического давления или эмоционального унижения со временем трансформируются в физическое насилие, жестокое обращение либо сексуальную эксплуатацию [9]. Дополнительную опасность представляет тот факт, что несовершеннолетние нередко воспринимают агрессивное поведение внутри семьи как норму повседневного взаимодействия. Подобное восприятие существенно осложняет своевременное выявление преступлений и формирует предпосылки для дальнейшей виктимизации личности.

С виктимологической точки зрения несовершеннолетние относятся к категории наиболее уязвимых жертв насильственной преступности [10]. Возрастные особенности психики, ограниченный жизненный опыт, зависимость от взрослых и неспособность объективно оценивать противоправный характер

происходящего существенно повышают риск повторной виктимизации. Особую роль играет психологический механизм так называемой «травматической привязанности», при котором ребенок продолжает эмоционально зависеть от лица, причиняющего вред [11]. В подобных условиях даже очевидные признаки насилия могут скрываться потерпевшим, а любые попытки вмешательства со стороны государства воспринимаются несовершеннолетним как угроза разрушения семьи.

Отдельного внимания заслуживает проблема цифровой латентности насильственных преступлений в семейно-бытовой сфере. Современные технологии не только создают дополнительные механизмы выявления насилия, но и используются самими правонарушителями для контроля над несовершеннолетними [12]. Речь идет о мониторинге переписки, ограничении доступа к средствам связи, психологическом давлении через цифровые платформы и использовании угроз распространения личной информации. В результате цифровая среда становится одновременно пространством потенциальной помощи и дополнительным инструментом виктимизации ребенка.

Международные исследования демонстрируют, что последствия семейно-бытового насилия оказывают долгосрочное влияние на психическое и социальное развитие несовершеннолетних. У детей, систематически подвергавшихся насилию, значительно чаще фиксируются депрессивные состояния, тревожные расстройства, нарушения эмоционального контроля и склонность к агрессивному поведению во взрослом возрасте [13]. Кроме того, сохраняется высокий риск воспроизводства насильственных моделей поведения уже в собственной семье потерпевшего [14]. Подобная тенденция превращает семейно-бытовое насилие не только в проблему конкретной семьи, но и в фактор воспроизводства преступности в обществе.

Сложность рассматриваемой проблемы обусловлена также недостаточной координацией между правоохранительными органами, образовательными учреждениями, медицинскими организациями и социальными службами. Во многих случаях информация о признаках насилия остается фрагментарной и не приводит к своевременному вмешательству. Отсутствие единого механизма обмена данными, сложность межведомственного взаимодействия и недостаточная цифровая интеграция государственных структур существенно снижают эффективность предупреждения насильственных преступлений против несовершеннолетних [15].

На современном этапе уголовно-правовая защита несовершеннолетних жертв семейно-бытового насилия требует комплексного подхода, сочетающего меры уголовно-правового воздействия, криминологической профилактики и цифровых механизмов раннего выявления угроз. Особое значение приобретает формирование безопасной системы обращения несовершеннолетних за помощью, способной обеспечить конфиденциальность, оперативность реагирования и минимизацию риска повторной виктимизации. Именно поэтому дальнейшее развитие цифровых механизмов выявления и оказания помощи

постепенно становится одним из ключевых направлений модернизации системы защиты детей от насильственных преступлений [16].

Проведенное исследование показало, что семейно-бытовое насилие в отношении несовершеннолетних представляет собой одну из наиболее латентных и социально опасных форм насильственной преступности, оказывающую негативное влияние на физическое, психическое и социальное развитие ребенка. Особая уязвимость несовершеннолетних потерпевших обусловлена их зависимым положением, психологической привязанностью к агрессору, страхом обращения за помощью и ограниченными возможностями самостоятельной защиты своих прав.

Установлено, что действующие механизмы уголовно-правовой защиты несовершеннолетних жертв семейно-бытового насилия не в полной мере учитывают современные цифровые формы выявления и предупреждения насилия. Несмотря на активное развитие цифровизации государственного управления, существующая система профилактики бытового насилия остается преимущественно ориентированной на традиционные способы обращения в правоохранительные и социальные органы, что существенно снижает эффективность раннего выявления латентных форм насилия в отношении детей.

Проведенный анализ показал, что цифровые технологии способны существенно повысить эффективность выявления насильственных преступлений в семейно-бытовой сфере посредством внедрения анонимных цифровых платформ обращения, мобильных приложений экстренной помощи, систем дистанционного взаимодействия с уполномоченными органами, а также межведомственного цифрового обмена информацией. Особое значение подобные механизмы приобретают для несовершеннолетних потерпевших, которые зачастую не имеют возможности безопасного личного обращения за защитой.

В связи с этим представляется целесообразным совершенствование отдельных положений законодательства Республики Казахстан в сфере профилактики семейно-бытового насилия. В частности, предлагается дополнить Закон Республики Казахстан «О профилактике правонарушений» [17] нормами, предусматривающими:

-создание цифровых механизмов анонимного обращения несовершеннолетних жертв насилия;

-внедрение защищенных мобильных приложений экстренной помощи детям;

-развитие единой межведомственной цифровой системы взаимодействия правоохранительных органов, организаций образования, органов опеки и социальных служб;

-обеспечение конфиденциальности цифровых обращений несовершеннолетних потерпевших;

-использование цифровых технологий раннего выявления признаков насилия в отношении детей.

Кроме того, представляется необходимым разработать единые организационные стандарты цифрового сопровождения несовершеннолетних

жертв семейно-бытового насилия, включающие алгоритмы оперативного реагирования, порядок межведомственного обмена информацией и гарантии защиты персональных данных детей. Реализация указанных мер позволит повысить эффективность предупреждения насильственных преступлений, снизить уровень их латентности и обеспечить более высокий уровень уголовно-правовой защиты несовершеннолетних в условиях цифровой трансформации современного общества.

1. **Kachynska M.O.** Causes of Domestic Violence Latency //JE Eur. L. – 2016. – P. 27.
2. **Valan L., Isaksson U., Hörnsten Å., Carlsund Å.** Evaluating the Impact of Digital Support on Parental Stress in Swedish Child Health Care: Results From an Intervention Study // International Journal of Pediatrics. – 2025. – Vol. 2025. – Article 8780069. – 8 p. – DOI: 10.1155/ijpe/8780069
3. Указ Президента Республики Казахстан № 1151 «Об объявлении Года цифровизации и искусственного интеллекта» от 6 января 2026 года // https://adilet.zan.kz/rus/docs/U2600001151 (дата обращения: 01.05.2026г.)
4. Послание Главы государства Касым-Жомарта Токаева народу Казахстана «Казахстан в эпоху искусственного интеллекта: актуальные задачи и их решения через цифровую трансформацию» от 8 сентября 2025 года // https://adilet.zan.kz/rus/docs/K25002025_1 (дата обращения: 01.05.2026г.)
5. **Ramesh K.** Criminology and penology with victimology //Pedagogy. – 2025. – Vol. 1. – P. 18.
6. Gasser M. et al. The Digital distributed system security architecture //Proceedings of the 12th National Computer Security Conference. – 1989. – P. 305-319.
7. **Mitchell K. J., Finkelhor D.** Risk of crime victimization among youth exposed to domestic violence //Journal of Interpersonal violence. – 2001. – Vol. 16. –№. 9. – P. 944-964.
8. Нормативное постановление Верховного Суда Республики Казахстан N 6 «О судебной практике по делам об уголовных правонарушениях несовершеннолетних и о вовлечении их в совершение уголовных правонарушений и иных антиобщественных действий» от 11 апреля 2002 года // https://adilet.zan.kz/rus/docs/P02000006S (дата обращения: 01.05.2026г.)
9. **Akers T.A., Hervey W.G., Billington-Hughes T.** Triggers of brutality: Unraveling the dialectics of extreme violence through an epidemiological criminology lens //Research Handbook on Violent Crime and Society. – Edward Elgar Publishing, –2025. – P. 620-636.
10. **Kuatova A.** et al. Challenges of Victimological Prevention of Criminal Offences against Minors //International Annals of Criminology. – 2025. – P. 1-22.
11. **Doroudchi A.** et al. Psychological complications of the children exposed to domestic violence: a systematic review //Egyptian journal of forensic sciences. – 2023. – Vol. 13. – №. 1. – P. 26.
12. **Harris B.A., Woodlock D.** Digital coercive control: Insights from two landmark domestic violence studies //The British Journal of Criminology. – 2019. – Vol. 59. – №. 3. – P. 530-550.
13. **Chemtob C.M., Carlson J.G.** Psychological Effects of Domestic Violence on Children and Their Mothers //International Journal of Stress Management. – 2004. – Vol. 11. – №. 3. – P. 209.
14. **Haselschwerdt M.L., Savasuk-Luxton R., Hlavaty K.A** methodological review and critique of the «intergenerational transmission of violence» literature //Trauma, Violence, & Abuse. – 2019. – Vol. 20. – №. 2. – P. 168-182.
15. **Pardo T.A., Tayi G.K.** Interorganizational information integration: A key enabler for digital government //Government information quarterly. – 2007. – Vol. 24. – №. 4. – P. 691-715.
16. **Wahyu M.A.** Child Protection in the Digital Ecosystem under the Convention on the Rights of the Child //E-Justice: Journal of Law and Technology. – 2025. – Vol. 1. – №. 2. – P. 1-14.
17. Закон Республики Казахстан № 245-VIII ЗРК «О профилактике правонарушений» от 30 декабря 2025 года // https://adilet.zan.kz/rus/docs/Z2500000245#z1020 (дата обращения: 01.05.2026г.).

АНАЛОГИ ЦЕНТРОВ ОПЕРАТИВНОГО УПРАВЛЕНИЯ В ЗАРУБЕЖНЫХ ПОЛИЦЕЙСКИХ ПРАКТИКАХ: СХОДСТВА, РАЗЛИЧИЯ, ВОЗМОЖНЫЕ ПУТИ УЧЕТА ЭФФЕКТИВНЫХ МЕТОДИК

ШАУДЫРОВ Темирбек Сатемирович
Докторант 1 курса факультета послевузовского образования
Академии управления МВД Республики Казахстан
магистр национальной безопасности и военного дела

В статье рассматривается зарубежный опыт функционирования командно-координационных, ситуационных и аналитических центров полиции, функционально близких к центрам оперативного управления органов внутренних дел Республики Казахстан (ЦОУ). Обосновывается, что в современных условиях противодействие преступности требует перехода от преимущественно реактивной модели реагирования к модели ситуационного управления, основанной на оперативной обработке информации, межведомственной координации, цифровой аналитике и поддержке принятия управленческих решений в режиме реального времени. Особое внимание уделяется опыту США, Сингапура, Великобритании, Гонконга и Индии, где применяются различные организационные модели: Real-Time Crime Centers, Police Operations Command Centre, Gold-Silver-Bronze command structure, Regional Command and Control Centres и Integrated Command and Control Centres. На основе сравнительного анализа выделяются элементы, представляющие интерес для совершенствования деятельности казахстанских ЦОУ - развитие аналитического блока, интеграция видеонаблюдения и городских информационных систем, регламентация работы с цифровыми данными, подготовка специализированных кадров и внедрение измеримых критериев эффективности реагирования.

Центры оперативного управления (далее - ЦОУ) являются по структуре своего функционала своего рода командно-координационными центрами, основной функционал которых концентрируется на вопросах ситуационного реагирования на правонарушающее и криминальное поведение. К настоящему времени в большинстве стран мирового сообщества фактически сложилась такая криминологическая идеологема, в контексте которой предупредительное и оперативно-купирующее воздействие на правонарушения и (или) преступления определяется в качестве задачи первостепенного порядка. Во многом этому способствовало повышения уровня технического развития общества, благодаря которому тотально сократилось время на обмен значимой информацией, возник фактор проницаемости городской среды. Однако решающим моментом следует все-таки считать именно фактор перехода к новой концепции воздействия на правонарушения, когда случилось осмысление «цены преступности» на фоне которой затраты на предупреждение (выявление, пресечение) правонарушений стали представляться гораздо более социально-рентабельным решением, нежели рост расходов на содержание механизма карательного воздействия.

В этом смысле образование в РК центров оперативного управления стало одновременно и организационным решением, и органичным продолжением соответствующей новой концепции противодействия преступности. К настоящему времени ЦОУ представляют собой не просто дежурные подразделения, а особый организационно-технический механизм оперативного (ситуационного)

реагирования в режиме круглосуточного получения, обработки информации и реагирования на соответствующие события и сигналы. Функции казахстанских ЦОУ сосредоточены на нескольких основных направлениях: 1) информативно-кумулятивная (прием, обработка и учет оперативной информации, получаемой, в том числе, посредством видеонаблюдения); 2) объектно-наблюдательная (мониторинг криминогенной и общественной обстановки); 3) командно-координационная (оперативное управление нарядами и силами полиции, координация реагирования); 4) обеспечительная (первичная обработка, надлежащая фиксация информации для обеспечения качества последующих решений).

Научно-исследовательский компонент оценки деятельности ЦОУ (равно как и их зарубежных аналогов) до настоящего времени существенно уступает ведомственно-нормативной регламентации. При этом, как совершенно справедливо отмечается в отдельных исследованиях, «решение задач управления силами и средствами невозможно без проведения аналитической деятельности, осуществляемой на основе мониторинга событий, анализа причин их возникновения и возможных последствий, а также прогнозирования развития оперативной обстановки, контроля выполнения принятых решений как в штатных, так и в нештатных ситуациях» [1, С.3]. Акценты, как правило, производятся на оценке потенциала ситуационного реагирования, а также на тех организационных дефектах и затруднениях, которые возникают в процессе организации и осуществления соответствующей деятельности. В частности, отмечается, что в качестве основных достоинств ситуационного управления можно назвать такие аспекты, как возможность достижения высокой оперативности принятия решения в условиях дефицита времени; обеспечение принятия эффективных решений; высокая степень универсальности применения по отношению к уровням управления (масштабируемость) и отраслям деятельности, высокая мобильность, т. е. готовность к применению в любое время и в любых условиях и др. [1, С.3].

При этом значимо, что независимо от организационной формы сама идея ситуационного управления есть «совокупность приемов и методов подготовки и принятия управленческих решений по управлению разнородными силами и средствами для контроля оперативной обстановки в реальном масштабе времени» [3, С.42]. Весьма значимым аспектом в данном случае является акцент на том, что ситуационное управление - это именно «управление», а не просто сбор максимально возможного количества информации посредством технических устройств и иных организационно-коммуникационных механизмов. Это означает, что соответствующая информация, во-первых, должна быть соответствующим образом принята, обработана, а также использована в последующей аналитической деятельности. Выход за пределы работы по принципу «дежурных суток», очевидно, должен стать одним из перспективных направлений деятельности казахстанских ЦОУ. В этом смысле совершенно справедливо утверждение, что «…ситуационное управление - это не только и не столько работа с массивами данных. Прежде всего необходим процесс предвидения, упреждения и обеспечения руководства реальными рабочими решениями по различным ситуациям» [3, С.42].

Изучение зарубежного опыта организации и функционирования аналогичных систем ситуационного командно-координационного реагирования является одним из наиболее эффективных инструментов для повышения качества его организации в рамах национальной юрисдикции. Общие тенденции, которые имеют место в большинстве стран мирового сообщества в контексте современной модели противодействия преступности привели к тому, что и организационные решения, перестройка функционала полицейских служб происходили в рамках аналогичных тенденций. К настоящему времени в значительном количестве зарубежных полицейских практик имеются аналоги ЦОУ, хотя утверждать наличие однозначно идентичной модели все-таки нельзя. При этом специфика нередко формируется вокруг не столько отдельно взятых функций и направлений деятельности, сколько в аспекте их сочетания и взаимодополняемости. Особенности функционирования того или иного командно-координационного подразделения в отдельно взятой стране зависит от большого количества факторов - начиная от самой модели полиции, интенсивности ее сотрудничества с местным сообществом, заканчивая такими факторами, как административно-территориальное устройство, специфика организации экстренных вызовов, уровень цифровой инфраструктуры, особенность распределения полномочий между отдельными службами (911/112, местными органами управления, органами реагирования на чрезвычайные ситуации и т.д.).

Так, в частности, Real-Time Crime Centers (RTCC) - Центр преступлений в реальном времени в США. Эти центры в США можно назвать одним из наиболее полных аналогов казахстанских ЦОУ, однако будет справедливым указать, что их функционал все-таки имеет некоторые отличия в контексте степени решения задач именно оперативного реагирования. Основное различие заключается в том, что казахстанские ЦОУ в большей степени функционируют все-таки в качестве дежурно-управленческого звена, задачи которого полностью сосредоточены и ограничиваются именно в режиме дежурного реагирования. Real-Time Crime Centers (RTCC) в качестве своего предназначения имеют централизованную обработку оперативной информации, поддержке реагирования на угрозы в режиме реального времени, использование видеонаблюдения, баз данных, аналитических инструментов, а также на передаче значимой информации сотрудникам полиции.

Таким образом, Real-Time Crime Centers (RTCC) гораздо в большей степени ориентированы именно на аналитику, техническую поддержку расследований, но также и на ситуационную осведомленность. В данном случае особо примечательно, что в структуру функционала Real-Time Crime Centers (RTCC) входит, в том числе, мониторинг социальных сетей на предмет выявления, в первую очередь, острых ситуационных угроз. В частности, в докладе RAND (американская некоммерческая исследовательская организация) отмечается, что включение социальных сетей в функционал оперативных полицейских центров представляет собой не сплошной (фоновый) мониторинг, требует специальной подготовки с точки зрения обеспечения защиты частной жизни и иных гарантий[i]. То есть в данном случае речь идет в большей степени о тех или иных реальных публичных действиях (их вербализации), которые могут нести в себе определенные криминальные риски.

В исследовательском обзоре, опубликованном Национальным центром правосудия в США и непосредственно посвященном функционированию Real Time Crime Centers, отмечается, что RTCC представляют собой специализированное подразделение общественной безопасности, которое осуществляет прием и мониторинг приоритетных вызовов или значимых событий, просмотр и анализ поступающих видеосигналов, поиск по камерам, архивным записям, считывание номерных знаков, информированием патрульных и следователей, формирование оперативных ориентировок и первичных следственных версий, а также поддержку на месте совершения преступления участников криминального события [2, -80 с. С 8].

Также в аналитическом докладе Бюро содействия правосудию Минюста США прямо отмечается, что функционал RTCC в большей степени ориентирован на предоставлении релевантной значимой информации патрульным и следователям (детективам) [2,-80 с. С8], что свидетельствует о явном преобладании аналитическо-обеспечительной функции над «дежурной». Специфику данной функции определяет исключительно тот фактор, что она сопряжена именно с режимом «реального времени» (что и является признаком, объединяющим данные центры с казахстанскими ЦОУ). С другой стороны, RTCC это и не просто «комнаты с камерами», поскольку в их задачи, как и в контексте работы ЦОУ, входит также и поддержка операций на месте, помощь в принятии тактических решений.

Примечательно, что работы RTCC могут организовываться круглосуточно только в крупном городе, что же касается небольших населенных пунктов, то здесь могут определяться наиболее криминогенные временные интервалы. Учитывая то обстоятельство, что работа RTCC до настоящего времени проходит определенную организационно-функциональную эволюцию, в публикациях и аналитический обзорах настоятельно рекомендуется максимально расширять их функционал именно до поддержи мероприятий, связанных с криминальным инцидентом, то есть повышать акцент на оперативное реагирование. Кроме того, примечателен и опыт кадрового укомплектования RTCC, которое основано не только на сотрудниках правоохранительных органов и криминальных аналитиков, но и включает «гражданских» лиц», в первую очередь, технических специалистов (по видеонаблюдению) и специалистов IT. Наиболее типичным режимом работы RTCC к настоящему времени является 10-часовой график (с 07.00 до 03.00), при этом к значимым качествам кандидатов относятся технические и аналитические навыки, а также самостоятельность в совокупности с навыками работы в команде, креативность, осведомленность о ресурсном потенциале центра и т.д. Что касается руководства сменой, что является важной координирующей составляющей, то данный вопрос преимущественно связывается не столько с руководящей должностью (что характерно для организации деятельности ОВД в РК), сколько с практикой возложения соответствующей функции, то есть руководство в разные смены может осуществляться разными сотрудниками.

Как было отмечено в начале данной статьи, предупредительный вектор воздействия на правонарушения и преступления связан не только с ценностным компонентом, но и с рациональным элементом, который заключается в том, чтобы уровень затраченных усилий (кадровых, технических, финансовых и др.)

соответствовал позитивным ожиданиям. То есть предполагается необходимость подтверждения, что внедрение соответствующих практик ситуационного реагирования дает более или менее заметные результаты. Конечно же, оценка данных результатов не может быть достоверной в рамках краткосрочных периодов. Именно по этой причине исследователи эффективности RTCC с достаточной осторожностью пока указывают на некоторые положительные сдвиги. В частности, относительно ситуации в Чикаго в специальной научной публикации было отмечено, что за три года было достигнуто повышение на 5 % раскрываемости насильственных преступлений, на 12% - имущественных, на 11 % - иных общеуголовных преступлений[ii]. При этом подвергался также анализу большой массив исследовательских данных (34 региональных исследований), на основе которых четкого подтверждения тому, что RTCC способствуют предотвращению преступности, пока с достаточной долей достоверности установить нельзя [4, С. 80].

По отдельным внешне-организационным маркерам в качестве одной из наиболее близких моделей командно-координационной полицейской деятельности в режиме «реального времени» можно назвать практику функционирования подобных центров в Сингапуре (Police Operations Command Centre). Структурно управление данным подразделением включает нескольких лиц, которые осуществляют руководство работой центра в различных направлениях – непосредственно руководитель, его заместитель, а также руководители по отдельным направлениям (по разработке мероприятий и по управлению мероприятиями). В контексте оценки опыта Сингапура в сравнении с опытом регламентации и функционирования ЦОУ в РК важно отметить, что есть как значимая объединяющая составляющая (элемент реального «дежурного» сопровождения), так и заметный отличительный аспект, который заключается в том, что помимо смен оперативного реагирования действует также направление операционного развития, связанное с совершенствованием алгоритмов, цифровых решений, стандартов диспетчеризации, а также межведомственного обмена[5].

Близким аналогом сингапурской модели можно назвать и организацию командно-координационной функции полиции в Великобритании, наиболее сильным элементом которой также является четкая внутренняя дифференциация функций, которая имеет образное наименование «Gold, Silver, Bronze» (дословно: «золото-серебро-бронза»), где «золото» - осуществление стратегического руководства; «серебро» - реализация тактического управления, а «бронза» - непосредственное выполнение задач на месте. Причем, данный функционал используется не только непосредственно полицейским ведомством, но также и иными экстренными службами и заинтересованными партнерами с явным приоритетом реагирования на спонтанные инциденты, но и также в сочетании с выполнением плановых мероприятий. В данной модели ценными представляются такие элементы, как выраженная вертикализация и алгоритмизация управленческих решений (причем, вертикализация в данном случае в большей степени функциональная, а не формально-служебная). Выработка четких алгоритмов относительно оперативного реагирования на ситуации различного типа (обычное происшествие, осложненное происшествие, массовое мероприятие, ЧС,

террористическая угроза, межрегиональная операция и т.д.) обеспечивает четкую координацию действий, понятные границы свободы и ответственности за принятие решений [5].

Имеются элементы сходства также и с работой аналогичных центров оперативного реагирования Гонконга (Regional Command and Control Centres). Сходство в данном случае определяется несколькими компонентами: организация работы по территориальному признаку (региональные и районный уровни), кумуляция информации для ее передачи в центральные подразделения и другие заинтересованные и функционально задействованные органы, прием звонков в режиме «реального времени», а также организационное сопровождение сотрудников посредством компьютеризованной системы [5].

Схожие центры функционируют и в Индии (Integrated Command and Control Centres). Специфика данной модели заключается в том, что она является по своему характеру более тотальной, поскольку интегрирует работу полиции, экстренных служб и городских муниципалитетов в рамках единой платформы. Например, в Лудхиане объединение систем беспроводного управления дорожным движением и экстренной диспетчерской службы с использованием программ AI (ИИ) привело к тому, что среднее время реагирования на инциденты сократилось с 15 до 7 минут. В г. Коимбатор полиция осуществила интеграцию собственных камер также с камерами частных организаций, что позволило расширить возможности круглосуточного наблюдения, более эффективного раскрытия преступлений, заметного сокращения времени реагирования [6].

Таким образом, проведенный сравнительный анализ зарубежного опыта функционирования командно-координационных ситуационных полицейских центров в отдельных странах позволяет сформулировать ряд выводов, имеющих значение для дальнейшего совершенствования деятельности ЦОУ РК:

- перспективным направлением модернизации ЦОУ является переход от преимущественно дежурно-диспетчерской модели к модели ситуационно-аналитического управления, при которой ЦОУ не должны восприниматься только как место приема сообщений, наблюдения за видеокамерами и направления нарядов. В ближайшей перспективе их функционал должен включать мониторинг оперативной обстановки, анализ причин и возможных последствий событий, прогнозирование развития ситуации, подготовку вариантов управленческих решений и др.;

- перспективным является развитие единого информационного пространства, в рамках которого данные полиции, экстренных служб, городских систем видеонаблюдения, транспортной инфраструктуры и иных источников могут использоваться для формирования целостной картины оперативной обстановки;

- эффективность работы ЦОУ зависит не только от технического оснащения, но и от профессионального состава сотрудников. Наряду с сотрудниками полиции, обладающими практическим опытом реагирования и пониманием оперативной обстановки, в работу таких центров должны вовлекаться криминальные аналитики, IT-специалисты, специалисты по видеонаблюдению, обработке данных, геоинформационным системам и информационной безопасности;

- при заимствовании зарубежного опыта необходимо учитывать правовые и этические пределы использования цифровых технологий. Работа с видеонаблюдением, социальными сетями, открытыми источниками, биометрическими инструментами и базами данных должна быть строго регламентирована. В данном случае соответствующие источники информации допустимо рассматривать только как специализированный инструмент выявления конкретных угроз и информационного сопровождения;

- результативность деятельности ЦОУ должна оцениваться с использованием измеримых показателей - среднее время приема и обработки сообщения, время передачи информации наряду, время прибытия на место происшествия, доля происшествий, по которым использовались видеоданные и т.д., но больше с точки оценки эффективности самой структуры, а не отдельно взятых сотрудников;

- повышение эффективности ЦОУ должно быть связано с их постепенным превращением в интеллектуальные командно-координационные центры, способные не только реагировать на уже совершенные правонарушения, но и выявлять признаки осложнения оперативной обстановки, прогнозировать развитие угроз, обеспечивать своевременный маневр силами и средствами, а также формировать управленческие решения, направленные на предупреждение и пресечение криминальных проявлений.

1.**Терентьев А.А.** Модели и алгоритмы аналитической деятельности ситуационной деятельности органов внутренних дел: автореф. дис…канд. технич. наук. - Воронеж, 2022. - С. 3.
2.Ситуационное управление в деятельности органов внутренних дел: курс лекций / [**В.Б. Княжев и др**.]. - М. : Академия управления МВД России, 2020. - 80 с. С. 8
3.**Лукашов Н.В.** Методические аспекты обучения руководителей органов внутренних дел Российской Федерации основам теории и организации ситуационного управления // Труды Академии МВД России. - 2022. - № 1 (61) -. С. 42.
4.**Княжев В.Б., Грищенко Л.Л., Егоров К.А.** О перспективных направлениях совершенствования ситуационного управления в органах внутренних дел // Труды Академии управления МВД России. 2021. № 2 (58). С. 80.
5.**Hollywood J.S., Vermeer M. J.D., Woods D., Goodison S.E., Jackson B.A.** Using Social Media and Social Network Analysis in Law Enforcement: Creating a Research Agenda, Including Business Cases, Protections, and Technology Needs. Santa Monica, CA: RAND Corporation, 2018. Report No. RR-2301-NIJ. 28 p.
6.Real-Time Crime Centers: Integrating Technology to Enhance Public Safety. Washington, DC: National Institute of Justice, April 2025. NCJ 310472. 24 p.
7.Charlotte-Mecklenburg Police Department, North Carolina: Case Study. Washington, DC: Bureau of Justice Assistance, U.S. Department of Justice, [s. a.]. 21 p.
8.**Arrietti R.** Do real-time crime centers improve case clearance? An examination of Chicago's strategic decision support centers // Journal of Criminal Justice. 2024. Vol. 90. Article 102145.
9.**Peterson B.E., Lawrence D.S.** The nexus of data and technology: a scoping review of established and emerging law enforcement intelligence centers // Police Practice and Research. 2025.
10.**Muggah R., Soh C.** Smart CCTVs for Secure Cities: Potentials and Challenges. Singapore: S. Rajaratnam School of International Studies, Nanyang Technological University, 2017.
11.**Pearce T., Fortune J.** Command and control in policing: a systems assessment of the gold, silver and bronze structure // Journal of Contingencies and Crisis Management. 1995. Vol. 3. No. 3. P. 181-187.
12.Hong Kong: The Facts - Emergency Services. Hong Kong: Information Services Department, Government of the Hong Kong Special Administrative Region, 2025.
13.**Praharaj S.** Command and control governance in the 100 smart cities mission in India: Urban innovation or utopias? // Applied Geography. 2025. Vol. 184. Article 103766.

МАЗМҰНЫ
СОДЕРЖАНИЕ
CONTENS

ҚҰРМЕТ СӨЗ **ДИЛЬБАРХАНОВА Ж.Р.** **АКИМЖАНОВ Т.К.**	**2-3**
О поиске новых путей противодействия преступности в современных условиях и обеспечения закона и порядка в Республике Казахстан **АБЕНОВ А.А.**	**4-15**
Правовая система в эпоху глобальной трансформации: современные угрозы цифровой безопасности и перспективы международного правового сотрудничества **АБЕНОВ Р.Т.**	**16-24**
Ішкі істер органдарының құқық қолдану қызметі саласындағы қазіргі заманғы сын-қатерлері **АБУБАКИРОВА Г.М.**	**25-29**
Невзаимозаменяемые токены как элемент механизма предупреждения незаконного вывода цифровых активов в Республике Казахстан **АСКАРОВ А.А.**	**30-35**
К вопросу о понятиях «Объект» и «Цифровой объект» в действующем праве Республики Казахстан **АХМЕТОВ К.Р.**	**36-44**
Цифровизация правоприменительной деятельности: риски, перспективы и трансформация юридической ответственности в условиях глобальных вызовов **ВОЗНЯК О.А., НИЕТУЛЛАЕВ Н.Н.**	**45-52**
Новые составы в УК РК: теоретические и практические проблемы процесса (ДЕ) криминализации **ДАЕТОВА А.А.**	**53-56**
Трансформация правовых институтов обеспечения общественной безопасности на воздушном транспорте в условиях глобализации и цифровизации **ДЮСЕБЕКОВА С.Б.**	**57-61**
Применение технологий «Искусственного интеллекта и Digital twin» для повышения уровня безопасности сотрудников полиции **ЖАКИПБЕКОВ Е.Н., ЖАРЫЛКАСЫНОВ К.Ә.**	**62-72**
Перспективы использования систем искусственного интеллекта в организации расследования преступлений на воздушном и железнодорожном транспорте	**73-78**

ЗАЙНУЛДИН Е.С.
Жаңа буын автомобильдерінің қауіпсіздігіне қарсы трансшекаралық қылмыстар: кибер осалдықтар, дәлелдемелердің криминалистикасы және Қазақстан Республикасындағы қылмыстық жауаптылық мәселелері **79-85**

КАДРИН Т.Б.
Жалған ақпаратты таратқаны үшін қылмыстық жауаптылықтың шегі **86-90**

ПРИМКУЛОВА А.А.
Ответственность за сбыт и потребление наркотических средств: проблемы и пути решения **91-97**

САГИМБАЕВА М.Қ.
Цифровизация в условиях развития киберпреступности: уголовно-правовые и криминологические аспекты **98-104**

САГИНБАЕВА А.У.
Заңдылық пен құқықтық тәртіпті қамтамасыз ету саласында жасанды интеллекттің технологиялық жүйелерін пайдаланудың өзекті мәселелері **105-111**

САУТБАЕВ Д.Б.
К вопросам морально-психологического обеспечения служебно-боевой деятельности национальной гвардии Республики Казахстан **112-115**

ТЕМІРЖАНОВ А.Т.
О проводимой работе по внедрению искусственного интеллекта **116-119**

ТУЛЕУОВА М.Е.
Кәмелетке толмағандарды ұстаудың процестік шектері: құқықтық айқындық пен конституциялық кепілдіктер теңгерімінің мәселелері **120-126**

УТЕГЕНОВА Г.А.
Проблемы уголовно-правовой защиты несовершеннолетних жертв семейно-бытового насилия в условиях цифровизации: системы выявления и оказания помощи **127-132**

ШАУДЫРОВ Т.С.
Аналоги центров оперативного управления в зарубежных полицейских практиках: сходства, различия, возможные пути учета эффективных методик **133-139**