АКАДЕМИЯ УПРАВЛЕНИЯ
МИНИСТЕРСТВА ВНУТРЕННИХ ДЕЛ РЕСПУБЛИКИ КАЗАХСТАН

Мусин Айдар Булатович

ПРОАКТИВНЫЙ ПОДХОД В ОПЕРАТИВНО-РОЗЫСКНОЙ ДЕЯТЕЛЬНОСТИ ОРГАНОВ ВНУТРЕННИХ ДЕЛ РЕСПУБЛИКИ КАЗАХСТАН

Монография

Алматы
2026

УДК343(035.3)
ББК67.408
М79

Публикуется по решению ученого совета
Академии управления МВД Республики Казахстан
(протокол № 9 от 29.04.26 г.)

Рецензенты:
Карымсаков Р.Ш., кандидат юридических наук;
Амангельдиев Д.А., доктор философии (PhD).

Мусин А.Б.
М79 **Проактивный подход в оперативно-розыскной деятельности органов внутренних дел Республики Казахстан:** монография / А.Б. Мусин. – Алматы: «ADAL KITAP», 2026. – 148 с.

ISBN 978-601-384-655-2

Монография посвящена теоретико-методологическому обоснованию проактивного подхода к оперативно-розыскной деятельности органов внутренних дел Республики Казахстан. В работе рассматриваются сущность и содержание проактивной парадигмы ОРД, её отличие от традиционных реактивных моделей, а также организационно-правовые и тактико-технологические основы её реализации в условиях трансформирующейся криминальной среды.

Монография адресована руководящему составу и сотрудникам органов внутренних дел, преподавателям ведомственных образовательных организаций, курсантам и слушателям магистратуры и докторантуры, научным работникам в области оперативно-розыскной деятельности и криминалистики. Результаты исследования предназначены для совершенствования методического обеспечения оперативной деятельности и развития образовательных программ МВД РК.

УДК343(035.3)
ББК67.408

ISBN 978-601-384-655-2

© Мусин А.Б., 2026
© «ADAL KITAP», 2026

ОГЛАВЛЕНИЕ

ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ 4
НОРМАТИВНЫЕ ССЫЛКИ 5
ПРЕДИСЛОВИЕ 6
ВВЕДЕНИЕ 7

ГЛАВА 1. СОВРЕМЕННАЯ МОДЕЛЬ ОРД ОВД: КРИЗИС РЕАКТИВНОГО ПОДХОДА 9
§ 1.1. Характеристика действующих подходов к осуществлению ОРМ органами внутренних дел РК 9
§ 1.2. Гибридизация преступности как вызов традиционной модели ОРД 31

ГЛАВА 2. КОНЦЕПЦИЯ ПРОАКТИВНОГО ПОДХОДА К ОСУЩЕСТВЛЕНИЮ ОРМ ОВД РК 50
§ 2.1. Оперативно-розыскное прогнозирование как информационная основа 50
§ 2.2. Сетецентризм как организационная основа проактивного подхода 70
§ 2.3. Информационно-психологические операции в системе проактивного подхода 89
§ 2.4. OSINT и БПЛА как инструменты проактивного подхода 108

ЗАКЛЮЧЕНИЕ 126
СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ 130
ПРИЛОЖЕНИЯ 141

ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

AR – augmented reality (дополненная реальность)
OSINT – open-source intelligence (разведка из открытых источников)
PSYOP – Psychological operation (информационно-психологические операции)
БПЛА – беспилотные летательные аппараты
ДОУ – дело оперативного учёта
ЕАЭС – Евразийский Экономический Союз
ИИ – искусственный интеллект
КНБ – Комитет национальной безопасности
МВД – Министерство внутренних дел
ОВД – органы внутренних дел
ООН – Организация Объединённых Наций
ОПГ – организованные преступные группы
ОРД – оперативно-розыскная деятельность
ОРМ – оперативно-розыскные мероприятия
РК – Республика Казахстан
СМИ – средства массовой информации
УБОП – Управление по борьбе с организованной преступностью
УК – Уголовный кодекс
УПК – Уголовно-процессуальный кодекс

НОРМАТИВНЫЕ ССЫЛКИ

Конституция Республики Казахстан: принята на республиканском референдуме 30 августа 1995 года.

Послание Президента РК К.-Ж. Токаева народу Казахстана «Справедливое государство. Единая нация. Благополучное общество» (1 сентября 2022 года).

Закон Республики Казахстан «Об оперативно-розыскной деятельности»: принят 15 сентября 1994 года, №154-XIII.

Закон Республики Казахстан «О противодействии экстремизму»: принят 18 февраля 2005 года, №31-III.

Закон Республики Казахстан «Об органах внутренних дел»: принят 23 апреля 2014 года, №199-V.

Закон Республики Казахстан «Об участии граждан в обеспечении общественного порядка»: принят 9 июля 2004 года, №590-II.

Закон Республики Казахстан «Об информатизации»: принят 24 ноября 2015 года, №418-V.

Закон Республики Казахстан «Об искусственном интеллекте»: принят 17 ноября 2025 года, №230-VIII ЗРК.

Цифровой кодекс Республики Казахстан: принят 9 января 2026 года, №255-VIII ЗРК.

Уголовный кодекс Республики Казахстан: принят 3 июля 2014 года, №226-V.

Уголовно-процессуальный кодекс Республики Казахстан: принят 4 июля 2014 года, №231-V.

ПРЕДИСЛОВИЕ

Настоящая монография написана под непосредственным впечатлением от событий января 2022 года, которые обнажили структурную неготовность правоохранительной системы Казахстана к угрозам нового типа – гибридным по природе, сетевым по организации, действующим одновременно в криминальном, экстремистском и информационном измерениях.

Автор подходит к этой теме с двух сторон. Годы службы в подразделениях криминальной полиции дали понимание оперативной работы изнутри – с её реальными возможностями, институциональными ограничениями и разрывом между тем, что есть, и тем, чего требует современная криминогенная ситуация. Стремление осмыслить этот разрыв научно привело к многолетнему исследованию, завершившемуся защитой докторской диссертации по данной тематике. Соединение практического опыта с теоретическим анализом и определило логику настоящей работы.

Центральный тезис монографии состоит в том, что деятельность оперативных подразделений ОВД по-прежнему строится на реактивной модели – реагировании на уже совершённые преступления. Между тем современная преступность давно перешла к проактивной тактике: она планирует, адаптируется, использует информационную среду и сетевую децентрализацию как защиту от разоблачения. Ответом на этот вызов должна стать смена парадигмы – переход к проактивному подходу, основанному на оперативно-розыскном прогнозировании, сетецентрической организации и применении методов информационно-психологического воздействия на криминальные структуры.

Этот переход уже происходит – в отдельных подразделениях, в рамках конкретных операций, в логике ряда управленческих решений последних лет. Читатель, работающий в системе, без труда узнает эти тенденции. Задача монографии – дать им теоретическое обоснование и организационную логику, пригодную для последовательного тиражирования.

ВВЕДЕНИЕ

Настоящая монография посвящена обоснованию и разработке проактивного подхода к осуществлению оперативно-розыскных мероприятий органами внутренних дел Республики Казахстан. Впервые в отечественной юридической науке данная проблематика рассматривается комплексно – в единстве теоретических, организационных и правовых аспектов, с опорой на практику оперативных подразделений ОВД и адаптированный зарубежный опыт.

Актуальность темы определяется принципиальным изменением характера угроз, с которыми столкнулась правоохранительная система Казахстана. Январские события 2022 года обнажили системную неготовность оперативных подразделений ОВД к противодействию гибридным формам преступности, сочетающей общеуголовный криминал, организованные структуры и экстремистские движения. Действующая реактивная модель – ориентированная на реагирование после совершения преступления – утратила эффективность. Между тем современная преступность действует на опережение: она сетевая, технологически оснащённая и управляемая. Ответом на этот вызов служит переход к проактивной стратегии – упреждающей, аналитически обоснованной, опирающейся на прогнозирование и информационное превосходство.

В монографии впервые сформулировано предложенное определение понятия «проактивный подход к осуществлению ОРМ» и разработана его концепция применительно к условиям ОВД РК. Предложены алгоритмы внедрения оперативно-розыскного прогнозирования, сетецентрической организации деятельности, информационно-психологических операций в отношении подучётного контингента, а также новых технологий – OSINT и беспилотных летательных аппаратов. Сформулирован проект нормы для восполнения правового пробела в Законе РК «Об оперативно-розыскной деятельности».

Значимость монографии обусловлена тем, что её положения непосредственно применимы в практической деятельности оперативных подразделений ОВД. Разработанные организационные алгоритмы прошли апробацию в подразделениях МВД Республики Казахстан и внедрены в учебный процесс Академии управления МВД Республики Казахстан. Теоретические выводы расширяют доктринальную базу ОРД в части её разведывательно-поискового характера и вводят в научный оборот понятия, ранее не применявшиеся в казахстанской правовой науке.

Цель монографии – на основе критического анализа действующей модели деятельности оперативных подразделений ОВД РК показать её системные ограничения и предложить концепцию проактивного подхода, адекватного современному состоянию преступности. Для достижения этой цели решаются следующие задачи: выявить недостатки реактивной модели и причины её неэффективности; раскрыть сущность и принципы проактивного подхода; разработать алгоритмы оперативно-розыскного прогнозирования;

обосновать применение сетецентрических форм организации деятельности; адаптировать методы информационно-психологических операций к условиям ОРД; определить правовые и организационные рамки применения OSINT и БПЛА.

Монография адресована руководителям и сотрудникам оперативных подразделений ОВД, преподавателям ведомственных вузов системы МВД, слушателям магистратуры и докторантуры, а также исследователям в области оперативно-розыскной деятельности.

ГЛАВА 1. СОВРЕМЕННАЯ МОДЕЛЬ ОРД ОВД: КРИЗИС РЕАКТИВНОГО ПОДХОДА

§ 1.1. Характеристика действующих подходов к осуществлению оперативно-розыскных мероприятий органами внутренних дел Республики Казахстан

Наиболее наглядной демонстрацией степени эффективности действующих подходов к работе всей системы правоохранительных и специальных служб Казахстана к осуществлению ОРМ стали итоги трагических событий января 2022 года, которые высказал Глава государства К.-Ж.К. Токаев:

«…Крайне важный момент – почему государство проспало наличие спящих ячеек боевиков и деятельность их командного пункта, почему на территории нашей страны оказалось так много нелегального оружия и спецсредств, почему не проводилась агентурная работа по выявлению и нейтрализации агентов терроризма» [5].

Внешне эти события выглядят совершенно внезапными. Однако анализ показывает, что информация, отражающая эти процессы, всё же попадала в поле зрения правоохранительных органов и, прежде всего, оперативных подразделений ОВД. Об этом свидетельствуют результаты опроса их сотрудников: значительная часть (почти 60%) отметила, что сведения о наличии определённых признаков нарастающей угрозы имелись, однако по различным обстоятельствам соответствующей реакции на них не последовало (Приложение А).

Системные проблемы в организации деятельности соответствующих государственных органов явились закономерным результатом игнорирования объективных процессов, происходивших как внутри Казахстана, так и на внешнем контуре.

В чем же заключаются эти системные проблемы?

Ключевая из них – явное несоответствие действующей модели правоохранительной системы кардинально изменившимся условиям криминогенной среды [6].

Начиная с конца 1980-х годов, в ней произошел динамичный «скачок», выразившийся в расцвете организованной преступности.

Уже в то время С.С. Овчинский и А.В. Христюк отмечали, что активизация деятельности организованных преступных групп (ОПГ) не ограничилась так называемым «ретро-профессионализмом». На арену социальной патологии «прорвался» так называемый «нео-профессионализм», суть которого в том, что ОПГ стали формироваться не только из уголовных рецидивистов, но и из деморализованных категорий – представителей разных слоев общества, в том числе служащих, бывших спортсменов, студентов, работников госаппарата и уволенных по различным мотивам сотрудников правоохранительных органов. «Нео-профессионалы» преступного мира – явление не менее (а зачастую и более) опасное, чем «воры

в законе». Их появление предопределило необходимость поиска новых тактических решений, так как интеллект, образованность, знакомство с образцами организованной преступности других стран (в том числе и западных), привлечение в свои ряды бывших (а иногда и действующих) сотрудников оперативных аппаратов способствовали освоению этими группами весьма квалифицированных способов и технических средств в совершении преступлений, не говоря о хорошо поставленных контрагентурных мероприятиях, сплоченности, взаимной подстраховке и ведении разведки. У «нео-профессионалов» имелся ряд качеств, которые делали их менее уязвимыми по сравнению с рецидивистами и «ворами в законе»:

1) во-первых, они до разоблачения и выявления не состояли на оперативных учетах, поскольку не подпадали под перечни оснований постановки на учет, распространяющихся на лиц, допускающих отклонение от норм поведения: пьяницы, хулиганы, ранее судимые и др.;

2) во-вторых, «нео-профессионалы» не допускали в свою среду лиц, которые в силу негативно-отклоняющегося поведения могли попасть в поле зрения правоохранительных органов и оказаться на учетах;

3) в-третьих, как правило, они имели легальное прикрытие, не позволявшее относить их к антиобщественным элементам (фирмы, предприятия, организации);

4) в-четвертых, образовательный уровень, внешний облик, круг интересов, круг общения, интеллект, досуг «нео-профессионалов» не имели ничего общего с формировавшимся десятки лет представлением работников ОВД о типичных представителях преступной среды [7].

С тех пор феномен организованной преступности пережил еще несколько качественных трансформаций, связанных с общим изменением внешних условий – политических, социальных, экономических, геополитических и др. Общий вектор этих процессов обозначил А.С. Овчинский.

Структуры криминальных связей в развивающейся организованной преступности им было предложено классифицировать по четырем основным типам: очаг, ансамбль, центр и сеть. Очаговая преступность – это первый, можно сказать, начальный этап криминальной активности, не организованный и функционально не структурированный. Сначала наблюдается рост концентрации отдельных актов именно в эпицентрах очагов, когда одни преступления и правонарушения притягивают другие. Фиксируя динамику развития очагов преступлений, можно предположить последующие места ожидаемых преступлений. При очаговой преступности работа строится по территориальному принципу и включает последовательную «обработку» контингентов лиц, проживающих в районах, где фиксируются вспышки преступлений [8].

На практике это нагляднее всего видно по квартирным кражам. Как правило, они распространяются в так называемых спальных районах, где и располагается основная масса объектов преступного посягательства.

Аналогичная ситуация обстоит с карманными кражами, особенно совершаемым в общественном транспорте в часы наибольшей загруженности пассажирами (час пик).

Такие уголовные правонарушения на начальном этапе формирования криминальных групп, как правило, не носят организованного характера и не особо сложны в раскрытии, так как способы их совершения и сокрытия еще не стали технически подготовленными и изощренными.

Далее, развиваясь, преступный бизнес, как правило, дифференцируется, приобретает структуру. Очаговая преступность приобретает структуру «ансамблей». Структуру ансамблей имеют многие виды преступной деятельности. Так, криминальный автобизнес включает заказчиков престижных автомобилей и непосредственно угонщиков машин. Здесь же организация их сокрытия, использование производственных мастерских для перекраски, изменения идентификационных номеров, ремонта и предпродажной подготовки, изготовление поддельных документов, перегон в другие регионы, наконец, реализация – продажа похищенного автотранспорта. Аналогично, наркобизнес начинается с плантаций по выращиванию наркосодержащих растений, первичной обработки «урожая», хранения, последующего производства наркотиков, их транспортировки к перевалочным пунктам и непосредственно к местам реализации. Он включает расфасовку по дозам, распределение по мелким оптовикам и продажу потребителям. Если правоохранительные органы сталкиваются с криминальными «ансамблями», работа приобретает «отраслевую» направленность. Ее целью является выявление производственных участков, баз, лабораторий, притонов, составляющих звенья преступной деятельности.

Для тех же вышеупомянутых квартирных и карманных воров «партнерскими» элементами «ансамбля» могут быть ломбарды, точки по реализации подержанных мобильных телефонов, ювелирные салоны и т.д.

Для противодействия им в структуре криминальной полиции имеются подразделения по раскрытию имущественных преступлений, которые должны отслеживать работу этих объектов на предмет прохождения через них похищенных вещей.

Следующим принципиальным этапом развития вслед за очагами и ансамблями является создание органов управления, то есть переход к структуре, которую можно обозначить как «центр». Если структуры типа «ансамбль» предполагают определенное разделение функций и равноправное отношение между партнерами, то структуры типа «центр» отражают сосредоточение управляющих и координирующих функций в одних руках и более или менее однотипную деятельность многочисленных, связанных с центром криминальных групп. Наиболее ценная оперативно-розыскная информация может быть получена из тех криминальных, полукриминальных или связанных с ними кругов, где формируется замысел, осуществляются планирование и координация организованной преступной деятельности
[8, с. 72-73].

Практика показывает, что разрозненные группы квартирных и карманных воров, а также их партнеры по «ансамблям» рано или поздно попадают в поле зрения более серьезных преступников. Как правило, это представители организованных криминальных формирований (так называемые «уголовные авторитеты» и «положенцы»), которые, в свою очередь, входят в состав более крупных структур – сообщество «воров в законе». Согласно их неформальным правилам, все, кто совершает преступления в зоне их ответственности, обязаны платить взнос в «общак». Отказ влечет за собой физическое наказание или, как более изощренный вариант, «слив» информации о них оперативным подразделениям.

Но уже на этом уровне привлечь к ответственности «уголовных авторитетов» и «положенцев» (не говоря уже о «ворах в законе») представляет большую проблему, так как они, как правило, сами к преступлениям не причастны, осуществляя лишь общий контроль за деятельностью «очагов» и «ансамблей».

Наконец, как отмечает А.С. Овчинский, наиболее сложные задачи перед ОРД возникают в ситуациях, когда правоохранительные органы сталкиваются с сетевыми структурами преступного бизнеса, терроризма или экстремистской деятельности. Ни локализация очагов, ни разрушение связей, ни ликвидация «центров» не гарантируют успеха в противодействии криминальным явлениям и антисоциальным процессам, которые сформировались в разветвленные сетевые структуры. Именно сетевые структуры в значительной мере обеспечивают устойчивость колоссальных криминальных доходов наркомафии. Периодические изъятия крупных партий наркотиков, уничтожение плантаций, разрушение цехов и лабораторий, аресты курьеров и продавцов, даже судебные процессы над лидерами преступного мира, а в некоторых случаях и смена правящих режимов в странах, поставляющих на мировой рынок наркотики, хотя и наносят определенный урон, но не могут переломить ситуацию в борьбе с международной и с «внутренней» наркоторговлей [8, с. 74-75].

Вероятно, эта проблема будет оставаться актуальной и в последующем.

Отсюда следует, что четвертая, сетевая модель преступной деятельности является в настоящее время высшей и наиболее сложной формой организованной преступности.

Более детально о сетевых криминальных структурах и методах противодействия им будет изложено ниже.

Следует подчеркнуть, что большинство современных организованных преступных формирований находятся на этапе активного перехода на сетевую модель. В то же время основная часть оперативных подразделений ОВД РК (особенно в звене район-город) до сих пор не могут «перешагнуть» с первого уровня (очаговой преступности) на второй («ансамбли»). Это несоответствие приобретает определяющий характер и отводит им роль хронически отстающего.

Нагляднее всего это видно по картине развития организованной преступности, которую описал А.С. Овчинский.

Он отмечает, что правоохранительные органы столкнулись с качественно новым антисоциальным явлением, которое не подпадает под сложившиеся уголовно-правовые и криминологические представления о ней. Дело в том, что противодействовать организованной преступности можно только комплексно, не разделяя ее на общеуголовную и экономическую. ОРМ должны производиться не от совершенного преступления или экономического объекта, а от конкретных преступных сообществ на основе информации, полученной «изнутри». В 2007 году руководители МВД России отмечали, что они контролируют деятельность более 400 крупных преступных организаций в стране, была разработана Концепция борьбы с организованной преступностью, где главная роль отводилась специализированным подразделениям. Однако 6 октября 2008 года органы по борьбе с организованной преступностью (УБОП) были ликвидированы, а их функции возложены на подразделения уголовного розыска и службы по борьбе с экономической преступностью. Если образование специализированных подразделений по борьбе с организованной преступностью в МВД СССР в ноябре 1988 года считалось революцией в рамках системы ОВД, то их ликвидацию через 20 лет в октябре 2008 года можно считать настоящей контрреволюцией [8, с. 83-84].

В Казахстане протекали аналогичные процессы. УБОПы продержались на десять лет дольше, чем в России, служа примером взвешенного подхода к организации противодействия организованной преступности. Однако и здесь деструктивные тенденции привели к недальновидным решениям.

Так, УБОПы были упразднены в 2018 году после череды чрезвычайных происшествий, связанных с сотрудниками подразделений. Их остатки были влиты в криминальную полицию в виде отделов. Но уже в следующем, 2019 году, стало очевидно, что это был неверный шаг [9].

Время показало, что решение о ликвидации УБОПов было преждевременным и ошибочным, так как мафия в Казахстане никуда не делась. Она просто приобрела другие формы и стала действовать не столь нагло и открыто, как в лихие 1990-е годы. Проблема заключалась в том, что малочисленные отделы по борьбе с оргпреступностью едва справлялись с нагрузкой, поскольку им не хватало сил и средств. Поэтому назрела необходимость в воссоздании этих подразделений, и это произошло в 2022 году [10].

Вместе с тем закономерно, что за прошедшее время был в значительной степени утрачен кадровый потенциал этой службы. Вслед за этим контроль за подучетным контингентом был серьезно ослаблен и, соответственно, криминогенная ситуация ухудшилась. Поэтому пришлось наверстывать упущенное.

Первые результаты работы возрожденных подразделений УБОП начались в 2023 году. Так, в Карагандинской области сотрудниками ДБОП МВД и областного департамента КНБ была проведена специальная операция по обезвреживанию опасной преступной группировки, которая на протяжении длительного времени негативно влияла на криминогенную

обстановку в регионе. Ее члены неоднократно устраивали криминальные разборки с применением огнестрельного оружия, дерзко нарушая общественный порядок. Численность группировки составляли около 50 активных участников, в том числе бывшие сотрудники правоохранительных органов, а также работники охранных организаций. В группе имелась четкая иерархия с определением роли каждого, соблюдались меры конспирации. Установлена причастность членов группировки к ряду нераскрытых тяжких и особо тяжких преступлений: вымогательства, причинение тяжкого вреда здоровью, покушение на убийство и хулиганства. В ходе спецоперации проведено более 100 обысковых мероприятий, изъято девять единиц огнестрельного оружия, около 200 боеприпасов, гранатомет, тротил, гранаты, документация и поддельные печати, религиозная литература, крупная сумма денежных средств, движимое и недвижимое имущество, а также специальные технические средства для прослушивания удаленным доступом [11].

Очевидно, что столь длительная безнаказанная преступная деятельность стала возможной вследствие функциональной неспособности других служб осуществлять целевую разработку современных организованных криминальных формирований.

Для лучшего понимания их сущности А.С. Овчинский вводит такие понятия, как экструзивная и интрузивная преступность. Экструзия означает технологическую операцию выдавливания пластического материала через отверстия в свободное пространство. Экструзивная преступность представляет ту часть криминальных явлений, которые достаточно четко осознаны обществом как преступные. Такая преступность категорически осуждается и выдавливается системой социально-правовых отношений и, в первую очередь, нормами уголовного права из общественной жизни. В то же время, выдавливаясь, эта часть преступности создает собственные структуры, формирует свои организованные сообщества, развивает свои традиции и даже порождает свою криминальную субкультуру. В подавляющем большинстве научных исследований, посвященных проблемам борьбы с рецидивной и профессиональной преступностью, речь идет именно об экструзивной преступности.

Ярким примером такой преступности является деятельность сообщества «воров в законе». Хотя в Казахстане они немногочисленны и периодически привлекаются к уголовной ответственности, отрицать их влияние на криминогенную ситуацию в стране не приходится.

При всей общественной опасности экструзивная преступность представляет собой известный и предсказуемый феномен. Для противодействия ей в арсенале ОРД ОВД имеются адекватные организационные и тактические меры, применяемые с различной степенью эффективности. Пусть и с опозданием, жизненная необходимость воссоздания специальных подразделений по борьбе с организованной преступностью в Казахстане была осознана.

В отличие от нее, интрузивная преступность оказывала и продолжает оказывать значительно большее негативное влияние на социально-экономические процессы в современном обществе. Технический термин «интрузия» означает технологическую операцию, заключающуюся уже не в выдавливании пластического материала в свободное пространство, а во вдавливании – заполнении им некоторых полостей. Характерным примером интрузии является заполнение жидким полимером пространства между волокнами композиционного материала. Главная отличительная черта интрузивной преступности состоит в том, что она естественным образом проникает, встраивается и начинает играть существенную роль в системе социальных, правовых, финансовых, экономических и других отношений, постепенно изменяя политическую, культурную и духовную жизнь общества. Интрузивная организованная преступная деятельность привела к обнищанию значительной доли населения и к невероятно быстрому обогащению участников грандиозных афер в лихие 1990-е годы [8, с. 85-86].

Картина, предлагаемая А.С. Овчинским, во многом носит теоретический характер, поскольку не может опираться на подтверждённые материалы уголовных дел. Сама форма существования описываемой интрузивной организованной преступности не даёт уголовной юстиции возможности процессуально зафиксировать её сущность.

Между тем именно интрузивная преступность представляет в настоящее время наибольшую опасность для общества и государства. Её существование учёные, в частности А.С. Овчинский, устанавливают по совокупности косвенных признаков, выявляемых в результате многолетних наблюдений за различными криминальными формированиями – по аналогии с тем, как астрономы по гравитационным отклонениям рассчитывают характеристики далёких невидимых планет.

А.С. Овчинский применительно к организованной преступности вводит и такие понятия, как конструктивность и деструктивность. По его мнению, в организованной преступной деятельности в ряде случаев можно усмотреть и конструктивную роль. Конструктивная организованная преступность представляет собой ту традиционную преступность, которая занимается запрещенными видами деятельности, устанавливает криминальный контроль над легальной экономикой, развивает различные сферы теневой экономики, в результате чего возникает необходимость создания новых рабочих мест, а иногда и участия в развитии инфраструктуры регионов [8, с. 86].

Такой неожиданный взгляд на эту сторону организованной преступности может показаться парадоксальным. Тем не менее, данный ее феномен действительно имеет место и исследуется зарубежными учеными на протяжении многих лет. Речь идет о контроле с ее стороны над теневой экономикой.

В этом смысле показательна книга перуанского экономиста Эрнандо де Сото «Иной путь. Невидимая революция в третьем мире», которая вышла в свет в 1987 году. Главное научное открытие Э. де Сото – это принципиально новый подход к объяснению генезиса теневой экономики. Э. де Сото

перевернул с головы на ноги качественные оценки теневого и легального бизнеса в «третьем мире». Считалось, что легальный сектор является носителем современной экономической культуры, в то время как теневой сектор – уродливый пережиток традиционной экономики. На самом же деле, доказывает перуанский экономист, легальная экономика развивающихся стран опутана меркантилистскими узами, в то время как именно теневики устанавливают истинно демократический экономический порядок, организуя свое частное хозяйство на принципах свободной конкуренции [12].

Э. де Сото описал экономическую ситуацию, когда на нелегальную деятельность в Перу приходится 48% экономически активного населения и 61,2% рабочего времени, 38,9% официального валового национального продукта. В некоторых сферах экономики теневики вообще стали основными производителями. Так, например, нелегальный транспорт составлял 93% транспортного парка Лимы, столицы Перу. При этом товары и услуги, производимые теневиками, по существу, ничем не отличались от продукции легального производства [13].

На определённом этапе своего развития организованная преступность выполняет подобную социальную роль, которую нельзя однозначно квалифицировать как отрицательную.

Но, по утверждению А.С. Овчинского, отличительной чертой современной организованной преступности и одним из ее основных направлений является не конструктивность, а деструктивность. Она проявляется в извлечении криминальных доходов из разрушения экономических и социальных отношений, из подрыва основ государственности, из уничтожения духовных и моральных устоев общества. При разрушении социальных структур и экономических комплексов происходит перераспределение материальных ценностей и финансовых средств. Социальные потрясения представляют собой стратегическую цель деструктивной организованной преступности [8, с. 87].

Применительно к России такое понимание целей организованной преступности имеет под собой реальную основу. Применительно к Казахстану интрузивный криминалитет, по всей видимости, заинтересован в определённой стабильности общества и государства, поскольку паразитирует на них. Дестабилизация создаёт для организованной преступности препятствия в сохранении налаженных источников незаконной прибыли. В известной мере прослеживается симбиоз организованной преступности с государством.

Иное дело – экстремистские и террористические движения. Их коренное отличие заключается в том, что получение криминальных доходов является для них не целью, а лишь средством для достижения дестабилизации общественной, политической и экономической жизни страны.

Именно поэтому общественная опасность экстремизма и терроризма выше, чем у организованной преступности, хотя в некоторых случаях разница невелика, особенно в случаях, когда два этих негативных социальных явления соединяются друг с другом. Особую опасность таким

процессам придает то, что они протекают незаметно для государства и общества, которые привыкли смотреть на них через призму традиционных подходов.

Это связано с проявлением мощной иммунной системы организованной преступности. Она часто неуязвима для правоприменительной и законотворческой деятельности и уголовной политики в целом, если речь идет о высших эшелонах криминальной иерархии или о разветвленных сетевых структурах криминального бизнеса. Это качество современной преступности наиболее емко определяется таким понятием, как мимикрия. Мимикрийную организованную преступность отличает то, что она практически сливается с социально-экономическим и политическим ландшафтом современного общества. Преступные сообщества, которые в значительной мере определяли экономическую и социальную жизнь во многих регионах в 1990-е годы прошлого века и начале нынешнего века, в настоящее время таинственным образом стали незаметными, как будто на них накинули вдруг «шапки-невидимки». На фоне стабилизации экономики, затухания политических баталий в обществе, укрепления вертикали власти и административных реформ незаметно сошла со сцены проблема борьбы, противодействия или контроля над организованной преступностью. Но, усиливая свое давление на общество, преступные формирования настолько мимикрировали, настолько встроились в социально-экономическую жизнь, что стали не только неуязвимыми для правоохранительной системы, но и практически невидимыми на фоне социальных и политических проблем. Как правило, они проявляются в процессе криминальных разборок при переделе сфер влияния [8, с. 88].

Примером может служить изложенная выше ситуация с деятельностью преступной группы в Карагандинской области, которая была выявлена в результате внутренних конфликтов в ней. Если бы их не было, то возможно, эта группа действовала бы до сих пор.

Такое положение логично выводит на вопрос: а сколько еще подобных замаскированных криминальных формирований незаметно и безнаказанно занимаются своей преступной деятельностью?

Здесь верен давно высказанный тезис о том, что пока соблюдаются «правила игры», организованная преступность малозаметна и не воспринимается как общественная проблема. Американские криминологи Г. Барнс и Н. Титер еще в 1950-е годы отмечали: «Основная причина, по которой общество терпеливо мирится с дополнительным бременем рэкета, заключается в том, что оно даже не подозревает о его существовании» [14].

Современную оперативную обстановку в Казахстане осложняет ещё один негативный фактор – мимикрирующий характер актуальной угрозы: религиозного экстремизма и терроризма. В памяти сохраняются их массовые проявления периода 2011–2016 годов: подрывы смертников, атаки на здания государственных органов, войсковые части, учреждения уголовно-исполнительной системы.

Но на определенном этапе они быстро прекратились. Значительный вклад в это внесли силовые органы – КНБ, МВД, а также другие государственные органы и гражданское общество. Но значит ли это, что эта опасность миновала?

Очевидно, что нет, о чем свидетельствуют январские события 2022 года. Как известно, представители деструктивных религиозных течений принимали в них активное участие [15].

Поэтому их деятельность, адаптируясь к внешним условиям, трансформировалась в сторону меньшей заметности, что автоматически повышает ее общественную опасность.

В результате описанных выше процессов, большей частью невидимых, складывается внешне не вызывающая особых опасений ситуация, не требующая кардинального изменения существующей традиционной модели работы правоохранительных органов и специальных служб.

В то же время внутреннее напряжение этой ситуации постоянно возрастает из-за давления новых возникающих факторов. Так, еще несколько лет назад мало кто мог прогнозировать, что повышение отпускной цены на автомобильный газ на 50 тенге в начале 2022 года способно стать триггером событий, поставивших под угрозу существование Казахстана в сложившемся виде.

Характеризуя криминогенную ситуацию в России несколько лет назад, А.С. Овчинский внес новое понятие – интрузивно-деструктивно-мимикрийная преступность (ИДМ-преступность) как сформировавшееся социальное явление, имеющее весьма сложную структуру. Среди ее основных признаков он выделяет:

1. ИДМ-преступность порождена системой сложившихся в обществе правовых, экономических и политических отношений, включающих распределение властных и управленческих полномочий как в высших эшелонах законодательной, исполнительной и судебной власти, так и во властных структурах всех уровней.
2. ИДМ-преступность обладает реальной возможностью, опирающейся на властные полномочия и политическую волю, поддерживать и развивать те правовые и экономические отношения, которые способствуют увеличению и совершенствованию многообразия механизмов криминального обогащения.
3. Наличие преступного умысла и криминальный характер конкретных деяний, совокупность которых подпадает под понятие ИДМ-преступности, чрезвычайно трудно доказуемы в рамках действующего уголовного права. Эти деяния объективно являются преступными по своим антисоциальным последствиям, проявляющимся в финансовых кризисах, политической дестабилизации, подрыве основ государственности, обнищании широких слоев населения. Они оцениваются как преступные общественным мнением, хотя средства массовой информации обрушивают на людей широкую палитру взглядов, отражающих ту информационно-психологическую борьбу, которую ведет ИДМ-преступность за утверждение нужных ей стереотипов общественного сознания.

4. В отличие от «классической» преступности, в значительной мере, занимающейся как запрещенными видами деятельности, так и криминальным контролем над легальной экономикой, ИДМ-преступность направляет свои усилия в основном на создание, поддержание и развитие таких правовых и экономических отношений и социально-политических ситуаций в стране, которые позволяют обогащаться определенным слоям общества, уходя от ответственности. В то время, как организованная преступность извлекает криминальные доходы из целенаправленной преступной деятельности, проникая в самые разнообразные сферы общественной жизни, ИДМ-преступность получает свои доходы, формируя выгодные ей социально-экономические, правовые и политические отношения в обществе.

5. В отличие от теневой экономики, состоящей в незаконном производстве товаров и услуг, в развитии высокодоходных криминальных видов деятельности, в производстве неучтенных товаров, в уклонении от налогов, ИДМ-преступность занимается изъятием финансовых средств из бюджетов (так называемые нецелевые расходы), из производства (невыполнение обязательств по инвестированию предприятий), у отдельных граждан (невыполнение обязательств по возврату вкладов).

6. В отличие от нелегальных видов деятельности, при которых преступные сообщества получают сверхдоходы за счет построения незаконных, противоправных экономических отношений, более масштабные доходы ИДМ-преступностью извлекаются путем целенаправленного разрушения реального сектора экономики. Одним из механизмов такого извлечения доходов являлось существенное занижение стоимости приватизированных производственных комплексов с целью последующей их неоднократной перепродажи.

7. В отличие от коррупции, предполагающей участие государственных служащих в организованной преступной деятельности и теневой экономике или за определенное вознаграждение, или за некоторую долю в преступном бизнесе, ИДМ-преступность поднимает коррумпированность общественных отношений на качественно новый уровень. Под давлением огромных средств, сосредоточенных в руках уже сформировавшейся группы олигархов, реализуется такая законодательная политика, которая поддерживает, укрепляет и совершенствует систему правовых и финансовых отношений, позволяющих выводить из-под уголовной ответственности деяния, максимально способствующие личному обогащению заинтересованных лиц и наносящие наибольший урон экономике страны [8, с. 89-90].

На первый взгляд может показаться, что эти признаки ИДМ-преступности не присущи Казахстану. Однако, анализируя наиболее резонансные факты, связанные с организованной преступностью и сопутствующей ей инфраструктурой, можно сделать обоснованные выводы, что различия между российской и казахстанской реальностью не так уж и велики.

Например, взять громкое «Хоргосское дело», когда в 2011 году была выявлена сложная схема контрабанды из Китая в Казахстан. Казахстан и Китай делали взаимную сверку статистики, цифры не сходились, причем на огромные суммы – 3-5 миллиардов долларов США. То есть соседи писали, что пропустили товара на 3-5 миллиардов долларов больше, чем декларировала казахстанская сторона. Либо наши вообще не декларировали, либо декларировали те же шубы как трикотаж. Стало известно, что хоргосская ОПГ получала по 3-5 миллионов долларов в день. В год это как раз составляет те самые миллиарды, которых не хватало в статистике. Будучи свободной экономической зоной, «Хоргос» позволял проводить определенные махинации: можно было зарегистрировать фирму и сделать производство на бумаге, а в реальности покупать импортный товар, переклеивать этикетки и ввозить его в Казахстан беспошлинно. В состав ОПГ входили высокопоставленные чины КНБ, устранявшие конкурентов-контрабандистов по наводке руководителей сообщества. Хотя на скамью подсудимых сели 45 человек, а 19 объявили в розыск, эксперты считают, что рассчитывать на полное искоренение коррупции на границе не стоит [16].

Приведенные цифры и факты наглядно свидетельствуют о наличии в них многих признаков ИДМ-преступности, аналогичной российской. Об этом говорят и результаты расследования преступной деятельности ОПГ под руководством бывшего акима Атырауской области Бергея Рыскалиева.

В настоящее время он разыскивается за миллиардные хищения. Согласно материалам дела, он организовал преступную схему еще в 2006 году с момента назначения на пост главы региона. Б. Рыскалиев создал преступное сообщество, состоящее из объединения представителей ОПГ в целях разработки планов и условий для извлечения личной материальной выгоды, совершения тяжких и особо тяжких преступлений. Лица, входившие в преступное сообщество, преследовали единую преступную цель, направленную на извлечение материальной выгоды в результате хищения бюджетных денежных средств при строительстве социально-важных объектов на территории города и области, таких как газификация, электрификация, водоснабжение, строительство жилых домов, мостовых переходов, канализационно-очистных сооружений и других социальных объектов. В результате деятельности возглавляемого Б. Рыскалиевым преступного сообщества причинен ущерб государству на общую сумму свыше 71 миллиарда тенге [17].

В итоге Бергея Рыскалиева приговорили к 17 годам лишения свободы заочно. Его брата, экс-депутата Мажилиса Парламента РК Аманжана Рыскалиева, также приговорили к 16 годам лишения свободы заочно [18].

Обращает на себя внимание тот факт, что с момента создания ими преступного сообщества прошло несколько лет до того времени, когда его криминальная деятельность попала в поле зрения соответствующих органов. Получается, что продолжительное время для всей правоохранительной системы оно было «невидимым» в лучших традициях классической ИДМ-преступности. Лишь когда ущерб от масштабной преступной схемы

превысил все возможные границы, «включилась» машина уголовной юстиции.

Ещё одним подтверждением существования в Казахстане проявлений ИДМ-преступности является дело 2016 года о преступной группе Тохтара Тулешова, так называемого «пивного короля» Шымкента (он являлся владельцем ТОО «Шымкентпиво», а также многих других объектов бизнеса). Даже краткое описание деяний его и многочисленных соучастников (процесс проходил в закрытом режиме) заставляет поверить в реальность модели такой преступности, которую описал А.С. Овчинский.

Так, специализированный военный суд Астаны (он являлся военнослужащим) признал виновным Т. Тулешова и осудил его на 21 год лишения свободы по ряду статей УК РК:

– ч. 3 ст. 262 (создание и руководство организованной группой, преступной организацией, а равно участие в них с использованием своего служебного положения);

– ч. 3 ст. 268 (создание устойчивой вооруженной группы (банды), а равно руководство такой группой с использованием своего служебного положения);

– ч. 3 ст. 24, ч. 3 ст. 28, пункт «з» ч. 2 ст. 96 УК РК редакции 1997 года(организация совершения убийства, сопряженного с бандитизмом);

– ч. 3 ст. 28, п. 1 ч. 3 ст. 125 (организация похищения человека, совершенного преступной группой с применением оружия или предметов, используемых в качестве оружия);

– ч. 3 ст. 28, п. 1 ч. 3 ст. 126 (организация совершения незаконного лишения свободы, не связанного с его похищением, с применением насилия, в отношении 2-х лиц, совершенного группой лиц);

– ч. 3 ст. 28, п. «а», «б», «в» ч. 2 ст. 107 УК РК редакции 1997 года (причинение физических или психических страданий путем систематического нанесения побоев, совершенное в отношение похищенных лиц);

– ч. 3 ст. 28, п. «а» ч. 2 ст. 187 УК РК редакции 1997 года (организация умышленного уничтожения или повреждения чужого имущества, совершенного путем поджога, причинившего значительный ущерб);

– ч. 2 ст. 265 (создание и руководство транснациональным преступным сообществом, а равно участие в нем);

– ч. 3 ст. 266 (финансирование деятельности преступной группы, а равно хранение, распределение имущества, разработка каналов финансирования);

– ч. 3 ст. 179 (пропаганда или публичные призывы к захвату или удержанию власти, а равно захват или удержание власти либо насильственное изменение конституционного строя РК);

– ч. 3 ст. 182 (создание, руководство экстремистской группой или участие в ее деятельности);

– ч. 2 ст. 367 (дача взятки);

– ч. 2 ст. 296(незаконное приобретение, хранение наркотических средств без цели сбыта);

– ч. 1 ст. 287 (незаконное ношение холодного оружия) [19].

По материалам дела, бизнесмен Тохтар Тулешов готовил государственный переворот, длительное время поддерживал контакты оказывал финансовую поддержку лидерам и авторитетам транснационального преступного сообщества, известного за рубежом как «Братский круг». В своем подчинении Т. Тулешов имел более 90 вооруженных и прошедших соответствующее обучение бойцов. По его указанию криминальное звено его организованной преступной группы совершило ряд убийств, похищений и избиений людей. Получение доступа и контроля над финансовыми ресурсами государства стало для Тулешова одним из существенных стимулов для захвата власти [20].

Как и в случаях с «Хоргосским делом» и ОПГ Б. Рыскалиева, преступное формирование Т. Тулешова функционировало продолжительное время, захватив влияние над значительными ресурсами.

Почему реакция была столь запоздалой, а принимаемые меры осуществлялись постфактум? Способна ли существующая правоохранительная система адекватно противодействовать таким концептуальным криминальным вызовам?

Для того чтобы ответить на эти вопросы, следует изучить, как организована действующая, традиционная модель ОРД ОВД, по которой она осуществлялась на протяжении продолжительного периода времени и к которой привыкла вся система МВД.

Теория говорит, что для эффективного противодействия преступности правоохранительные органы должны иметь определенную структуру, приспособленную к выполнению своих основных функций. ОРД осуществляется системой подразделений специальных органов, наделенных полномочиями применять оперативно-розыскные силы, средства и методы и имеющих свою компетенцию. Внутри каждого оперативно-розыскного органа компетенция между отраслевыми оперативно-розыскными подразделениями в основном распределяется на основе специализации по видам преступлений. Чтобы подразделение работало эффективно, необходимо определить основной организационный принцип: линейный или объектовый (зональный), в соответствии с которыми распределяются функциональные обязанности каждого конкретного сотрудника. Когда оперативное обслуживание строится в расчете на закрепление сотрудников за определенными объектами (территориями), говорят о зональном принципе работы. Если закрепляется как предмет ведения вид преступления или определенная служебная функция, говорят о линейном принципе. В некоторых случаях в качестве организационного принципа приняты зонально-линейные начала, то есть смешанный принцип [20].

Таким образом, начальным и направляющим организационным аспектом деятельности оперативных подразделений ОВД является принцип оперативного обслуживания.

Его можно определить как самостоятельное организационно-управленческое направление деятельности оперативных подразделений, обеспечивающее поступление информации о состоянии оперативной обстановки, мониторинг ее текущего состояния, выработку управленческих решений в целях организации их деятельности в пределах профессиональной компетенции [21].

Вместе с тем изучение практических материалов показывает, что уровень оперативного обслуживания повсеместно и неуклонно снижается. Причиной этого является слабая заинтересованность сотрудников оперативных подразделений ОВД в последовательном выстраивании системы мониторинга криминогенной ситуации.

Об этом говорят результаты их опроса, когда более 45% признают, что на такую системную работу их не нацеливают (Приложение А).

Дело в том, что это длительная и кропотливая работа, а быстрого результата в виде уголовных дел не гарантирует. В то же время налаженное оперативное обслуживание способно заблаговременно выявить ранние признаки формирования преступных групп, перерастания их в более организованные формы – очаги, «ансамбли» – и дальнейшего развития до централизованных и сетевых структур.

Принцип оперативного обслуживания полностью соответствует известной «теории разбитых окон», в основе которой лежит утверждение о том, что преступность и ее развитие – это неизбежный результат отсутствия порядка. Для исключения более серьезных и тяжких преступлений необходимо бороться с мелкими правонарушениями, служащими факторами для развития тяжких. Соответственно, основной задачей являются устранение малейших сигналов нарушения порядка на объекте (сфере или территории) и постоянная осведомленность о складывающейся оперативной обстановке, которая возможна при осуществлении оперативного обслуживания объектов (сфер, территорий) [22].

Действительно, в основе нормальной работы оперативных подразделений ОВД должен лежать именно такой подход. Однако в реальности этот процесс постепенного накопления предкриминального потенциала их не интересует, прежде всего, в силу неверно выстроенной системы критериев их оценки. Проще говоря, никто из оперативных работников не будет заниматься группами несовершеннолетних, бьющих стекла в соседних микрорайонах, пока они не совершат значимое уголовное правонарушение. Максимум реакции со стороны ОВД на это – профилактическая беседа со стороны участкового инспектора полиции, за которую не начисляются такие условные «баллы», как за его участие в раскрытии уже совершенного преступления.

Тем не менее, для обеспечения деятельности оперативных подразделений необходимо постоянно располагать информацией о положении дел и оперативной обстановке, складывающейся на закрепленном направлении деятельности (объекте, сфере, территории). Для реализации указанной задачи необходимы на постоянной основе сбор, накопление,

систематизация, анализ и прогнозирование (мониторинг) оперативной информации, с целью выявления «зараженности» объекта криминальным «вирусом» для последующей борьбы и ликвидации указанных проявлений и факторов, способствующих их возникновению. Сущностными элементами оперативного обслуживания являются:

–своевременная, быстрая деятельность (совокупность мер) оперативных подразделений ОВД;

–задачи сбора, систематизации, диагностики и прогнозирования информации об изменении оперативной обстановки на территории объекта (сферы, территории);

–единая цель деятельности – предупреждение, выявление и пресечение преступлений для обеспечения безопасности на объекте от преступных посягательств и поддержание надлежащего функционирования объекта (сферы, территории) [22, с. 140].

Таким образом, сущность оперативного обслуживания двойственна: с одной стороны – это своевременная реакция на изменения обстановки; с другой – осуществление мер по упреждению развития ситуации по негативным сценариям.

К сожалению, в повседневной работе оперативных подразделений упреждающая составляющая постепенно уменьшалась, пока не исчезла совсем, полностью подменившись ситуативным реагированием на совершаемые уголовные правонарушения.

В этом смысле оправдана позиция российских авторов В.А. Галушко и О.Г. Половникова, что важность и актуальность оперативного обслуживания должна быть нормативно регламентирована, вплоть до закрепления в оперативно-розыскном законе как дополнительного основания для проведения ОРМ [23].

Оперативное обслуживание носит ярко выраженный разведывательно-поисковый характер. Собственно, именно за счет этого получается основной объем оперативно-розыскной информации, позволяющей мониторить состояние криминогенной ситуации и определять тенденции ее развития. На этой основе впоследствии должно осуществляться управленческое воздействие на данный процесс.

Но если проанализировать нормы Закона Республики Казахстан «Об оперативно-розыскной деятельности» (Закон РК об ОРД), то обнаруживается, что и разведывательно-поисковый характер ОРД в нем не отражен.

На это обстоятельство указывает М.М. Галиханов при раскрытии п. 1 ст. 10 Закона РК об ОРД, где в подпункте б) в качестве оснований проведения ОРМ значится поступившая в органы, осуществляющие ОРД, информация о:

–подготавливаемом, совершаемом или совершенном правонарушении;

–лицах, скрывающихся от органов дознания, следствия и суда или уклоняющихся от уголовного наказания;

–безвестном отсутствии граждан и обнаружении неопознанных трупов [24].

На этом основании М.М. Галиханов задается вопросом: если оценивать эти нормы буквально, получается, что основанием для осуществления ОРМ должна быть соответствующая информация. Значит ли это, что надо пассивно ждать ее поступления? Или же допускается инициативно проводить ОРМ для получения таких сведений? В первом случае намеренно ограничивается инициативный характер ОРД, отчего ее эффективность только снижается. Естественно, наиболее предпочтительным для целей противодействия преступности является второй подход. Поэтому для устранения данной правовой коллизии им предлагается п. 1 ст. 8 «Права органов, осуществляющих оперативно-розыскную деятельность» изложить в следующей редакции:

«Органы, уполномоченные осуществлять оперативно-розыскную деятельность, имеют право:

1) проводить *инициативно* в пределах своей компетенции гласно и негласно оперативно-розыскные мероприятия…» и далее по тексту [25].

Таким образом, получается, что важнейшие «краеугольные» положения ОРД ОВД, направленные на выявление и упреждение самых опасных угроз общественной безопасности, не находят отражения в действующем законодательстве.

Представляется, что пока на оперативные подразделения ОВД не будут законодательно возложены обязанности вести упреждающую работу по недопущению развития предкриминального потенциала в оконченное уголовное правонарушение, инициативная разведывательно-поисковая деятельность будет отторгаться.

Следовательно, наиболее опасные виды криминальной деятельности (такие, как ИДМ-преступность) останутся недосягаемыми для уголовной юстиции, а угроза повторения аналогов событий января 2022 года будет постоянной.

Кроме того, помимо правовых проблем, имеются системные недостатки организационного характера. Прежде всего это относится к существующей модели ведомственных критериев оценки работы полиции.

Они объявлены соответствующим приказом и в их перечень включены:

1. Количественные критерии:

–состояние преступности;

–количество убийств;

–раскрываемость убийств, а также других тяжких и особо тяжких преступлений;

–количество уголовных правонарушений, совершенных на улицах и иных общественных местах;

–криминологическая характеристика лиц, совершивших уголовные правонарушения;

–состояние дорожной безопасности.

2. Качественные критерии:

–состояние личной, имущественной и общественной безопасности;

–оценка эффективности работы полиции;

–уровень доверия населения [26].

Анализ этих показателей сразу показывает явный дисбаланс в сторону количественных показателей в ущерб качественным. Первые гораздо легче подсчитать хотя бы по данным уголовной статистики. И это обстоятельство во многом и обусловливает повсеместно порицаемую, но все-равно продолжающуюся «погоню за показателями».

Об этом доходчиво говорит А.Н. Медведева. Получается, что основой для оценки количественных критериев деятельности полиции служит формируемая самой полицией статистическая отчетность, главным образом отражающая уровень преступности и раскрытия правонарушений. Система сравнения количественных показателей с аналогичным периодом прошлого года призвана измерять эффективность деятельности полиции на разных уровнях: на уровне отдельного сотрудника, далее на уровне отдела, отделения и т.д. Движение между макро- и микроуровнями осуществляется посредством коррекции плана работ на численность подразделения. Данные статистической отчетности составляют основу для поощрения или наказания сотрудников. Для понимания сути функционирования этой системы принципиально важно уяснить, что понятия «зарегистрированное происшествие» и «правонарушение» не являются синонимичными. Одним из главных недостатков такой системы оценки деятельности полицейских является то, что данная система способствует подмене содержательных целей деятельности формальными: выдвигает на первый план погоню за показателями, а не реальную работу. То есть основная проблема в полиции состоит в том, что цель руководителя ОВД – это не борьба с преступностью, а борьба со статистикой, подгонка системы оценки под нужные показатели. Гонка за показателем привела к тому, что все занимаются не охраной общественного порядка, а выявлением правонарушений [27].

Оперативные подразделения ОВД также действуют в рамках этих показателей, будучи органичной частью полицейской структуры. Соответственно, они лишены возможности или не видят острой необходимости перестраиваться с количественных критериев на качественные.

И у них, как и в целом у системы МВД, имеется формальное обоснование, связанное с тем, что на протяжении последних лет преступность в Казахстане идет на заметное снижение.

Если до 2019 года по республике на 10,0 тысяч населения приходилось свыше 100 преступлений, то начиная с 2020 года данный показатель снизился до 87. В 2022 году уровень преступности в стране снизился до 80 преступлений на 10,0 тысяч населения [28]. По итогам 2024 года общее количество уголовных правонарушений составило 132 778 единиц, что на 5,3% меньше показателей 2023 года. За январь-август 2025 года в республике зарегистрировано 88,4 тысячи правонарушений, на 7,3% ниже аналогичного периода предыдущего года. По международной оценке (Numbeo) Казахстан занимает 76-е место из 148 стран с индексом преступности 45,6 из 100, что свидетельствует об умеренном уровне криминальной ситуации в стране.

Тем не менее, А.Н. Медведева делает упор на качественные критерии, что основным ориентиром разработанной системы оценки деятельности полиции является необходимость вернуть ОВД доверие граждан, поднять общественный престиж его деятельности, развернуть все полицейские подразделения и каждого сотрудника в отдельности в сторону реальной, гарантированной защиты жизни, здоровья, прав и свобод граждан, собственности, интересов общества и государства от противоправных посягательств, а также перейти к полномасштабному сервисному формату работы полицейских во всех регионах страны [27, с. 285].

И вот здесь возникает вопрос: каков механизм возврата этого доверия граждан относительно работы оперативных подразделений? Очевидно, что доверие возникает между субъектами или структурами как результат открытых и прозрачных отношений, определенной подконтрольности и подотчетности друг другу. В какой степени оперативные подразделения ОВД должны и могут быть открытыми гражданскому обществу с учетов таких принципов ОРД, как конспирация и негласность?

Если судить по вышеуказанному приказу МВД, оценка деятельности полиции осуществляется по итогам работы за полугодие и год, а состоит она из:

1) ведомственной оценки, включающей количественные критерии, основанные на сведениях правовой статистики;

2) внешней оценки, формируемой по качественным критериям, на основе ежегодных социологических исследований, проводимых Министерством национальной экономики [26].

Таким образом, оценка качества работы МВД в целом осуществляется социологами на основе мнения населения того или иного региона. Но, если они могут иметь обоснованное представление о деятельности наружных служб (участковые инспектора, патрульная полиция, разрешительная система и др.), то как они оценят качество работы оперативных подразделений?

Очевидно, что такие критерии являются внутриведомственной прерогативой. Однако, на практике они по вышеописанным причинам были подменены количественными показателями раскрытых преступлений, проведенных ОРМ, заведенных ДОУ и т.д.

Однако отойти от чисто количественных показателей в сторону качественных до сих пор не получается.

Ни в одной оперативной службе не практикуются такие критерии, как уровень оперативного перекрытия обслуживаемой территории или подучетного контингента; степень достоверности информации, получаемой от источников; доля предупрежденных уголовных правонарушений на стадии формирования преступного замысла.

Естественно, что оценить такие критерии гораздо сложнее, чем взять данные из уголовной статистики. Поэтому не удивительно, что остается такой живучей вышеупомянутая «погоня за показателями». Она выгодна для многих руководителей и сотрудников оперативных подразделений, так как

позволяет функционировать им в привычной комфортной среде, действовать в традиционной модели.

Но в стратегическом, общегосударственном масштабе такой подход вреден, поскольку не устраняет первопричины воспроизводства преступности, позволяя ей дальше развиваться и расширяться.

О том, что существующая модель деятельности оперативных подразделений является не только безнадежно устаревшей, но и принципиально опасной для стабильного функционирования общества и государства, свидетельствует анализ данных уголовной статистики по наиболее показательным видам преступлений в 2022 году, когда произошли январские события (поставившие на грань существования Казахстан), по сравнению с предыдущим «благополучным» 2021 годом.

Прежде всего проанализируем уголовную статистику по наиболее наглядным категориям преступлений, составлявшим основу указанных событий.

Так, в эфире информационного агентства «Хабар» бывший министр информации и экс-советник первого президента страны Ермухамет Ертысбаев заявил, что КНБ годами скрывал информацию о существующих в стране многочисленных тренировочных лагерях боевиков, созданных в горах [29].

Но, согласно уголовной статистике, количество выявленных фактов создания баз (лагерей) для подготовки наемников (ст. 171 УК РК) в 2021 г. – 0, в 2022 г. – 0 [25, с. 143-147].

Если нулевые показатели по данной статье объяснимы по 2021 году, когда такие факты тщательно скрывались, то почему их нет в 2022 году, когда они стали известны?

Аналогичная ситуация с иными характерными составами:

–прохождение террористической либо экстремистской подготовки (ст. 260 УК РК): в 2021 г. – 0, в 2022 г. – 0;

–наемничество (ст. 170 УК РК): в 2021 г. – 0, в 2022 г. – 0.

Количество фактов вербовки или подготовки либо вооружения лиц в целях организации террористической, либо экстремистской деятельности (ст. 259 УК РК) изменилось не принципиально: в 2021 г. – 5, в 2022 г. – 8. Кардинальная активность правоохранительных органов и специальных служб выразилась лишь в выявлении актов терроризма (ст. 255 УК РК). Если в 2021 году их было 2, то в 2022 году – 27, или в 13,5 раз больше [30].

Однако анализ данного показателя во взаимосвязи с многими смежными показал целый ряд проблем. Общеизвестно, что теракты совершаются тогда, когда существует подготовленная почва для них, то есть призывы к ним. Январские события 2022 года это наглядно показали. Но в уголовной статистике парадокс – количество актов терроризма выросло в десятки раз, а число выявленных фактов его пропаганды уменьшилось. Так, число фактов пропаганды терроризма или публичных призывов к совершению актов терроризма (ст. 256 УК РК): в 2021 г. – 61, в 2022 г. – 50. Более того, в 3,5 раза снизилось количество выявленных фактов финансирования

террористической или экстремистской деятельности или иного пособничества терроризму или экстремизму (ст. 258 УК РК): в 2021 г. – 7, в 2022 г. – 2. Аналогичным образом меньше выявлено фактов возбуждения социальной, национальной, родовой, расовой, сословной или религиозной розни (ст. 174 УК РК): в 2021 г. – 58, в 2022 г. – 46. Совсем незначительно увеличилось количество фактов создания, руководства экстремистской группой или участия в ее деятельности (ст. 182 УК РК): в 2021 г. – 1, в 2022 г. – 2 [30].

Вместе с тем общеизвестно, что терроризм не появляется на пустом месте, человек не становится сразу террористом, этому предшествует подготовительный процесс – прохождение через стадию радикализации сознания – экстремизма. В то же время этот этап остается не охваченным оперативным наблюдением. Картина та же, что и по общеуголовным правонарушениям – пока нет явных признаков терроризма, не будет реакции государственных органов на многие экстремистские проявления. Здесь тоже видится проявление феномена «гонки за показателями».

Эту проблему подметил К.Р. Тусупбеков. Анализируя ситуацию в сфере противодействия экстремизму, он пришел к выводу, что главное внимание в основном сосредоточено на реагировании на факты терроризма. Что касается экстремизма, то он остается как бы «в тени», хотя именно он является питательной средой для последующих террористических актов. Поэтому необходимо придавать большее внимание признакам экстремизма. Прежде всего, это касается создания системы мониторинга угрозы экстремистских проявлений, аналогичной вышеуказанной схеме по терроризму. В специальных и правоохранительных органах накоплен достаточно значительный объем информации о руководителях и участниках экстремистских организаций, а также об их межрегиональных и международных связях. Эта информация постоянно дополняется и меняется, как и сама оперативная обстановка. Соответственно, существует градация серьезности ситуации по линии религиозного экстремизма в зависимости от конкретных регионов. Так, например, геополитические условия объективно указывают на преимущественную распространенность деструктивной идеологии в западных и южных регионах страны и на относительно благополучную обстановку на севере и востоке. С учетом этого предлагается ввести градацию степеней опасности в регионах по линии религиозного экстремизма. С этой целью могут быть использованы буквенные (А, Б, С и т.д.) или цифровые (1, 2, 3 и т.д.) степени опасности.

Для чего это нужно? Правовое урегулирование этой актуальной области позволит более рационально распределять государственные ресурсы, выделяемые на противодействие религиозному экстремизму и терроризму. При этом можно наконец четко разделить меры по каждому из этих направлений по отдельности. Это также позволит придать более планомерный и аналитический характер бюджетному планированию расходов на эти сферы [31].

Таким образом, ситуация с комплексным упреждением проявлений экстремизма и, соответственно, терроризма, остается на том же уровне, что и до январских событий 2022 года.

Ничего не меняется и в сфере противодействия организованной преступности, которая также принимала в них участие [32].

Так, количество выявленных фактов создания и руководства организованной группой, преступной организацией, а равно участие в них (ст. 262 УК РК) даже снизилось: в 2021 г. – 93, в 2022 г. – 73 [30].

Еще одна «болевая точка» январских событий – незаконная миграция (ст. 394 УК РК) также показывает серьезное снижение: в 2021 г. – 116, в 2022 г. – 83 [30].

Это при том, что российская внешняя разведка имела информацию о подготовке январских событий в Казахстане. Она фиксировала прибытие в страну многочисленных отрядов, составленных из бойцов террористической организации «Исламское государство» (запрещена в России и Казахстане). Эти данные были предоставлены всем среднеазиатским государствам [33].

Таким образом, анализ уголовной статистики также подтверждает тезис о том, что работа правоохранительных органов, прежде всего ОВД, и их оперативных подразделений носит преимущественно фрагментарный характер по наиболее актуальным направлениям, прямо влияющим на состояние общественной безопасности в стране.

Обобщение изложенного позволяет констатировать наличие нескольких системных проблем в современных подходах к осуществлению ОРМ:

1. Существующая привычная модель ОРД ОВД не способна выявить глубинные факторы, обусловливающие постоянное воспроизводство преступности, которая динамично меняет формы и методы своей деятельности.

2. Даже в процессе и по результатам масштабного расследования январских событий 2022 года действующая модель скорректирована не была, вышеуказанные глубинные факторы остались практически нетронутыми, что создает перманентную угрозу повторения аналогов таких событий.

3. Для своевременного и адекватного противодействия современной преступности необходимы иные модели организации деятельности оперативных подразделений ОВД, построенные на упреждающих принципах.

Рассмотрению этих моделей посвящены следующие подразделы настоящего исследования.

§ 1.2. Гибридизация преступности как вызов традиционной модели ОРД

В современных условиях динамичного развития внешних и внутренних угроз и вызовов общественной безопасности особую актуальность приобретает негласная деятельность правоохранительных органов по их заблаговременному выявлению и пресечению.

Проблемы в этой сфере наглядно продемонстрировали события января 2022 года, по результатам которых Глава государства К.-Ж.К. Токаев дал поручение кардинально реорганизовать всю систему обеспечения национальной безопасности, в том числе в правоохранительных органах. Цель этих мер – быть готовыми противостоять тотальным террористическим атакам, для чего необходимо полностью перестроить деятельность разведывательного сообщества, включая внешнюю, военную, криминальную и финансовую разведку [34].

Тем самым Президент Республики Казахстан дал ясно понять, что вся эта работа должна носить опережающий характер.

С учетом этого усиливаются требования, прежде всего к оперативным подразделениям ОВД, так как они первые сталкиваются с проявлениями криминала, даже когда уголовное правонарушение еще находится в стадии умысла или начала приготовления. Как правило, единственным средством раннего обнаружения таких действий является ОРД с только ей присущим инструментарием негласного проникновения в сферу и инфраструктуру преступности.

В то же время, как указывалось выше, анализ сложившейся практики деятельности оперативных подразделений показывает очевидное ее несоответствие возникающим и прогнозируемым угрозам и вызовам общественной безопасности Казахстана.

В этом смысле примечательны результаты опроса их сотрудников о причинах неготовности к подобным событиям. Почти 70 % из них назвали комплекс таких обстоятельств: отсутствие оперативных подходов к протестной среде, незнание ее внутренней структуры, незнание методов оказания на нее влияния, незнание экономических условий возникновения протестов, неумение прогнозировать возможное их развитие (Приложение А).

Общепринято, что стандартная схема базируется на прошлом опыте выявления, предупреждения и пресечения различных уголовных правонарушений. На основе данного опыта формируются организационно-тактические аспекты работы оперативных подразделений как ответная реакция на них. Такая схема была вполне адекватна даже в недавнем прошлом, когда криминальная обстановка менялась не так динамично, и система организации деятельности успевала реагировать на эти изменения, внося коррективы в процесс обучения.

В соседней России складывается аналогичная ситуация. Там оперативные подразделения столкнулись с новыми видами преступлений,

противостояние с которыми долгое время, а в ряде случаев и в настоящее время, осуществляется методами, которые были эффективными два, а то и три десятилетия тому назад. Предпринимаемые меры пока не приносят ожидаемого результата. Изучение практики показывает, что их эффективность не превышает 30% [35].

Эту тенденцию подтверждают результаты опроса оперативных работников. Лишь треть из них говорят об эффективности такого метода ОРД, как личный сыск (Приложение А).

На этом фоне, по изученным уголовным делам, лишь в 15% упоминалось о применении каких-либо сил, средств и методов ОРД, как правило, без конкретизации, из чего сложно делать вывод об их эффективности.

Получается, что ситуация кардинально трансформировалась. Прошлый опыт быстро устаревает и не может служить надежным фундаментом для продуктивной работы. Январские события явно продемонстрировали, что сфера криминальной деятельности серьезно расширилась за счет деструктивных проявлений на различной почве (религиозной, экономической, социальной и др.), приводящих к возникновению и развитию протестной активности значительных слоев населения. Очевидно, что система ОВД и ее оперативные подразделения, настроенные преимущественно на традиционную общеуголовную преступность, не готовы к подобным вызовам и угрозам [6, с. 163].

Поэтому пришла пора переходить к иной модели, основывающейся на прогнозировании будущих криминальных событий, выработки мер по их нейтрализации и обучению им сотрудников.

Одним словом, необходимо перестраиваться с устаревшего «реактивного» подхода к перспективному «проактивному».

Разница между «реактивным» и «проактивным» способами видна из названия. Цель первого – реагировать на инциденты и не допускать их повторения. Цель второго – предотвращать их возникновение [36].

Для того чтобы выстроить проактивную модель ОРД ОВД, прежде всего необходимо перестроить действующую систему информационного обеспечения оперативных подразделений. Такая перестройка заключается в расширении информационного поля об инфраструктуре, сопутствующей любым криминальным событиям.

Например, по линии противодействия организованной преступности необходимо владеть знаниями о:

– компьютерной разведке и компьютерном поиске, предусматривающим получение интересующей информации как в процессе оперативно-розыскных и оперативно-аналитических мероприятий, так и в процессе следствия и общего контроля за развитием ситуации;

– аналитической разведке и оперативно-аналитическом поиске, с целью электронной обработки информации о преступных сообществах;

– стратегическом и оперативно-тактическом прогнозировании, которое, как и аналитический поиск, предусматривает применение моделей

компьютерного объектно-структурного анализа и методов моделирования развития ситуаций;

– оперативном управлении развитием ситуаций с использованием технологии информационно-психологического воздействия на лидеров и членов преступных формирований, информационно-психологических атаках, направленных на создание в преступных структурах неустойчивого психологического состояния тревоги, неуверенности, недоверия, страха, неотвратимости наказания, компрометации лидеров и т.д.;

– информационно-психологическом давлении на окружение преступного мира с целью его компрометации, изоляции, показа неприглядных сторон, использования разнообразных каналов массовой информации для создания общего морально-психологического фона нетерпимости к преступным проявлениям.

Отсюда видно, что помимо юридических знаний, здесь необходимы определенные психологические навыки и умения. При этом для сотрудников оперативных подразделений ОВД, использующих методы негласного проникновения в криминальную среду, такие компетенции крайне необходимы.

А.С. Овчинский показывает общую методологию «проактивной» работы в сфере организованной преступности. Примером активного целенаправленного психологического воздействия является создание «тревожной» ситуации в разрабатываемых структурах. Эта ситуация создается с помощью тревожных для них сообщений, которые массированно передаются по различным информационным каналам. Эффективность такого воздействия обеспечивается глубоким тактико-психологическим анализом внутренних и внешних отношений, моделированием и прогнозированием развития ситуации в преступной структуре. Следует стремиться к наибольшему вкладу «тревожной» ситуации в актуализацию программ активного поведения лидеров организованных преступных формирований. Это создает благоприятные условия для перехвата телефонных переговоров и, в целом, для эффективного использования технических средств снятия информации по различным каналам. Открывается возможность фиксации перемещения денег, ценностей, оружия, сбыта автомашин, выезда из данной местности, иногда физической или юридической ликвидации предприятий. В свою очередь, это открывает и определяет возможности документирования и реализации материалов оперативной работы [37].

Следующим обязательным моментом в формировании проактивной модели работы оперативных аппаратов ОВД должен стать учет экономических основ существования различных видов преступности. Как уже отмечалось выше, уголовная статистика наглядно показывает результативность работы в данном направлении. Проводимые реформы привели к тому, что в сознании оперативных работников укореняется убеждение, что экономические проявления преступности выходят за рамки их функций и относятся к компетенции иных правоохранительных органов, таких как служба экономических расследований (СЭР).

На деле эта чрезмерная специализация приводит к тому, что оперативные аппараты ОВД не выявляют финансовые основы существования организованных формирований, даже если имеют для этого необходимые оперативные подходы. В основном это связано с недостатком знаний и соответствующего образования, но немаловажным фактором является и то, что это не входит в перечень критериев оценки их деятельности.

В свою очередь, СЭР выявляют лишь экономическую составляющую криминала, не имея возможности увидеть остальную преступную схему. Там ситуация зеркальная – видя преимущественно экономическую сторону, они не владеют в нужной мере оперативной информацией обо всей сфере и инфраструктуре организованной преступности; не владеют навыками и знаниями документирования фактов традиционной криминальной деятельности. В итоге, в условиях слабого оперативного взаимодействия и традиционного недостатка доверия между УБОП и СЭР, организованные формирования сравнительно безболезненно продолжают функционировать, время от времени теряя лишь свои периферийные звенья.

В этой связи необходимо создавать в оперативных аппаратах, особенно специальных (УБОП, УПЭ, УПН), а там, где они формально существуют – активизировать, структурные подразделения – отделы, отделения, группы, в функцию которых должны входить выявление и пресечение экономической базы существования различных видов преступности.

При этом данная работа должна строиться на реальной аналитической основе, о которой сказано выше. Соответственно, для этого должна быть выстроена система подготовки, охватывающая не только юридические, но и экономические аспекты функционирования криминальной среды.

Вместе с тем, по изученным делам оперативного учета, активные мероприятия по взаимодействию с другими службами ОВД или правоохранительными органами по вышеуказанным линиям не осуществлялись. Такие меры планировались при заведении некоторых из них, но информации о их исполнении не было.

Есть еще одно важное направление современной деятельности оперативных аппаратов ОВД, которое требует отражение в их организационной структуре. Оно напрямую связано с январскими событиями 2022 года и выражается в неготовности к реагированию на подобные процессы. Как уже отмечалось выше, поводом к их активизации послужили чисто экономические вопросы, связанные с повышением цены на автомобильный газ.

Оценка этих внешне спонтанных событий с аналитических позиций показывает, что данные процессы имели свою историю. Скорее всего, планы местных предпринимателей по повышению цены обсуждались в определенных бизнес-кругах, возможно, даже доводились местным исполнительным органам.

Главной причиной этого рокового повышения стало то объективное обстоятельство, что потребление газа в Казахстане ежегодно растет, а

объемы его производства не увеличивались, оставаясь на уровне прошлых лет. При этом в период с 20 по 24 декабря 2021 года на электронной торговой площадке было проведено пять торговых сессий, в ходе которых на основе спроса и предложения сформировалась цена на сжиженный нефтяной газ. Так, средняя прогнозная оптовая цена на январские поставки сжиженного газа в Мангистаускую область составила 78 тенге/литр, а розничная цена в городах Актау, Жанаозен, а также в Мангистауском районе составила 100-120 тг/литр [38]. То есть о резком повышении цены на газ стало известно более чем за неделю до начала массовых протестных акций, но никто не придал этому процессу значения и, соответственно, не стал прогнозировать его возможные негативные последствия.

И это было не в первый раз. Подобное пренебрежение нарастающими угрозами уже имело место в недавней истории Казахстана и также привело к трагическим последствиям.

Декабрьским жанаозенским событиям 2011 года предшествовал многомесячный трудовой конфликт (с мая 2011 года) между работниками и руководством нефтедобывающих предприятий. Кроме того, на эти процессы негативно повлияли и ряд преступлений. 2 августа на предприятии «Мунайфильтрсервис» был найден убитым профсоюзный активист Жаксылык Турбаев. Убийство произошло после профсоюзного собрания, где Турбаев выступил инициатором переизбрания председателя профсоюзной организации, который, по мнению рабочих, проводил политику работодателя. 24 августа было обнаружено тело пропавшей накануне дочери председателя профсоюзного комитета рабочих компании «Озенмунайгаз» Кудайбергена Карабалаева. Рабочие-нефтяники считали, что эти события напрямую связаны с забастовкой, и что эти преступления являлись попыткой запугать бастующих [39].

Проблема заключается в том, что эта сфера никогда ранее не входила в компетенцию оперативных аппаратов ОВД, привыкших иметь дело с явными криминальными событиями. Но главная проблема заключается в том, что с последствиями подобных процессов первыми приходится сталкиваться именно системе ОВД, которая первая обязана затем устранять возникшие массовые беспорядки и нарушения общественного порядка.

При этом функции взаимодействия с общественными формированиями (различными движениями социального и политического характера) в системе ОВД возложены на службу административной полиции, которая, как известно, не осуществляет ОРД. То есть она имеет возможность наблюдать только внешнюю сторону происходящих событий, не имея механизмов выявления скрытых процессов.

Между тем аналогичные процессы происходят и в привычной криминальной сфере. Не секрет, что в настоящее время широко распространяются преступления, совершенные с использованием глобальной сети. Правоохранительные органы выработали методы противодействия тем из них, которые совершаются в общедоступном, видимом сегменте Интернета.

Однако криминал все чаще прибегает к так называемым анонимным сегментам глобальной сети, прежде всего «темному Интернету», или Darknet.

По мнению специалистов, именно там концентрируются наиболее опасные преступники: торговцы наркотиками и оружием, детьми и детской порнографией, террористы и экстремисты. Их привлекает относительная безнаказанность и защищенность анонимных сетей. По некоторым данным, обнародовавший информацию о программе электронной слежки экс-агент американских спецслужб Эдвард Сноуден тоже пользовался «темным Интернетом», чтобы установить контакт с редакцией газеты The Guardian, журналистам которой он передал сведения о деятельности западных спецслужб [40].

По мнению российских специалистов, наибольший процент наркооборота приходится на анонимную сеть, поскольку усовершенствование возможностей мобильной связи открыли перед наркодилерами новые возможности. При этом отсутствует необходимость в личном контакте сбытчика и приобретателя наркотиков. Сбытчик создает интернет-сайт с целью торговли наркотиками, приобретатели наркотиков с использованием криптовалюты обеспечивают анонимный платеж. После получения платежа наркосбытчик скрытым образом делает «закладку» и сообщает своим клиентам о месте, где можно забрать наркотики, через сообщения с использованием средств шифрования, встроенных в различные виды устройств [41].

В соседней России действует одна из самых крупных на постсоветском пространстве анонимных интернет-площадок по продаже наркотиков – Russian Anonymous Marketplace или RAMP, работающей более чем в 100 городах России, Белоруссии и Украины [42].

Учитывая тесные связи отечественного и российского криминалитета, нельзя исключать, что аналогичные площадки действуют и в сетевом сегменте Казнета. В то же время изучение практики работы оперативных аппаратов ОВД РК в этом направлении показало отсутствие каких-либо результатов.

Российско-украинский конфликт спровоцировал взрывной рост нелегального оборота оружия по всему миру.

По данным независимого исследовательского агентства The Small Arms Survey, в настоящий момент на Украине находится около 5 миллионов единиц нелегального оружия. Украина превратилась в чёрный рынок нелегального оружия №1 в Европе. В августе 2020года тогдашний глава МВД Украины Арсен Аваков рассказывал, что оружие на «черный рынок» поставляют военные и сотрудники Нацгвардии. Сегодня, когда на Украину льётся поток оружия, его так много, что цены ползут вниз. Торговцы оружием проводят скидочные акции. Знаменитый пистолет Глок сегодня в Darknet стоит всего 500-600$. Столько же стоит пистолет Смит и Вессон. Легендарная Беретта можно приобрести за 700$, а новый автомат АК-47 – за 550$. ПМ (пистолет Макарова) стоит на чёрном рынке в пределах 700 $, автоматический пистолет Стечкина (АПС) – 1300$, железный цинк с

патронами калибра 5,45мм (1080 штук) – 120$, ценник на гранаты Ф-1и РГД-5 начинается от 100$ за штуку. Ручные гранатометы стоят от 500$, станковый гранатомет СПГ-9 - 3000$. Винтовки с оптикой натовского образца с базовой ценой 1600$ сейчас стоят 1200$. Противотанковые управляемые ракеты, украденные при поставках из США для армии Украины – Javelin ATGM, продаются по 30 000$ [43].

Судя по этой информации, сравнительно за небольшую сумму можно приобрести через Darknet партию оружия, достаточную для снабжения небольшой армии. Это тем более тревожно в свете уроков январских событий 2022 года. При таком подходе, организаторам террористических атак будет не обязательно идти на штурм административных зданий МВД и КНБ, чтобы завладеть арсеналом оружия.

И этот канал его оборота в настоящее время практически не отслеживается правоохранительными органами. Тем самым создается большой риск бесконтрольного накопления криминогенного потенциала, который может активизироваться в любой момент.

В такой ситуации меры противодействия всегда оказываются вторичными, поскольку они – «ответ». Другими словами, во взаимодействии с криминальными рисками общество неизменно «играет вторым номером», – позиция невыгодная в силу неизбежной роли догоняющего. Это утраченный шанс минимизировать (а может, и подавить) опасность в зародыше, прервать развитие потенциала [44].

Чтобы избежать подобного развития событий, необходимо работать на опережение, то есть внедрять проактивную модель. Прежде всего, необходимо в заинтересованных оперативных службах МВД – ДБОП, ДПЭ, ДПН – при общем руководстве Центра противодействия киберпреступности начать обучение своих сотрудников методам поисковой работы в сегменте Darknet. На следующем этапе появится возможность проводить ОРМ по идентификации поставщиков и заказчиков наркотиков, оружия и иных запрещенных к обороту предметов.

Вместе с тем методика такой работы пока не создана.

Такой подход неизбежно повлечет за собой трансформацию и развитие в проактивном ключе аналитической работы оперативных подразделений ОВД. А.С. Овчинский называет ее инициативной аналитикой.

Ее задача – это получение и формирование потоков оперативно-розыскной информации по основным направлениям борьбы с преступностью, наркобизнесом, терроризмом, экстремизмом и пр. Речь идет о генерировании такого информационного продукта, который позволяет оперативно принимать адекватные меры по предотвращению преступлений и пресечению преступной деятельности непосредственно из складывающейся ситуации или на основе выявления тенденций развития того или иного антисоциального явления [8, с. 34].

Сущность инициативной оперативно-розыскной аналитики, упоминаемой А.С. Овчинским, в целом совпадает с сущностью предлагаемой

проактивной модели, так как в основе обеих лежит принцип упреждающего воздействия на криминогенные факторы.

Их стратегическая задача заключается в том, чтобы деятельность правоохранительных органов и уголовную политику наполнить новым смыслом: борьбой не только с самой преступностью, но и с наиболее опасными ее качествами и проявлениями. Первое стратегическое направление деятельности правоохранительных органов должно состоять в том, чтобы интрузивные качества преступности, связанные с проникновением ее во все поры общества, менялись на экструзивные, то есть преступность выдавливалась бы из общественных отношений и из легальных сфер деятельности усилиями оперативных аппаратов и следственных органов. При этом преступность может создавать свои собственные криминальные отношения и структуры, криминальные сферы деятельности, развивать криминальные традиции, порождать криминальную субкультуру – строить по существу свое альтернативное общество. Наличие криминального альтернативного общества, этой «сточной ямы социальных отходов», однако не столь опасное явление, как тотальная криминализация общественных отношений, когда в общественном сознании стираются грани между преступным и непреступным, и вся общественная жизнь начинает подчиняться интересам преступных сообществ [8, с. 93].

Таким образом, А.С. Овчинский предлагает обществу и государству выбор между большим и меньшим злом, то есть процесс управляемого контроля преступности, что также вполне укладывается в исследуемую проактивную модель.

Второе стратегическое направление деятельности правоохранительных органов должно быть сконцентрировано против деструктивных проявлений организованной преступности. Как показывает мировой опыт, организованная преступность может играть в обществе в определенном смысле и конструктивную роль, то есть содержать конструктивные элементы, быть заинтересованной, например, в развитии тех секторов экономики, над которыми устанавливается криминальный контроль, в строительстве и расширении инфраструктуры, в частности, связанной с игорным и туристическим бизнесом. Отмывание криминальных доходов путем инвестирования их в реальные сферы экономики содержит, безусловно, известные опасности, особенно для неокрепших социально-экономических систем. Однако это все же значительно меньшее зло, чем извлечение криминальных доходов из разрушения производственных отношений, перераспределения собственности или путем непосредственного изъятия денежных средств у миллионов людей и из государственного бюджета. Таким образом, в оперативной работе и следственной практике следует различать деструктивные и условно конструктивные элементы в организованной преступной деятельности. Уголовная практика должна быть направлена на борьбу, прежде всего, с теми элементами организованной преступности, которые составляют «злокачественные опухоли» и своими «метастазами» разрушают общественный организм, их породивший. В то же

время те элементы системы организованной преступности, которые паразитируют на несовершенстве экономических, социальных и государственных отношений, некоторое время могут заполнять определенные ниши общественной жизни, поскольку природа дает неисчерпаемые примеры довольно гармоничного соседства самых разнообразных паразитов как рядом, так и внутри организма [8, с. 93-94].

Интересный взгляд на место и роль организованной преступности в общественной жизни продемонстрировал один из нобелевских лауреатов по экономике Джеймс Бьюкенен.

Он применил к сфере организованной преступности законы конкуренции и монополии, существующие в экономике, и пришел к следующему выводу. Монополия в производстве обычных товаров и услуг социально неэффективна, поскольку сокращает предложение. Но если монополия в предложении «хороших» товаров социально нежелательна, монополия в предложении «плохих» товаров может быть социально желательной. Следовательно, монопольная организация преступности социально предпочтительнее конкурентной организации, так как сокращает общее количество преступлений [45].

Ранее другой американский экономист-криминолог, также лауреат Нобелевской премии Томас Шеллинг высказывал мысль, что на определенной ступени своей эволюции организованная преступность начинает выполнять социально полезные функции. Ее стремление к монополизации криминальной деятельности приводит к минимизации числа резонансных преступлений, вызывающих излишний общественный резонанс. Поэтому желательно, чтобы некоторые виды преступности были бы более организованными [46].

Иными словами, их подход говорит о том, что лучше иметь на территории оперативного обслуживания одну крупную ОПГ, контролирующую ситуацию и регулирующую уровень криминала, чем несколько противоборствующих групп, выясняющих свои отношения при помощи насильственных методов.

Естественно, при такой позиции возникает закономерный вопрос: не означает ли это некоторое примирение с существованием организованной преступности как социального явления? Более того, не станет ли такая политика определенным сращиванием государства и общества с ней?

Свой ответ на подобные опасения Дж. Бьюкенен сформулировал следующим образом: «Я хотел бы подчеркнуть, - пишет он, - что в моем анализе нет ничего, что подразумевало бы эту точку зрения». Проделанное им исследование «лишь наводит на мысль, что могут быть выгоды от монопольной организации преступности». Автор только предлагает, чтобы «правительства выбрали пассивную роль, наблюдая попытки предпринимателей сократить эффективную конкуренцию в криминальном производстве. Практически это предложение сводится к предостережению против... «крестовых походов» на организованную преступность,

проводимых за счет снижения правоохранительных усилий, нацеленных против обычной, конкурентной преступности» [45, с 54].

Такой подход соответствует формирующейся в отечественной практике тенденции отхода от максималистской парадигмы «борьбы с преступностью до полного её искоренения» к взвешенной уголовной политике сдерживания путём противодействия. Это нашло отражение в изменении наименований ряда отраслевых оперативных служб ОВД – противодействия наркопреступности и экстремизму, – названия которых прежде содержали слово «борьба». УБОП, однако, до сих пор расшифровывается как Управление по борьбе с организованной преступностью.

Третье стратегическое направление усилий правоохранительных органов – это преодоление неуязвимости высших эшелонов криминальной иерархии, ослабление системы защиты организованной преступности. Сложившаяся система защищенности авторитетов, лидеров преступного мира и их пособников из числа коррумпированных чиновников обусловлена многоуровневым влиянием преступных сообществ на властные структуры и огромными объемами денежных средств, которые находятся в обороте в преступном бизнесе. Не раз уже говорилось о необходимости подрыва экономических основ и финансовых возможностей организованных преступных сообществ, а также о заслоне для «выдвиженцев» преступного мира на пути во властные и управленческие структуры. Основная задача третьего направления заключается в создании и укреплении оперативных позиций непосредственно в криминальной среде и в различных сферах организованной преступной деятельности. Что означает установление контроля, а в идеале – и создание механизмов управления криминальными процессами в обществе [8, с. 94].

И эта задача также совпадает с сущностью предлагаемой проактивной модели, а создание таких механизмов управления и контроля будет детально исследовано ниже.

Но если представить, что достигнуты конкретные успехи в движении по трем намеченным направлениям, то можно получить вполне приемлемый образ организованной преступности будущего. Во-первых, эта преступность имеет экструзивный характер, она вытеснена из всех сфер общественных отношений и из многих сфер легальной деятельности. Представляя собой некоторое альтернативное общество, притягивающее к себе криминально настроенных по тем или иным причинам личностей, она является «сточной канавой» для негативных социальных устремлений. Во-вторых, эта преступность содержит определенные конструктивные элементы, давая выход отрицательным социальным энергиям, с одной стороны. Паразитируя, с другой стороны, на общественном организме, она питается его «отходами», заполняя только те социальные и экономические ниши, которые в данный момент не представляют интереса для здорового общества. Наконец, в-третьих, эта преступность контролируема и управляема. Ее лидеры и авторитеты в любой момент могут оказаться в местах лишения свободы, если в деятельности их организованных групп и сообществ будут выявлены

деструктивные или интрузивные элементы. Как альтернативу интрузивно-деструктивно-мимикрийной преступности, то есть ИДМ-преступности, можно сформировать представление об экструзивно-конструктивно-управляемой преступности, то есть об ЭКУ-преступности [8, с. 95-96].

Подобный образ преступности будущего представляется в целом обоснованным. Однако очевидно (о чем детально изложено выше), что существующая модель деятельности оперативных подразделений ОВД – реактивная – объективно не способна обеспечить формирование этого образа с силу неадекватности применяемых сил, средств и методов.

Только обороняясь, невозможно победить ни в борьбе с преступностью, ни в вооруженном противостоянии, ни в информационной войне. Для достижения решающего превосходства над противником требуются активные, упреждающие действия. Борьба в информационном пространстве должна иметь наступательный характер. И здесь для достижения стратегических целей наряду с политической волей нужно фундаментальное аналитическое обеспечение, позволяющее не только в инициативном порядке выявлять и обезвреживать аттракторы хаоса, информационно-психологические вирусы, очаги деструктивного влияния на массовое сознание, но и предвидеть далеко идущие последствия процессов, происходящих как в реальном, так и в виртуальном мирах [8, с. 101].

Иными словами, на смену устаревшему реактивному подходу необходимо разрабатывать и внедрять в практику оперативных подразделений ОВД элементы «проактивного» подхода, под которым предлагается понимать систему оперативно-розыскных, организационных и управленческих мер, основанных на инициативной разведывательно-поисковой работе и аналитическом прогнозировании развития криминогенной ситуации, в целях оказания упреждающего контролирующего воздействия на ее ключевые элементы с использованием всех сил, средств и методов ОРД ОВД для решения задач, регламентированных Законом РК об ОРД [47].

Ключевыми в предлагаемой дефиниции является понятие «упреждающее контролируемое воздействие», детальное рассмотрение сущности которого и поэлементный анализ применительно к настоящему времени и среднесрочному будущему представлены ниже.

Проактивный подход не является чем-то принципиально новым в теории ОРД ОВД. Многие его элементы содержатся в ее разведывательно-поисковом характере, о котором писали такие известные российские ученые в сфере ОРД, как К.К. Горяинов, В.С. Овчинский, Г.К. Синилов, А.Ю. Шумилов [48], Ю.Ф. Кваша, С.Е. Матвеев, К.В. Сурков [49], Г.М. Меретуков, Е.С. Лунина, С.Н. Бирюкова [50], В.П. Легостаев [51] и многие другие.

Из отечественных специалистов эту проблему затрагивали А.Д. Шаймуханов [52], К.С. Лакбаев [53], М.П. Сысалов [54], Р.Ш. Карымсаков, М.А. Дусанбекова [55], М.М. Галиханов и ряд других специалистов.

Ряд норм Закона РК об ОРД также в той или иной мере указывают на ее разведывательно-поисковый характер. Прежде всего это проявляется в названии некоторых ОРМ и действий (ст. 1):

- оперативный поиск на сетях связи;
- поиск и отождествление личности по приметам;
- розыск;
- поиск устройств незаконного снятия информации.

Аналогичным образом задачи ОРД, регламентированные статьей 2, все так или иначе подразумевают разведывательно-поисковую направленность [24].

В то же время, анализируя данные нормы и точки зрения вышеприведенных авторов, выявляются существенные различия между проактивным подходом и устоявшимся взглядом на разведывательно-поисковый характер ОРД ОВД.

Прежде всего, это традиционная «зацикленность» последнего на преимущественное получение фактических данных для привлечения к ответственности лиц, причастных к совершению уголовных правонарушений, то есть выполнение лишь одной задачи, регламентированной в статье 2 Закона РК об ОРД – выявление, предупреждение и пресечение преступлений [24].

Об этом говорят и результаты изучения дел оперативного учета. По всем ним конечная цель обозначалась в виде привлечения фигурантов к уголовной ответственности. Меры предупреждения их криминальной деятельности не планировались. Но проактивный подход – это гораздо более широкий взгляд на ОРД ОВД. Прежде всего это касается самой первой задачи – защита жизни, здоровья, прав, свобод, законных интересов человека и гражданина, собственности от противоправных посягательств, которая обычно воспринимается как декларативно-вспомогательная, подводящая к основной задаче выявления, предупреждения и пресечения преступлений.

Но смысл этой нормы совершенно самостоятельный; именно она указывает на главную функцию ОРД ОВД – расширенную безопасность общества и государства не только (а может быть, и не столько) от уголовных правонарушений, сколько от комплекса негативных процессов, регулярно порождающих новые вызовы и угрозы стабильному развитию Казахстана. Даже «навскидку» можно назвать такие серьезные факторы, как организованный криминал (включая ИДМ-преступность) в 1990-е годы; религиозный экстремизм и терроризм в 2010-е годы; деструктивная протестная активность в настоящее время; прогнозируемая геополитическая турбулентность и экономические кризисы в ближайшее десятилетие.

Эти процессы напрямую влияют и обусловливают организацию ОРД ОВД, требуя адаптации к ним.

С учетом этого совершенно в новом свете предстает другая задача – содействие в обеспечении безопасности общества, государства и укреплении его экономического потенциала и обороноспособности.

Традиционное отношение к данной норме заключается в том, что она априори относится к исключительной компетенции специальных служб РК – КНБ, СВР «Сырбар» и военной разведки Министерства обороны. До недавнего времени такой подход был оправдан, но теперь он серьезно корректируется активизацией вышеизложенных стратегических вызовов и угроз.

Дело в том, что анализируемая задача ОРД состоит из трех частей:

1) содействие в обеспечении безопасности общества и государства;

2) укрепление его экономического потенциала;

3) укрепление его обороноспособности.

Очевидно, что первая часть входит в компетенцию не только специальных служб, но и всех органов-субъектов ОРД, прежде всего ОВД. Однако на практике мало кто обращает на нее внимание, и напрасно, потому что данная норма является продолжением первой задачи и в совокупности с ней составляет правовую базу для проактивной модели ОРД ОВД. То есть для ее активизации нет необходимости создавать новую нормативную базу, а следует просто активизировать «спящие» нормы, ошибочно воспринимаемые как декларативные или вспомогательные.

Это, по существу, возврат к истокам замысла законодателя, предусмотревшего при формировании рассматриваемых норм такую широкую «опцию» ОРД на случай кардинального изменения криминогенной ситуации, что наблюдается в настоящее время.

Более того, учитывая, что экономические факторы в развитии государства всё чаще связаны с состоянием общественной безопасности, можно прогнозировать, что и вторая часть – укрепление экономического потенциала – является не отдаленной, а смежной с ОРД ОВД областью, особенно при развитии ее проактивной модели.

Ну, и наконец, военная сфера также начинает с ней сближаться, прежде всего с точки зрения плавного перемещения оборонных технологий в правоохранительную деятельность.

В этом смысле целесообразно адаптировать положения военной сферы, касающиеся стратегии ведения современных войн четвертого поколения (так называемых «гибридных»). Но перед этим необходимо рассмотреть, что из себя представляют эти поколения.

Первое поколение – когда вооруженная борьба в этих войнах осуществлялась на тактическом уровне подразделений исключительно живой силы – пешими воинами и конницей, оснащенными холодным оружием. Войны первого поколения характерны для рабовладельческой эпохи (VI в. до н.э. – II в. н.э.).

Формы и способы ведения войн второго поколения были обусловлены революцией в военном деле, связанной с появлением пороха и гладкоствольного оружия.

Дальнейшее развитие человеческого общества способствовало прогрессу в технологиях, появлению большого количества нарезного многозарядного стрелкового оружия и нарезной артиллерии, обладающих

большой дальностью, скорострельностью и точностью. Это привело к очередной революции в военном деле и породило войны третьего поколения, которые проводились уже в оперативно-тактических масштабах.

В середине XX века произошла очередная революция в военном деле, вызвавшая возникновение войн четвертого поколения, когда они приобрели стратегический масштаб. Этому способствовали ускоренное создание и принятие на вооружение в больших количествах автоматического оружия, бронетехники, боевой авиации, боевых надводных и подводных кораблей, появление радиолокационных средств и средств связи различного назначения, новых транспортных средств [56].

Анализ показывает, что все крупные вооружённые конфликты в мире в настоящее время происходят в парадигме войн именно четвертого поколения, которые, помимо новых оружейных технологий, имеют еще одну специфическую черту. Она выражается в преобладающем развитии информационно-психологических воздействий на индивидуума, группу, целевую аудиторию или население городов и целых стран.

На этом основываются принципы ведения войн четвертого поколения (Fourth-generation warfare, или 4GW). Наиболее важными из них являются:

1. Асимметричность конфликта. В условиях трансформации современного общества под влиянием процессов глобализации участниками конфликта являются транснациональная корпорация и традиционное государство. Принцип асимметричности конфликта означает использование асимметричных методов борьбы, таких как оружие и технологии, которые радикально отличаются от того, что имеет противник, при оказании международной политической, информационной и юридической поддержки.

2. Маневренность. В стратегии 4GW традиционная военная сила утрачивает свое значение, массированные атаки и огневая мощь перестают быть решающими факторами. «Полем боя» становится все общество противника, исчезает понятие стратегического тыла. Удар наносится по уязвимым точкам, по важным объектам, памятникам культурного наследия, личностям и группам, способным к организованному сопротивлению, умеющим консолидировать общество.

3. Взаимодействия сетевых сообществ. В условиях тотальной сетевизации всей структуры противоборства меняются стратегические факторы ведения войн четвертого поколения. Высшее военное руководство заменяется отдельной боевой единицей информационных операций с использованием глобальных СМИ. Формируется многопотоковая система управления ячеисто-сетевого типа с несколькими универсальными центрами принятия решений, что предполагает возможность структурировать и обрабатывать огромное количество разноплановой информации, используя хакерские атаки.

4. Народная партизанская война, или «война без правил». Понятие фронта отсутствует, внешняя агрессия может быть закамуфлирована под гражданскую войну, акции гражданского недовольства и неповиновения и т.д.

5. Хаос, или создание атмосферы полной неопределенности. Информационно-психологическое воздействие направлено на раскалывание и вытеснение противника. Психологическое и физическое воздействие осуществляется на самые уязвимые места противника, а не на ожидаемые направления. Это аморфная, но скоординированная атака против единой цели в разных направлениях; это принцип доминирования телевизионных новостей.

6. Принцип спецэффектов, борьбы в когнитивно-смысловой, в семантической сферах и в сфере восприятия. Главным приоритетом информационно-психологического воздействия является фокусирование внимания противника на экономических, политических, культурных условиях безопасности, которые обостряют обиды населения, например, обсуждаются и вводятся разнообразные санкции и «страшилки» экономического и социального характера. В стратегии 4GW нет реальных сражений, а есть борьба эффектов. Тот, кто создает эффекты более высоких порядков, тот побеждает в стратегии 4GW.

7. Принцип боевой стаи, т.е. принцип работы автономными или полуавтономными боевыми группами (подразделениями, частями), связанный с децентрализованной, разнообразной, нешаблонной тактикой, которая выбирается каждым подразделением самостоятельно в рамках следования единой для всех стратегической цели. Цель – преследование противника и лишение его инфраструктуры и ресурсов.

8. Принцип индивидуализации ответственности, или «победа без управления». Огромное значение приобретает подготовка отдельного бойца профессиональных боевых сил, который должен быстро принимать самостоятельные решения. В ситуации лимита времени для связи с командиром и получения приказа знания и навыки такого бойца должны быть очень высокими, он должен понимать и осознавать план и цели операции, чтобы действовать самостоятельно для их достижения [57].

Конечно, не все эти принципы применимы в сфере ОРД ОВД. Но их анализ дает возможность сформулировать аналогичные принципы, но уже применительно к специфике противодействия преступности (прежде всего, ее организованным формам). Поэтому в постановочном плане предлагаются следующие принципы «проактивной» стратегии ОРД ОВД (они же являются ее элементами, применяемыми в различной последовательности):

1. Принцип асимметричности. Он означает использование оперативными подразделениями нестандартных инструментов, применение которых криминальные структуры не ожидают. Например, массовый легендированный «вброс» через социальные сети и СМИ информации, выставляющей их руководителей в негативном свете перед конкурентами, партнерами и обществом.

2. Принцип маневренности. Помимо традиционных «точек воздействия» на преступников (причастность к конкретным преступлениям), избираются другие уязвимые места – зависимости и наклонности, привязанности к родным и близким, приверженность определенным идеям.

Комбинированные удары в виде гласных и негласных ОРМ наносятся по всем выявленным «болевым точкам», создавая кумулятивный эффект и подрывая личностную ценность как отдельного участника криминальной структуры, так и ее в целом.

3. Принцип «боевой стаи», т.е. работа нескольких самостоятельных или условно самостоятельных подразделений, которые сосредотачиваются на решении одной задачи (например, разработка одной криминальной структуры). Каждое подразделение выполняет задачу своими методами, координируя с другими только вопросы взаимодействия. Цель – нанесение ударов сразу с нескольких сторон. Так, одна группа отрабатывает причастность фигурантов к конкретным преступлениям. Другая – занимается выявлением экономической основы их криминальной деятельности. Третья – ищет коррумпированные связи фигурантов с представителями правоохранительных и иных государственных органов.

4. Принцип управляемого хаоса, или создание беспорядка и суматохи у противника. Реализация первых двух принципов способен привести к дезорганизации спланированной криминальной деятельности, что автоматически снижает ее общественную опасность. Смысл данного принципа заключается в инициировании и управлении таким хаосом в общественно полезном направлении – недопущении активизации любой криминальной деятельности.

Данный принцип имеет своеобразный «подпринцип» – управляемой эскалации хаоса, чтобы в результате проводимых ОРМ не вызвать неконтролируемой вспышки агрессии и насилия фигурантов друг к другу или иным лицам.

5. Принцип индивидуализации ответственности, когда решающее значение приобретает подготовка каждого отдельного сотрудника, который в определенных границах может принимать самостоятельные решения, не тратя время и ресурсы на их согласование с руководством. Эти границы могут быть нормативно установлены ведомственными документами [6, с. 164].

Очевидно, что изложенные принципы кардинально отличаются от существующей «реактивной» модели организации деятельности оперативных подразделений ОВД.

Поэтому, прежде всего, структура предлагаемой проактивной модели должна в обязательном порядке содержать такой элемент, как критерии оценки их работы.

Как отмечалось выше, ведомственным приказом определены количественные и качественные критерии такой оценки. Также указывалось, что качественные показатели не адаптированы к специфике ОРД ОВД, из-за чего преобладающими стали количественные критерии, порождающие «гонку за показателями».

В этой связи для реализации рассматриваемой проактивной модели предлагаются следующие универсальные качественные критерии оценки деятельности оперативных подразделений ОВД:

1. Уровень оперативного перекрытия обслуживаемой территории (объекта) – информационное освещение (наличие источников) наиболее криминогенно пораженных участков либо подучетного контингента.

2. Качество получаемой оперативно-розыскной информации: достоверность, ценность, своевременность.

3. Наличие информации о финансовой и материальной базе выявленных преступных групп:

– подконтрольные экономические структуры, способы криминального контроля за ними;

– каналы и методы получения и легализации доходов, полученных незаконным путем;

– каналы и способы приобретения предметов, орудий и оружия для совершения уголовных правонарушений;

– каналы и способы сбыта похищенного имущества.

4. Меры оперативно-розыскной профилактики:

– выявление причин и условий, способствующих совершению уголовных правонарушений, их устранение;

– выявление лиц, у которых, судя по их образу жизни или поведению, может формироваться преступный замысел, либо уже началось приготовление к уголовному правонарушению;

–оказание на них гласного, негласного или зашифрованного воздействия с целью блокирования преступного умысла либо пресечение уголовных правонарушений на стадии приготовления.

Соответственно, реализация этих критериев оценки требует иного подхода к организации специальной подготовки сотрудников оперативных подразделений ОВД.

Для ее адаптации к проактивной модели необходимо серьезно трансформировать систему ведомственного образования.

На подобные актуальные проблемы обращал в свое время внимание К.С. Лакбаев. Он отмечал, что подготовка оперативных работников в ведомственных вузах ведется по единой оперативно-розыскной специализации. Такой подход не отражает объективные закономерности развития современной преступности и существующую организационную структуру оперативных аппаратов, включающую наряду с УКП такие специальные подразделения, как УБОП, УПЭ, УПН и иные. С учетом этого им предлагалось разделить единую оперативно-розыскную специализацию в ведомственных вузах системы МВД РК на ряд более узких специализаций по конкретным линиям:

–криминальная полиция (общеуголовная преступность);

–организованная преступность (криминальные формирования);

–экономическая преступность (в том числе связанная с организованной преступностью);

–наркопреступность (как местная, так и межрегиональная);

–коррупционные связи криминала с органами власти;

–терроризм и религиозный экстремизм;

–применение специальных технических средств;

–киберпреступность;

–оперативно-розыскная психология [53, с. 153].

Еще одним неразвитым направлением является специальная подготовка оперативных работников для учреждений уголовно-исполнительной системы (УИС). Если для других служб УИС существуют целевые программы обучения в специализированном ведомственном вузе (Костанайская академия МВД РК им. Ш. Кабылбаева), то сотрудники оперативных аппаратов готовятся по общей модели, зачастую не учитывающей явную специфику такой деятельности.

Дополнительный негативный эффект придает традиционная разобщенность оперативных аппаратов территориальных подразделений полиции и учреждений УИС. Пенитенциарная система неоднократно передавалась из одного государственного органа в другой, что отрицательно сказалось на культуре взаимодействия. Не секрет, что между оперативными работниками двух систем, несмотря на общую функцию противодействия преступности, стоят различные узковедомственные задачи: для УИС прежде всего приоритетно соблюдение режима содержания, для полиции – раскрытие ранее совершенных уголовных правонарушений. О синхронизации своей работы в таких условиях, а тем более оперативно-розыскной профилактике, говорить сложно.

На проблемы в организации такого взаимодействия указывают результаты изучения дел оперативного учета. Лишь в 20% из них предусмотрены меры по взаимодействию с учреждениями УИС, расположенными на территории обслуживания соответствующего оперативного подразделения .

Кроме того, учитывая злободневность происходящих криминогенных процессов (январские события 2022 года и другие), правомерно говорить об актуальности специализации по такой линии, как противодействие деструктивной деятельности на политической, экономической, социальной и иной почве.

Вместе с тем в современных условиях говорить о кардинальном расширении перечня специализаций оперативно-розыскного профиля пока преждевременно. Однако хотя бы частично решить проблему можно за счет введения специальных курсов по каждому из выше предложенных направлений. При этом разработка учебных программ должна охватывать стратегические уровни, такие как ИДМ-преступность, геополитические аспекты криминальной деятельности, генезис и предупреждение социальных протестов, и т. п.

Подготовка специалистов такого профиля обеспечит предлагаемую проактивную модель ОРД ОВД квалифицированными сотрудниками, способными выстроить наиболее оптимальную и гибкую систему противодействия преступности.

Таким образом, анализ сущности проактивного подхода к осуществлению ОРМ ОВД РК позволяет сформулировать следующие выводы:

1. Проактивная модель является следующей эволюционной ступенью развития оперативных подразделений ОВД, дающей возможность установить реальный контроль за развитием криминогенной ситуации.

2. Внедрение проактивного подхода способно коренным образом изменить соотношение сил в вечном противостоянии общества и государства, с одной стороны, и криминала (в широком смысле) – с другой, со значительным перевесом в пользу общества и государства.

3. Предложенные принципы проактивного подхода для оперативных подразделений ОВД призваны стать универсальным рабочим инструментом для эффективного противодействия преступности по всем линиям.

Конкретной реализации этих принципов посвящен следующий раздел настоящего исследования.

ГЛАВА 2. КОНЦЕПЦИЯ ПРОАКТИВНОГО ПОДХОДА К ОСУЩЕСТВЛЕНИЮ ОРМ ОВД РК

§ 2.1. Оперативно-розыскное прогнозирование как информационная основа проактивного подхода

Динамичное развитие современных общественно-политических и социальных процессов сопровождается не менее динамичным структурным изменением преступности. Для адекватного противодействия ей правоохранительным органам приходится планировать свою деятельность с учетом этих процессов, что невозможно без прогнозирования.

В настоящее время в юридической литературе выделяются криминологическое и криминалистическое прогнозирование. И то, и другое рассмотрены достаточно давно, и подходы к ним известны.

Так, Г.А. Аванесов детально рассмотрел теорию и методологию криминологического прогнозирования более пятидесяти лет назад [58]. Касались этой проблемы и другие видные ученые-криминологи: М.П. Клейменов [59], В.В. Лунеев [60], В.Н. Кудрявцев и В.Э. Эминов [61] и многие другие.

Аналогичным образом уже сложились устоявшиеся взгляды на криминалистическое прогнозирование, которое рассматривали в своих трудах Р.С. Белкин [62], К.В. Бугаев [63], А.Н. Васильев и Н.П. Яблоков [64], А.Ф. Волынский и В.П. Лавров [65], А.Н. Литвинов и Р.Л. Степанюк [66] и другие ученые.

В отличие от криминологического и криминалистического прогнозирования, оперативно-розыскное прогнозирование является новым и пока недостаточно изученным институтом. В Казахстане его исследование находится в зачаточном состоянии. Это понятно в силу того, что в отечественной науке ОРД еще не исследовано детально такое направление, как оперативно-розыскная криминология, составной частью которой является прогнозирование.

Более того, сфера оперативно-розыскной криминологии находится в стадии становления даже в России, считающейся общепризнанным лидером в области ОРД ОВД на постсоветском пространстве. Как отмечает А.П. Исиченко, в настоящее время – это зарождающееся междисциплинарное направление исследований [67].

Соответственно, какая-либо стройная теория оперативно-розыскного прогнозирования также еще не выстроена, и между учеными идут дискуссии на этот счет [68].

Так, некоторые российские специалисты понимают под оперативно-розыскным прогнозированием тематический или ситуационный анализ оперативно-розыскной и иной информации в отношении представляющих оперативный интерес событий, лиц (групп лиц, категорий лиц) с выводом о вероятном развитии событий, индивидуальном либо групповом преступном

поведении лиц, а также совершении конкретных преступлений и иных фактов, представляющих интерес [68].

Из данного определения очевидно, что такое прогнозирование, носящее явный упреждающий (проактивный) характер, является сложной мыслительной задачей, требующей определенный уровень интеллекта, профессионализма, аналитического мышления, а также способности и возможности творческой обработки информации.

Интересную интерпретацию данной проблемы дает А.С. Овчинский, который называет такую прогностическую деятельность предиктивной криминологией. По его мнению, ее задача заключается в том, чтобы предсказать развитие криминальной ситуации, то есть время и место возможного преступления, оценить вероятность криминальной активности отдельных лиц, находящихся в поле зрения оперативных аппаратов, определить характер и направления деятельности организованных преступных формирований, просчитать возможность террористических угроз и опасность криминальных последствий тех или иных тенденций, которые развиваются в жизни общества. В отличие от традиционной, предиктивная криминология опирается непосредственно на ресурсы оперативно-розыскной информации. Эти информационные ресурсы сейчас содержат огромные массивы самых разнообразных данных о лицах, их связях, сообществах, так или иначе связанных с противоправной деятельностью [8, с. 56].

Это действительно так. В информационных базах ОВД РК, а также специальных учетах оперативных подразделений на разных уровнях, находится очень большой объем информации о различных криминальных фактах и их признаках. Проблема заключается в том, что попытка грамотно использовать ее требует не только высокой квалификации оперативного работника, но и специализированных программных продуктов, адаптированных под потребности ОРД ОВД.

Видимо, поэтому более половины опрошенных сотрудников оперативных подразделений ОВД отметили, что прогнозирование развития на основе комплекса оперативно-розыскной информации у них либо не проводится, либо осуществляется редко (Приложение А).

Это подтверждают и результаты изучения внутреннего служебного делопроизводства оперативных подразделений ОВД. В подавляющем большинстве планов на календарный период (свыше 90%) отсутствовали промежуточные выводы и прогнозы дальнейшего развития оперативной обстановки на обслуживаемой территории.

На этом фоне главный вопрос оперативно-розыскного прогнозирования состоит в том, какого рода преступления можно ожидать? По мнению А.С. Овчинского, современная криминология может дать ответ на этот вопрос, так как все окружающие явления, процессы и отношения так или иначе построены на информационных взаимодействиях. Учитывая их характер, им предлагается придать каждому виду правонарушения или преступления определенное числовое значение – параметр рецидивности.

Под ним понимается численное значение вероятности того, что рассматриваемое конкретное правонарушение либо преступление, совершенное в прошлом, может повлечь аналогичное или более серьезное в будущем. Непосредственно величины интересующих параметров рецидивности могут быть получены на основе криминологических исследований, опирающихся на обработку статистических данных о рецидивной преступности. В этом случае потребуется анализ уже криминологической информации с выявлением корреляционных зависимостей между первыми правонарушениями или преступлениями и последующей криминальной активностью различных контингентов лиц, привлекавшихся неоднократно к административной или уголовной ответственности. Числовые значения параметров рецидивности по разным видам преступлений могут быть установлены и на основе экспертных оценок, то есть знаний, выраженных во мнениях опытных сотрудников оперативных или следственных аппаратов [8, с. 61].

Нестандартная позиция А.С. Овчинского не лишена смысла. Конечно, его идея промаркировать различные виды криминальных деяний и присвоить им определенный цифровой индекс может столкнуться с трудностями практического плана. Основной из них будет оценочный подход со стороны правоприменителей к оценке параметра рецидивности того или иного лица.

Но, в то же время, мысль о ранжировании его возможной общественной опасности интересна с точки зрения анализа и прогноза вероятной преступной деятельности.

А.С. Овчинский учитывает и параметры рецидивности реальных объектов оперативно-розыскного учета. Это числовые значения вероятности совершения ими преступлений, которые отражают широкий спектр факторов (предикторов), которые, по мнению экспертов-практиков либо по данным криминологических исследований, свидетельствуют о криминальном потенциале личности. Среди таких предикторов могут быть неблагополучная семья в детстве, алкоголизм родителей, исключение из школы за хулиганство, употребление наркотиков, жестокое обращение с животными, проявления агрессивности в отношениях с товарищами, вспышки ревности, стремление к «красивой жизни» и т.д. Если сформировать шкалы криминальных предикторов и наборы параметров рецидивности с определенными числовыми значениями, то открывается возможность вычисления коэффициентов криминальности лиц, состоящих на оперативном учете или попадающих в поле зрения правоохранительных органов. Значение коэффициента криминальности личности будет говорить об условной вероятности того, что от данного лица можно ожидать совершения преступления [8, с. 62].

Мы считаем, что при всей привлекательности «цифровизации» степени общественной опасности подучетного контингента, предлагаемый А.С. Овчинским схема имеет «слабое звено», которое может нивелировать ее эффект. По его задумке, выработку искомых факторов (предикторов) предполагается поручить экспертам-практикам или получать из результатов

криминологических исследований. Основная проблема такого подхода – фактор их субъективности, что может обесценить прогнозные оценки.

Нам кажется, для реализации замысла А.С. Овчинского необходимы иные, более объективные инструменты прогностической деятельности, о которых будет сказано ниже.

Возможные сложности на этом пути показал В. Плэтт. Он отмечает, что при оценке вероятности возникновения в будущем какого-нибудь явления следует различать несколько неодинаковых ситуаций. Может, например, сложиться такая ситуация, когда при выпадении одного звена из всей цепи обстоятельств данное предсказываемое событие не может иметь места. Многие прогнозы в информации имеют аналогичный характер. Могут возникнуть сотни препятствий, каждое из которых полностью нарушит предсказанный ход развития событий. В данном случае какое-либо непредвиденное обстоятельство не может сделать осуществление высказанных предположений более вероятным. Все непредвиденные факторы оказывают только отрицательное влияние. Успешным прогнозом можно назвать тот максимально точный прогноз, который позволили сделать имеющиеся данные и методы информационной работы, который был сделан своевременно и оказал существенную помощь тому, для кого он в первую очередь предназначался. По мнению В. Плэтта, основные условия успешного прогноза в информационной работе разведки определяются несколькими факторами:

– полнота, достоверность и точность сведений и обоснованность предположений;

– компетентность в области используемых естественных и общественных наук;

– знание национального характера изучаемого народа: каков характер народа, его культура, в какой мере он прогрессивен, какова его воля;

– творческие способности. Зрелость суждений. Образование, опыт и дисциплинированное воображение. Способность зрело судить, обладать (если возможно) мудростью [69].

Попробуем адаптировать указанные В. Плэттом факторы применительно к ОРД.

Фактор 1. Полнота, достоверность и точность сведений и обоснованность предположений.

Как и в разведывательной деятельности, в работе оперативных подразделений ОВД это фактор является отправным. Невозможно сделать надежный прогноз на информации, полнота, достоверность и точность которой внушают сомнения. Соответственно, эти сведения должны быть тщательно проверены, начиная с этапа получения первичных данных и заканчивая подготовкой к составлению прогноза. Вместе с тем аналитик редко делает его в обстановке полной информационной ясности. Как правило, каких-то фрагментов информации не хватает, а какие-то сведения выглядят недостаточно точными. В такой ситуации аналитик может опираться на них, с оговоркой о степени их полноты и точности.

Единственный фактор, на который он не может полагаться – это недостаточная достоверность данных. Их категорически нельзя включать в содержание прогноза.

Для наглядности рассмотрим следующий пример. В оперативное подразделение поступила информация о преступной группе, причастной к совершению ряда квартирных краж. Полный состав группы не установлен, как и способы совершения преступлений. Очевидно, что данные о ней не полные и не точные. Однако здесь можно делать обоснованный прогноз о том, что криминальная деятельность, скорее всего, будет продолжена. Соответственно, путем установления плотного наблюдения за известными членами группы можно получить недостающую информацию и задержать фигурантов, желательно с поличным.

Однако, если первоначальная информация не достоверная, то все последующие меры окажутся бессмысленной тратой времени и ресурсов.

Фактор 2. Компетентность в области используемых естественных и общественных наук.

Современная криминогенная обстановка на всех уровнях (район-город-область-республика) предъявляет к оперативным работникам повышенные требования к их компетенции. Если раньше было достаточно быть только квалифицированным юристом, то теперь нужны знания в ряде смежных областей. Самая опасная современная угроза общественной безопасности – протестные настроения – могут возникнуть, развиваться и обостряться на различной почве: религиозной (деструктивные течения), политической (электоральные процессы), геополитической (дестабилизация ситуации в регионе), экономической (повышение цен), социальной (многодетные матери, владельцы автомашин с иностранной регистрацией) и т.д.

Здесь от сотрудника оперативного подразделения ОВД требуется овладение новыми непривычными компетенциями, а от аналитика – их углубленное знание для обработки всей этой информацией.

Фактор 3. Национальный характер народа.

Данный фактор остается неизменно важным как для разведывательной деятельности, так и для ОРД. Но если для первой он интересен с позиции оценки военного потенциала государства, то для оперативных подразделений ОВД характеристики этнического состава населения актуальны с точки зрения межнациональных отношений, которые тоже могут стать почвой для протестных настроений, ведущих к столкновениям [64, с. 3-140]. К сожалению, ряд таких общеизвестных негативных проявлений с человеческими жертвами и пострадавшими имели место в недавнем прошлом, как например, в Кордайском районе Жамбылской области в феврале 2020 года.

Более локальным фокусом этого фактора является оценка внутренней характеристики преступных групп – личные качества их лидеров и активных членов, отношения между ними, а также с другими криминальными формированиями, наличие коррупционных связей в органах власти, механизмы и схемы получения преступных доходов, их легализации и т.д.

Как характер этносов на определенной территории, так и внутреннюю характеристику участников преступных групп трудно (если вообще возможно) выразить с помощью цифр, как выше предлагает А.С. Овчинский. Поэтому анализ данного фактора и основанный на нем прогноз – чистый продукт мыслительной деятельности аналитика, то есть информация, помноженная на его способность делать из нее определенные выводы.

Фактор 4. Творческие способности. Зрелость суждений.

Как отмечает В. Плэтт, эти качества позволяют свести все добытые многочисленные, но разрозненные данные, а также принципы предвидения и познания в области естественных и общественных наук в единое осмысленное целое, отражающее причинно-следственные связи между этими отдельными элементами знаний. Зрелость суждений помогает отобрать из множества факторов главные, решающие. Эти способности слагаются из трех элементов знания и личных качеств, которые приобретаются в различное время и различными способами. Во-первых, это знания в области тех естественных и общественных наук, с использованием которых в первую очередь связана работа над составлением прогноза. Знания этого рода приобретаются в процессе обучения в школе и высших учебных заведениях. Во-вторых, это знание методов информационной работы и знание изучаемого района. Эти знания приобретаются преимущественно в процессе информационной работы. В-третьих, это зрелость суждений и проницательность ума. Эти качества – для многих результат многолетнего опыта работы, глубоких раздумий и творческих споров [69].

Немаловажную роль в этом должна играть так называемая оперативная интуиция [70]. Вместе с тем ни в одном изученном деле оперативного учета она не прослеживалась, что свидетельствует о формальном подходе со стороны оперативных работников.

В. Плэтт точно описал тот образ разведчика-аналитика, который полностью подходит и для аналитика в сфере ОРД ОВД, за исключением одного немаловажного обстоятельства. В те времена, когда он создавал свои труды (1950-1960-е годы), темп жизни общества и государства был кардинально иной. Тогда можно было позволить будущему аналитику долгие годы нарабатывать зрелость суждений и проницательность ума.

Сейчас такой возможности уже нет. Поэтому, учитывая вышеуказанные факторы, необходимо переходить к проактивной (опережающей) модели аналитической деятельности оперативных подразделений ОВД за счет новых информационных технологий, что позволит кратно сократить этот срок.

Видимо, вставшие перед аналогичной проблемой россияне пошли по этому пути. Там еще в 2021 году, в рамках совершенствования системы информационного обеспечения МВД России, был сделан упор на развитие и внедрение следующих технологий:

1) искусственного интеллекта (ИИ)на основе нейросетей;

2) большие данные (Big Data) [71].

Внедрение столь перспективных информационных технологий открывает широкие возможности как для ОВД в целом, так и для

оперативных подразделений. Их применение может принципиально изменить существующие подходы к аналитической работе, прежде всего с точки зрения прогнозирования процессов в криминальной среде.

Что из себя представляют эти технологии?

Нейросети являются основным направлением по изучению возможности моделирования естественного интеллекта с помощью алгоритмов. ИИ – проблемная область исследований по моделированию человеческого интеллекта, поведения и выполнения творческих функций, которые считаются особенностями человека, с помощью вычислительных устройств. Одно из определений интеллекта, совокупности для человека и машины, можно сформулировать так: интеллект – способность системы создавать в ходе самообучения программы в первую очередь для решения задач определённого класса сложности и решать эти задачи [72].

История ИИ как нового научного направления начинается во второй половине XX века. Были созданы и сформулированы много идей и постулатов к его зарождению. В философии давно шли споры о природе человека, процессе познания мира. Отношение философии к искусственному интеллекту можно наглядно видеть в работах британского философа, ученого Алана Тьюринга, который задал вопрос «могут ли машины делать, что мы (как мыслящие существа) можем делать?» Еще в 1940-х Тьюринг в числе первых начал изучать проблемы первых «умных машин», или как их называют сейчас - ИИ. В настоящее время ИИ, создаваемый с помощью нейронных сетей, является одним из важных факторов, способствующих получению информации, их быстрому распространению и качественной обработке. Применение ИИ в различных сферах человеческой деятельности играет большую роль, так как охватывает все сферы деятельности человека, начиная с начального образования и заканчивая изучением новейших технологий, изучением новых видов материи, неизвестных пока человечеству [72, с. 15-16].

Если максимально упростить, то нейросеть – это компьютерная программа, работающая по тем же принципам, что и человеческий мозг. Нейроны этого «мозга» представляют собой вычислительные элементы, созданные по образу биологических. Если обычная программа ограничена набором заложенных разработчиком функций, то нейросеть может обучаться, причем иногда самостоятельно – как ребенок, получающий новые знания [73].

Для чего все это делалось? Кратко – для совершенствования машинного обучения. Нейросети используют для анализа гигантских массивов данных, прогнозирования, сопоставления и классификации информации в самых разных сферах: от экономики до астронавтики. Один из самых наглядных примеров работы нейросети с данными – обработка текста. Если загрузить в нее несколько десятков, а то и сотен, произведений одного автора, то со временем она научится составлять текст в том же стиле или сможет создать свое собственное произведение. То же применимо и к обработке изображений: получив «образцы» в стиле конкретного художника,

нейронная сеть создает копии на основе его работ. А обрабатывая большие массивы данных, нейросети учатся заглядывать в будущее, выстраивая различные прогностические модели и почти предсказывая события [73].

Видимо, учитывая все возрастающие перспективы использования ИИ на основе нейросетей в различных областях, в Казахстане началась активная проработка вопросов их внедрения. Так, в 2021 году в Закон Республики Казахстан «Об информатизации» были внесены соответствующие нормы, легализующие эти новые технологии.

В статью 1 «Основные понятия, используемые в настоящем Законе» добавлены следующие пункты:

«54) национальная платформа искусственного интеллекта – технологическая платформа, предназначенная для сбора, обработки, хранения и распространения наборов данных и предоставления услуг в области искусственного интеллекта;

55) оператор национальной платформы искусственного интеллекта - юридическое лицо, определяемое Правительством Республики Казахстан, на которое возложено обеспечение развития и функционирования закрепленной за ним Национальной платформы искусственного интеллекта» [74].

На этом фоне в Законе не забыты полномочия уполномоченных органов в сфере внедрения ИИ.

Добавлена статья 13-2 «Компетенция оператора национальной платформы искусственного интеллекта», куда включено:

«1) обеспечение функционирования национальной платформы искусственного интеллекта;

2) сопровождение и системно-техническое обслуживание национальной платформы искусственного интеллекта;

3) предоставление услуг в области искусственного интеллекта на базе национальной платформы искусственного интеллекта;

4) сбор, хранение, обработка и распространение данных из открытых источников, данных, представленных оператором информационно-коммуникационной инфраструктуры «электронного правительства», а также собственниками и владельцами объектов информатизации;

5) осуществление иных функций в соответствии с законодательством Республики Казахстан» [74].

Кроме того, определен планируемый оператор казахстанской национальной платформы искусственного интеллекта – «Фонд поддержки исследований и разработок в сфере искусственного интеллекта» [75].

Базовая правовая рамка для применения ИИ в Республике Казахстан к настоящему времени сформирована. Законом Республики Казахстан от 17 ноября 2025 года № 230-VIII «Об искусственном интеллекте» впервые на уровне специального закона закреплены понятийный аппарат, принципы функционирования систем ИИ (безопасность, прозрачность, ответственность и подконтрольность), классификация систем ИИ по степени их воздействия на права граждан, а также основы функционирования национальной платформы ИИ. Системы ИИ определены как объект информатизации, а сам

ИИ - как инструмент достижения человеком определённых задач [76]. Цифровой кодекс Республики Казахстан от 9 января 2026 года № 255-VIII, вступающий в силу в июле 2026 года, дополнительно закрепляет правовой режим цифровых объектов, в числе которых - программное обеспечение, составляющее технологическую основу систем ИИ [77].

Вместе с тем принятие общего законодательства об ИИ не устраняет специального правового пробела в сфере ОРД. Закон «Об искусственном интеллекте» регулирует отношения, связанные с созданием и эксплуатацией систем ИИ в целом, не затрагивая порядок их применения в оперативно-розыскной деятельности. Закон РК «Об оперативно-розыскной деятельности» 1994 года также не содержит норм, регламентирующих использование технологий ИИ и нейросетей при проведении ОРМ. Таким образом, общая правовая база для ИИ создана, тогда как ведомственное правовое обеспечение его применения в ОРД ОВД остаётся задачей, требующей решения.

В рамках этих планов необходимо укреплять цифровую инфраструктуру, прежде всего нарастить вычислительные мощности. С этой целью в течение 2024-2025 годов предполагается обеспечить строительство дата-центров, специализирующихся на ИИ [4].

Анализируя создаваемую нормативную базу ИИ и декларируемые планы, возникает еще один аспект, который, вероятно, должен решиться в дальнейшем: в программных документах предполагается использование ИИ в интересах государства. Каким образом будут в этой схеме учтены интересы частных лиц, субъектов бизнеса и других негосударственных формирований, каков будет порядок их доступа к национальной платформе?

Это принципиально важно, так как любые технологии имеют свою оборотную сторону.

По мнению Главы государства, в ближайшие десятилетия мы, вероятно, приблизимся к моменту, когда машина превзойдет разум человека. Другими словами, может возникнуть опасность для человечества со стороны искусственного интеллекта. В научных кругах нет единого мнения, к чему это приведет: к процветанию человечества или угрозе его уничтожения. Поэтому особенно важен разумный контроль над искусственным интеллектом. К примеру, в прошлом наряду с атомной энергетикой было создано и атомное оружие. Это привело к необходимости выстраивания новой парадигмы глобальной безопасности. Это означает, что требуется найти «золотую середину» между технологическим прогрессом и коллективной безопасностью [4].

Очевидно, что в этой «золотой середине» необходимо найти свое место и ОВД, иначе правоохранительные органы рискуют кардинально отстать от динамичного развития современной преступности.

Так, уже входит в криминальный оборот технология deepfake, когда осуществляется реалистичная подмена фото-, аудио- и видеоматериалов, созданная с помощью нейросетей [78].

В недалеком будущем мошенничества и иные преступления, совершенные с применением этой технологии, могут распространиться в казахстанском сегменте Интернета. Чтобы быть готовыми к этому, необходимо в проактивном (упреждающем) режиме осваивать данную технологию, чтобы создавать адекватные методы противодействия.

Как отмечено выше, основная особенность ИИ на основе нейросетей заключается в том, что он изучает методы построения алгоритмов, способных самостоятельно обучаться. Это особенно необходимо, если не существует четкого решения какой-либо задачи. В этом случае проще не искать правильное решение, а создать механизм, который сам придумает метод для его поиска [79].

Сфера ОРД ОВД и, в частности, оперативно-розыскное прогнозирование представляет собой именно такую область, где готовых решений в подавляющем большинстве случаев не существует, а степень неопределённости высока.

К тому же для нейросети на основе ИИ не требуется долгое и сложное обучение, в отличие от традиционной подготовки аналитика, на которую обычно уходят годы.

Еще одна современная технология, в дополнение к ИИ на основе нейросетей, имеет далеко идущие перспективы для проактивного оперативно-розыскного прогнозирования криминогенной обстановки. Речь идет о технологии больших данных (BigData), которая является логичным продолжением программ анализа данных на основе семантических (смысловых) поисковых алгоритмов, которые начинают внедряться в деятельность служб ОВД.

Технология больших данных основана прежде всего на методах статистического и интеллектуального анализа данных, применяемых на огромных, постоянно пополняемых, массивах данных. Эти технологии позволяют:

– проводить самые различные и сколь угодно подробные классификации той или иной совокупности людей, компаний, иных объектов по самым разнообразным признакам. Такие классификации обеспечивают точное понимание взаимосвязи тех или иных характеристик любого объекта – от человека до компании или организации, с теми или иными его действиями;

– осуществлять многомерный статистический математический анализ. Этот анализ позволяет находить корреляции между самыми различными параметрами, характеристиками, событиями и т.п. Корреляции не отвечают на вопрос – почему. Они показывают вероятность, с которой при изменении одного фактора изменяется и другой. В каком-то смысле большие данные представляют собой альтернативный традиционной науке метод познания действительности. Теоретические модели отвечают на вопрос – почему, а затем, выявив причинно-следственные закономерности, позволяют формировать рекомендации о порядке действий. В случае выявления корреляционных закономерностей в больших данных стадия выявления

первопричины отсутствует, а сразу выявляется закономерная связь различных факторов. При этом, если факторы тесно взаимосвязаны, на один из факторов возможно осуществить воздействие для достижения целенаправленного изменения связанного с ним фактора;

– прогнозировать. На основе классификаций и аналитических выкладок осуществляется прогнозирование, суть которого состоит в том, чтобы на основе выявленной корреляционной связи факторов определить наиболее целесообразный способ воздействия для того, чтобы один набор факторов, характеризующих тот или иной объект, лицо, компанию, событие и т.п., был преобразован в другой [80, 81].

Технология больших данных в связке с ИИ на основе нейросетей способна решить извечную проблему, о которой упоминал В. Плэтт – кардинально сократить объем человеческих ресурсов для выработки качественных аналитических продуктов. Естественно, что любые информационные технологии в обозримом будущем не заменят человека полностью, подготовленный аналитик останется конечной инстанцией, доводящей аналитический документ до финальной готовности.

Роль этих технологий заключается в осуществлении «черновой» подготовительной работы по сбору, обобщению и систематизации всей необходимой информации. Именно на эти процессы уходит львиная доля времени работы аналитиков.

Учитывая подобные перспективы, большие данные как прорывная информационная технология были осознаны такими странами, как США, Великобритания и Япония. Еще в 2012 году администрация Б. Обамы выступила с инициативой «Big Data Research and Development Initiative». Этой инициативой предусматриваются вложение значительных объемов ресурсов и проведение комплексных мероприятий в целях активного использования технологий больших данных в интересах ключевых направлений политики США. В 2013 году правительство Японии опубликовало информацию о разработке национальной программы по большим данным. Летом того же года правительство Австралии заявило, что рассматривает большие данные как важнейший национальный стратегический ресурс и выдвинуло задачу стать головной страной в сфере использования этих технологий как на правительственном уровне, так и на всех других уровнях государственного аппарата в масштабах Британского содружества [80, с. 221].

Казахстан отстает от передовых тенденций в информационных технологиях более чем на десять лет. В то же время в таком отставании, как ни странно, есть положительный аспект. За это время флагманы внедрения ИИ – западные страны – методом проб и ошибок наработали действенные методики его применения, что наглядно прослеживается в информационном поле на примере так называемых чат-ботов.

Чат-бот и искусственный интеллект – два понятия, которые претендуют на то, чтобы стать технологическими символами последних лет. ChatGPT, Bing, Bard, GitHub, Copilot, GigaChat, JasperChat, Rytr, YouChat, Socratic,

Chatsonic, Anyword, CharacterAI – это только наиболее известные из них, и их количество продолжает увеличиваться в геометрической прогрессии. Согласно статистике, чат-боты активно используют 1,4 млрд. человек, а более 50% сервисных компаний по всему миру применяют этот полезный инструмент для постпродажного обслуживания клиентов. Неудивительно, что эти высокотехнологичные инструменты стремительно развиваются и проникают во все новые сферы науки, экономики и быта [80].

На этом фоне приходится констатировать, что в Казахстане в сфере правоохранительной деятельности в целом и ОРД ОВД в частности исследования в данном направлении если и ведутся, то в инициативном режиме и на основе энтузиазма отдельных специалистов. Какая-либо чёткая политика ведомства в этой области пока отсутствует.

Между тем, технология больших данных лучшим образом подходит для оперативно-розыскного прогнозирования.

Одним из направлений эффективного ее применения является прогноз развития социальных, политических, военных и экономических процессов. При этом к началу нулевых годов, до появления технологии больших данных, специалисты, ведущие исследования в этой сфере, сформулировали по меньшей мере три фундаментальных положения, из которых следовало, что:

– используя самые изощренные и эффективные методы, можно прогнозировать процессы, но не события;

– прогнозы с высокой степенью вероятности можно делать в отношении групп различной размерности, но не отдельных индивидуумов;

– знания о действиях групп и индивидуумов в одной ситуации не позволяют давать точные прогнозы о подобных действиях, осуществляемых в другой ситуации [80, с. 223].

Соответственно оказалось, что различного рода прогнозы, базирующиеся на традиционных выборках, построении сценариев, экстраполяции, не обладают высоким уровнем адекватности. Развитие Интернета дало возможность оперировать большими данными относительно человеческого поведения, намерений, желаний и т.п. Прогнозирование на их основе состоит в извлечении нетривиальных выводов из заранее известных характеристик, признаков и сведений об объектах. Использование больших данных из Интернета как огромного, пополняемого в режиме реального времени поведенческого архива для прогнозирования развивается по таким трем ключевым направлениям, как:

– прямой интеллектуальный анализ общедоступных данных, предоставляемых поисковыми системами и различного рода социальными сетями и платформами;

– создание рекомендательных систем, которые прогнозируют различного рода выбор субъектов и групп и на этой основе рекомендуют им что угодно – от книг до кандидатов в президенты;

– создание сложных прогностических систем, использующих разнородные данные, получаемые из открытой и закрытой части глобальной сети, обрабатываемые с помощью большинства известных методов

интеллектуального анализа данных [80, с. 224].

Таким образом, большие данные позволяют уменьшить (а, возможно, вообще устранить) проблемы при прогнозировании отдельных процессов и действий конкретных лиц. Очевидно, что такой подход коренным образом меняет парадигму той картины, что будущее всегда будет скрыто за непроницаемой пеленой.

Применительно к оперативно-розыскному прогнозированию это значит, что построенная на преимущественно субъективных основаниях оценка аналитика обретает под собой объективную почву, обусловленную алгоритмами технологии больших данных.

Так, С.И. Макаренко и М.С. Иванов в качестве одного из наиболее ярких примеров успешного создания средства разведки как сложной прогнозной системы приводят проект Recorded Future. В январе 2010 г. он был запущен при поддержке инвестиций компании Google и инвестиционного фонда американского разведывательного сообщества In-Q-Tel. Таким образом, большие данные обеспечили появление новых, на порядки более эффективных, чем раньше, методов прогнозирования научно-технических, инженерно-технологических, инвестиционных, политических, социальных и военных процессов. Эти методы в совокупности с методиками глубокого анализа на основе все тех же больших данных позволяют говорить о создании принципиально нового вида информационного оружия, а именно – прогностических средств. Этот вид оружия может быть использован как обеспечивающий механизм для разработки и применения традиционных вооружений [83].

Применение этих информационных технологий стало логичным продолжением теоретических подходов прогнозирования в сфере разведывательной деятельности, о которых в середине прошлого века говорил известный теоретик в области стратегической разведки В. Плэтт как о разведывательных оценках в отношении будущего, применяя термин «предвидение».

Он настаивал, что предвидение в информационной работе стратегической разведки имеет жизненно важное значение для национальной безопасности, в связи с чем необходимо конструктивно и критически изучать методики предвидения в информационной работе [69].

При этом особенностью новых информационных технологий является то, что они могут находить ту информацию, которая в явном виде имеется в документах, размещенных в сети Интернет, а уже потом, за счет анализа различных документов с совпадающим целевым контентом, начинают собирать информационное наполнение запроса пользователей. Более интересным направлением развития средств разведки является анализ разнородных, изначально семантически не связанных между собой данных с целью выявления неслучайных совпадений или скрытых закономерностей и последующей их «привязкой» к объектам разведки. Такое направление получило развитие в рамках исследования проблемы больших данных [83, с. 578-579].

Более того, по мнению Е.С. Лариной и В.С. Овчинского, на этой основе можно определять наиболее важные факторы и вырабатывать оптимальные способы воздействия на них с целью изменения тенденции этих процессов [80, с. 257].

Конечно, целевое воздействие на объекты оперативного интереса – это, видимо, завтрашний или даже послезавтрашний день в аналитической работе оперативных подразделений ОВД РК. Тем не менее, ниже будет изложено наше видение этих методик в рамках проактивной модели ОРД.

Пока наиболее актуальным является адаптация технологий ИИ, нейросетей и больших данных к оперативно-розыскному прогнозированию. Как это видится на сегодняшний день?

Не секрет, что объем информации, поступающей к оперативному работнику, в настоящее время настолько велик, что он не успевает обрабатывать ее всю, а интуитивно выхватывает из нее лишь наиболее яркую (так называемую «цветную»). В то же время, менее заметные, но более перспективные сведения часто остаются без внимания, а позже оказываются «погребенными» под слоями поступающих новых данных. Эти «потерянные» возможности постоянно увеличиваются как в низовых подразделениях, так и по мере движения вверх – на уровне области (города республиканского значения) и всей страны. В будущем прогнозируется кратное увеличение объемов такой информации, обрабатывать которые без новых информационных технологий будет невозможно.

Об этой проблеме сказано в Концепции правовой политики Республики Казахстан до 2030 года. Поэтому нужно предпринимать меры, направленные на качественный сбор фактических данных в пределах каждого государственного органа. Общеизвестно, что государственными органами на постоянной основе формируются огромные массивы неструктурированной информации, что обуславливает необходимость закрепления в каждом органе специалиста, ответственного за их сбор и обработку [84].

Соответственно, у них должны быть специализированные инструменты для обработки информации, которыми могут стать ИИ на основе нейросетей и больших данных. Их применение видится на двух уровнях:

1. Использование специальных информационно-поисковых систем (ИПС) с семантическим анализом связей между отдельными фрагментами данных.
2. Использование технологии больших данных.

К сожалению, в настоящее время Казахстан находится в самом начале первого уровня – специальные ИПС имеются лишь на уровне МВД, и то лишь в некоторых службах в виде пилотных проектов. Остальным приходится осуществлять поиск необходимой информации в Интернете «по старинке» – сотрудник физически сидит за компьютером, вручную вводит нужные реквизиты и выбирает те сведения, которые он сочтет интересными в меру своего интеллекта и профессионального уровня [85].

«Эффективность» такого подхода демонстрирует следующий пример. Команда разработчиков из Технологического университета Сиднея

(Австралия) представила дронов для патрулирования пляжей. Основной задачей дронов является поиск акул в прибрежных водах и предупреждение людей на пляжах. Анализ видеоданных производят нейросети, что существенно отразилось на результатах: вероятность обнаружения и идентификации акул составляет до 90%, тогда как оператор, просматривающий видео с беспилотников, успешно распознает акул лишь в 20-30% случаев [79].

Поэтому задачей первого этапа – повсеместного использования ИПС – является масштабный сбор и обобщение всей информации (как оперативно-розыскной, так и иной), имеющей прямое и опосредованное (например, экономические или социологические данные) отношение к вероятным признакам криминальных событий.

С учетом этого в будущем, на втором уровне, схема использования ИИ на основе нейросетей для оперативно-розыскного прогнозирования представляется следующей. Для программы составляется исходный перечень наиболее важной опорной информации (в основном, оперативного характера). Соответственно, такой перечень будет различным для разных направлений работы. Например, по линии противодействия организованной преступности это могут быть:

– установочные данные (в том числе фото- и видеоматериалы) всего состоящего на учете контингента, их имущества, транспорта, телефонов, адреса почты, аккаунты социальных сетей и иная информация;

– аналогичные данные об их криминальных и родственных связях;

– известные источники их финансирования и получения («отмывания») преступных доходов;

– известные каналы взаимодействия с региональными и международными криминальными формированиями;

– известные типичные способы и методы совершения ими преступлений;

– материалы уголовных дел в отношении фигурантов, в которых зафиксированы методики формирования и фиксации доказательств преступной деятельности;

– имеющиеся практические рекомендации (с учетом опыта зарубежных стран) по наиболее юридически обоснованным методам фиксации доказательств организованной преступной деятельности.

Данный перечень не является исчерпывающим и может дополняться другими данными в зависимости от конкретной оперативной обстановки [85, с. 188].

Функция ИИ, как предполагается, будет заключаться в обработке таких сведений, их «усвоении» и постоянном пополнении за счет непрерывного мониторинга социальных сетей, средств массовой информации, а также дополнительных объемов оперативно-розыскной информации.

Уже на этом этапе ИИ способен дать значительный объём новых данных о фигурантах, их окружении, образе жизни и, возможно, о способах преступной деятельности. Но главные результаты ожидаются на следующем

этапе – самостоятельном машинном обучении, когда на базе накопленной информации будут формироваться рекомендуемые алгоритмы проведения ОРМ для документирования преступной деятельности подучетного контингента, в том числе вновь выявляемого.

Но и это может быть лишь промежуточной стадией. Подключение этого постоянно пополняемого объема информации к технологии больших данных даст возможность построения наиболее вероятных тенденций и направлений развития криминальной деятельности как по регионам, так и в целом по стране [85, с. 188].

Вместе с тем в существующих условиях недостаточной ресурсной обеспеченности отечественных ОВД предлагаемое внедрение ИИ придется проводить в несколько этапов. На первом этапе следует внедрить ее в пилотном режиме на уровне центрального аппарата МВД в подразделении, отвечающем за сбор, обработку и хранение всех имеющихся баз данных (Информационно-аналитический центр). После наработки практики и подготовки специалистов можно распространить систему на уровень областей (городов республиканского значения), а в дальнейшем – на городской (районный) уровень.

Понятно, что внедрение этих новых информационных технологий потребует значительного времени, усилий и ресурсов. В этой связи в текущих условиях промежуточным вариантом улучшения аналитической работы оперативных подразделений ОВД в прогностических целях является овладение навыками оперативно-тактического прогнозирования за счет повышения общего уровня аналитической подготовки сотрудников.

Следует учитывать, что указанный «ручной» режим прогнозирования относится к категории более вероятностного, нежели с применением новых технологий, и представляет собой разновидность предвидения, базирующегося на ранее собранной упорядоченной (систематизированной) информации, на знании закономерностей развития преступного поведения лиц, представляющих оперативный интерес, особенностей условий, в которых применяются методы ОРД, на оценке тактических возможностей оперативников и других участников ОРМ. На этом фоне приходится констатировать, что, несмотря на серьезный потенциал оперативно-тактического прогнозирования, оно не нашло четкого отражения в науке ОРД и практике отечественных оперативных подразделений ОВД РК, в отличие от России, где оно входит в учебные программы не только в ведомственных, но и в гражданских вузах юридической направленности [49, с. 24].

Даже современный бизнес, реализуемый в условиях жесткой конкуренции, давно имеет прогностическую основу. Научное прогнозирование уже давно стало атрибутом успешной предпринимательской и хозяйственной деятельности в высокоразвитых странах. Еще в большей мере потребность в прогнозировании ощущается в сфере деятельности ОВД. Оперативно-тактическое прогнозирование является результатом мышления оперативника, поиска им ответов на вопросы о том, как может измениться оперативная ситуация, как следует

действовать в ожидаемой ситуации; как поведет себя противоборствующая сторона. В оперативно-тактическом прогнозировании имеют значение не только установленные факты, но в большей мере теоретические положения, специальные знания, полученные оперативными сотрудниками благодаря профессиональной подготовке и опыту борьбы с преступностью. Логической основой для этого являются следующие категории познания:

– экстраполяция (распространение установленных в прошлом тенденций на будущий период времени);

– умозаключение по аналогии (перенесение знаний об изученных объектах, явлениях на вновь обнаруженные объекты и явления, схожие по существенным качествам и свойствам);

– моделирование (исследование изучаемых явлений и процессов путем построения схем) [86].

Например, метод экстраполяции можно применить при прогнозировании динамики так называемых кибермошенничеств. Еще лет десять назад они были распространены не так масштабно, как в настоящее время. Эта категория уголовных правонарушений сопутствует бурному развитию новых технологий, связанных с глобальной сетью Интернет. Выше уже упоминалось, что с появлением новых технологий, таких как deepfake, можно прогнозировать появление основанных на них способов кибермошенничеств и, не дожидаясь их роста, заранее вырабатывать методику их выявления, предупреждения, пресечения и раскрытия.

Примером умозаключения по аналогии может служить прогноз роста количества квартирных краж в новых домах, особенно строящихся в г. Астана, Алматы, Шымкенте и ряде других городов. Данная аналогия основывается на таком опыте по другим домам, где соседи не знают друг друга, система безопасности еще не подключена и под видом рабочих-ремонтников воры могут беспрепятственно проникать в квартиры.

Соответственно, для своевременного упреждения таких краж необходимо вести мониторинг сдаваемых в эксплуатацию жилых комплексов, заранее организовывать в районе их расположения оперативно-поисковые мероприятия с привлечением представителей компании-застройщика.

Метод моделирования, как правило, применяется для прогнозирования часто повторяющихся или серийных уголовных правонарушений, когда в результате анализа прошлых фактов криминальной деятельности имеется набор криминалистических характеристик способов, с помощью которых они совершены. При сопоставлении этих способов в различных сочетаниях появляется примерная модель действий, которые может производить преступник. Нагляднее всего метод моделирования проявляется при раскрытии серийных убийств и иных тяжких и особо тяжких преступлений, когда на основании имеющихся фактов и так называемого «профиля убийцы» прогнозируются возможные дальнейшие преступные действия.

В общей теории прогнозирования выделяют три вида прогнозов - интуитивный, гипотетический и теоретический. Интуитивный основывается

на интуиции, т.е. внезапном, часто безотчетном «озарении», которое, естественно, приходит из глубин жизненного и профессионального опыта [87].

Хотя считается, что интуиция не поддается алгоритмизации и моделированию, никакое «озарение» не рождается на ровном месте; это логическая цепочка умозаключений, которые и приводят к такому результату. Проблема в том, что после решения задачи эта цепочка, как правило, уже никого особо не интересует, хотя факты интуитивного раскрытия преступлений (в том числе прошлых лет) встречаются достаточно часто. Собрав и обобщив определенный их массив (достаточно нескольких десятков), можно составить примерную модель формирования искомой логической цепочки умозаключений. Затем на данной основе можно разработать методику для совершенствования оперативных работников-аналитиков [6, с. 164].

Гипотетический прогноз (от понятия «гипотеза») основывается на фактических данных, которыми располагает тот, кто ищет решения задачи.

Одним из наглядных примеров такого прогнозирования может служить ситуация после изъятия крупных партий наркотиков. Логично, что это создает их дефицит и, как следствие, резкий рост розничной цены. Отсюда можно делать прогноз, что через непродолжительное время вероятно увеличение количества корыстных и корыстно-насильственных преступлений со стороны наркозависимых лиц, которые будут искать дополнительные средства на приобретение наркотиков. Соответственно, оперативные подразделения должны заблаговременно принять меры реагирования (контроль подучетного контингента, оказание на них профилактического воздействия, наблюдение за каналами сбыта похищенного имущества и т.д.).

Теоретический прогноз основывается на специальных знаниях (теории), которые позволяют предвидеть вероятное развитие явлений [87].

Так, теория изучения организованной преступности говорит о том, что она всегда ищет сферы извлечения незаконной или теневой прибыли. С учетом этого можно с достаточной долей уверенности прогнозировать, что запуск новых крупных промышленных производств либо функционирование оптово-розничных центров (например, таких как рынок «Алтын Орда» в Алматы) предполагает активизацию криминала, прежде всего попытки взять их под свой контроль. Такой оперативно-тактический прогноз может лечь в основу последующих ОРМ [6, с. 167].

Если анализировать состояние такой работы на практике, то изучение дел оперативного учета показывает, что прогнозирование, если и осуществляется в очень редких случаях (около 5%), то ограничивается рамками отдельной преступной группы, без анализа ее взаимосвязей с другими криминальными формированиями, то есть на самом низком тактическом уровне.

В то же время все три вида рассматриваемых прогнозов могут применяться оперативными подразделениями как отдельно, так и в

комплексе, в зависимости от стоящих задач. Но основная проблема заключается в том, что оперативно-тактическое прогнозирование как важный элемент «проактивного» подхода в деятельности оперативных подразделений ОВД до настоящего времени своего развития не получил.

При этом, учитывая традиционную инерцию во внедрении вышеописанных новых информационных технологий, следует осваивать хотя бы сложившиеся методики оперативно-розыскного прогнозирования за счет аналитической деятельности, осуществляемой самими оперативными работниками.

В этой связи целесообразно выработать примерный алгоритм подобной прогностической работы для оперативных работников, выполняющих конкретные задачи оперативного обслуживания своих территорий. Он может включать следующие этапы:

1. Определение цели и задач прогноза. Цель – это получение аналитической картины процессов, которые интересуют подразделение на текущем этапе. Задачи – это необходимый набор действий, которые должны привести к цели. Например, общей задачей для любого оперативно-розыскного прогноза является сбор максимума информации об объектах оперативного интереса, их окружения и сопровождающих их процессах.

2. Анализ текущего состояния интересующих процессов. Изучение существующего положения является исходным пунктом для выработки прогноза. Чем детальнее известны подробности о текущем статусе фигурантов (установочные данные, образ жизни, вероятные схемы криминальной деятельности, используемый транспорт, связь, контакты и т.д.), тем полнее и достовернее будет прогноз.

3. Обзор общих факторов, относящихся ко всем анализируемым фактам. Как указывалось, выше, помимо чисто криминальной информации, важны сопутствующие или окружающие фигурантов условия в смежных сферах – экономике, социальной и политической плоскости, религии, геополитике и др. Каждый конкретный прогноз может потребовать изучение специфических областей, ранее не попадавших в поле зрения оперативных подразделений.

4. Исследование хронологии процессов, обусловивших сложившуюся ситуацию. Здесь важную роль играют архивные материалы, которые обычно не востребованы. Основная информация для этого содержится в делах оперативно-розыскного производства; кроме того, интересующая динамика может излагаться и в уголовных делах, даже если фигуранты проходили в них в качестве свидетелей.

Цель такой ретроспективы – мысленное (или графическое) построение диаграммы динамики анализируемых процессов – идут ли они по нарастающей или нисходящей все время, имеются ли чередующиеся стадии роста или падения (цикличность событий), каков их характер и амплитуда?

Это первая опорная точка, показывающая тренд развития ситуации, что должно учитываться в итоговом прогнозе.

5. Выявление факторов, облегчающих фигурантам их криминальную деятельность. Это могут быть коррупционные связи в правоохранительных органах, налаженная координация с другими преступными формированиями, применение сложных изощренных способов совершения преступлений (те же самые кибермошенничества с использованием новых технологий), специализация на экономических и финансовых правонарушениях и т.д.

6. Выявление факторов, затрудняющих фигурантам их криминальную деятельность: наличие конкурирующей противоборствующей группировки, ранее судимые и находящиеся под надзором члены группы, возрастающая степень оборудования объектов камерами видеонаблюдения, сужающиеся каналы сбыта похищенного имущества и др.

7. Сравнение анализируемой криминальной деятельности с аналогичными способами совершения преступлений другими группами, имевшими место в прошлом, либо в другом регионе. Идеального совпадения никогда не будет, но важно выявить общие условия из числа вышеуказанных, оказывающие воздействие на формирование таких способов.

8. Определение и подробное изучение аномалий в поведении или образе жизни лидера или участников анализируемой криминальной группы – чрезмерное злоупотребление наркотиками или спиртным, наличие неизлечимых заболеваний, неконтролируемая агрессия, жестокость к близким и родным, склонность к неоправданному риску и т.д.

9. Финальный этап – сведение воедино результатов всех предыдущих этапов и оценка их во взаимосвязи. На данном этапе важным является оценка точности сводимых фрагментов анализа и указание на это в итоговом материале, содержащем прогноз вероятного развития анализируемой ситуации.

Предложенный алгоритм отнюдь не является исчерпывающим, а лишь примерным и может дополняться в процессе практической аналитической работы.

Вместе с тем данный алгоритм – лишь инструментарий, который даст нужный эффект только в руках вдумчивого оперативного работника, склонного к творческому подходу в аналитической работе.

В связи с отсутствием альтернативных вариантов изложенные методики оперативно-розыскного прогнозирования необходимо внедрять в деятельность оперативных подразделений ОВД РК. Такая работа может проходить в несколько этапов:

1) определение в каждом оперативном подразделении наиболее подготовленных сотрудников, имеющих достаточный опыт по своему направлению: общеуголовная или организованная преступность, наркобизнес, религиозный экстремизм, деструктивная деятельность и др.;

2) их обучение методам сбора и обработки информации на специализированных курсах в ведомственных вузах или в гражданских организациях, занимающихся анализом больших объемов данных;

3) внедрение полученных знаний в непосредственную деятельность оперативных подразделений, когда подготовленные подобным образом аналитики обучают всех остальных сотрудников.

Такое соединение теоретических знаний с практической составляющей позволит создать понятные алгоритмы осуществления аналитической работы с выходом на оперативно-тактическое прогнозирование [6, с. 166].

Таким образом, оперативно-розыскное прогнозирование может быть поставлено на серьезную научную основу и стать значимым проактивным элементом государственной политики противодействия преступности.

В целом, завершая рассмотрение теоретических, организационных и правовых аспектов оперативно-розыскного прогнозирования как информационной основы проактивного подхода к осуществлению ОРМ, можно сделать следующие выводы:

1. Оперативно-розыскное прогнозирование как актуальное и в то же время не изученное направление работы оперативных подразделений ОВД требует дополнительного научного исследования с целью выработки проактивных методик, применимых в практической деятельности.
2. Для этого уже сейчас необходимы срочные меры по внедрению в системе ОВД новых информационных технологий, основанных на ИИ, нейросетях и больших данных, чтобы в упреждающем режиме противодействовать распространению уголовных правонарушений, совершаемых с применением аналогичных технологий.
3. Дополнением к технологическому оснащению системы ОВД должны стать оптимальные организационные меры, также построенные на проактивном подходе.

Их рассмотрению посвящен следующий подраздел настоящего исследования.

§ 2.2 Сетецентризм как организационная основа проактивного подхода

Анализ тенденций развития современной криминогенной ситуации как в Казахстане, так и в других странах показывает ее кардинальную трансформацию и уход от традиционных методов преступной деятельности к более сложным и глобальным трендам. Нагляднее всего они проявились в ходе январских событий 2022 года.

Как известно, террористические атаки включали в себя целый ряд различных аспектов: военный, политический, идеологический, дезинформационный и прочие. Причем это была ярко выраженная внешняя агрессия со стороны международного терроризма [34].

Очевидно, что в настоящее время угрозы и вызовы становятся качественно другими. Наряду с традиционными протестными группами, в этих событиях участвовали представители уголовно-преступной среды и религиозных экстремистских движений. Внезапность осуществленных ими

террористических актов во многом обусловлена тем, что они имеют сложную структуру, которая трудна для выявления правоохранительными органами. Для эффективного противодействия подобным проявлениям необходимо изменить подходы, взяв за аналогию методы, применяемые в сфере военного дела, а именно принципы сетецентрических войн.

Такой подход основан на выявлении стратегических «центров тяжести» противника с целью оказания на них силового или информационно-психологического воздействия.

В сфере правоохранительной деятельности в качестве противника воспринимается преступность в широком смысле этого понятия, которая в последнее время структурно и качественно меняется.

Например, если анализировать ее с точки зрения экстремистских и террористических угроз, то налицо кардинальные изменения всего за несколько лет. Если в известных событиях 2011, 2013 и 2016 годов было явно видно, что эти акции носят чисто экстремистский и террористический характер, то январские проявления 2022 года показали «гибридный» характер, выразившийся в неоднородности участвовавшего в них контингента [88].

После этих событий высказывается множество мнений относительно реальных истоков и причин произошедшего. Сама данная проблема многоаспектна и содержит целый ряд факторов.

Одним из таких признаков является изменение иерархической структуры высокоорганизованных криминальных формирований.

Так, общеизвестно, что транснациональные преступные организации основное внимание обращают на минимизацию риска и обеспечение безопасности. Способность адаптироваться и приспосабливаемость к обстоятельствам делают их неуязвимыми для правоохранительных органов [89].

Для этого они выработали так называемую сетевую структуру, которая представляет собой децентрализованную совокупность отдельных и относительно независимых звеньев, контактирующих друг с другом по мере необходимости (например, при распределении контролируемой территории).

Соответственно, чтобы успешно противодействовать подобным угрозам, необходимо понимать, какие наиболее характерные признаки им присущи.

К ним можно отнести следующие:

– наличие единой стратегической цели и отсутствие четкого планирования на тактическом уровне;

– отсутствие четкой иерархической структуры подчиненности, а зачастую и отсутствие центрального руководства;

– децентрализация и параллельность работы представителей организаций, затрудняющие контроль над их деятельностью, в том числе со стороны государственных и правоохранительных органов;

– многоуровневая структура с разветвленной и сложной системой связей и вложенных сообществ;

– координация своей деятельности с использованием средств глобальных информационных сетей;

– высокая динамика развития за счет хорошо налаженного обмена информацией и способности к быстрой реорганизации в случае необходимости [90].

Это новые тренды в построении известных преступных сообществ мира – итало-американской мафии, китайских «триад», японских «якудза» и других, менее известных формирований. В определенном смысле, пример – сообщество так называемых российских «воров в законе».

Более того, сетевые структуры получают все более широкое распространение и в других сферах.

По мнению российских специалистов, общество сейчас переживает распространение сетевой организационной культуры, которая по эффективности стоит выше нынешней, иерархической. Если иерархия основана на централизации, вертикальной субординации, штатном расписании и постановке формальных целей, то сетевая организация – на относительной автономии частей, аутсорсинге и распределении рисков. Даже если один кластер сети разрушен, остальные могут продолжать эффективно функционировать. Применительно к террористическим организациям это означает, что арест даже большой группы террористов может не затронуть работоспособности всей террористической сети [91].

Этот вывод очень важен для деятельности правоохранительной системы. Согласно ему, привлечение к уголовной ответственности какой-либо преступной группы даже в полном составе не дает гарантии того, что криминальная деятельность не продолжится другими элементами сети. Возможно, на некоторое время она замедляется или приостанавливается, но затем возобновляется без критического ущерба.

Вместе с тем понимание этого отсутствует у подавляющего большинства (более 80 %) опрошенных сотрудников оперативных подразделений ОВД, которые уверены, что привлечение к ответственности руководителей преступных групп ведет к полному прекращению их преступной деятельности.

Кроме того, в условиях сетевой организации роль ее отдельных элементов, способных действовать самостоятельно, кардинально меняется. Нейтрализация руководящего звена этих частей часто также не дает эффекта их разобщения. Соответственно, здесь необходим системный подход, охватывающий как структуру в целом, так и ее отдельные элементы, в том числе выполняющие вспомогательные функции – экономическая база, рекрутинг новых членов, поддержание связи с другими элементами сети и другие.

Очевидно, что действующая модель работы оперативных подразделений ОВД не охватывает (или почти не охватывает) эти элементы. Получается, что усилия государства по противодействию преступности зачастую носят поверхностный характер, не затрагивая элементов, обеспечивающих ее беспрепятственное последующее воспроизводство. Основная причина такой

ситуации состоит в том, что указанной сетевой структуре государство противопоставляет традиционную иерархическую модель, которая в существующих условиях является излишне жесткой, негибкой и, следовательно, не эффективной [92].

Наиболее наглядно тенденции перехода на сетевую структуру демонстрируют многочисленные террористические организации на Ближнем Востоке. Аналитические исследования показывают, что в организации террористического акта могут быть задействованы десятки и сотни человек. Одни принимают решения, другие находят источники финансирования, третьи выбирают цели, четвертые разведывают объекты и маршруты, пятые вербуют исполнителей, шестые осуществляют их психологическую подготовку, седьмые проводят обучение и инструктаж, восьмые и девятые изготавливают и подвозят «пояса шахидов», десятые доставляют исполнителей в нужные места и т.д. вплоть до реализации теракта [8, с. 75-76].

По аналогичной схеме действовали террористические организации в Казахстане, когда в начале–2середине 2010-х годов по стране прокатилась волна терактов, совершённых смертниками [93].

Как правило, в результате расследования уголовных дел, начатых по таким фактам, многие подготавливавшие и обеспечивавшие их звенья террористических сетей остаются не установленными.

Например, за несколько дней до совершения самоподрыва смертника в г. Атырау в октябре 2011 года в Интернете появился видеоролик, на котором четверо членов небезызвестной террористической группы «Джунд аль-Халифат» в масках требовали от властей отменить принятый новый закон о религии, ужесточавший ответственность за причастность к террористической деятельности [94].

Кто эти люди, где они находились, кем снабжаются, являются ли они частью более крупной организации, каковы их конечные цели? Эти и многие другие важные вопросы остаются без ответа, так как действующая правоохранительная система не ориентирована на эффективное противодействие сетевым структурам.

Соответственно, их форма позволяет им быстро адаптироваться к изменяющимся внешним условиям. И теперь, по мнению В.Р. Григорьева и Л.О. Шуркина, придется также перенимать сетевые правила игры. Чтобы попытаться победить врага на его же поле, необходима децентрализация и автономия объединенных общей целью мобильных адаптивных структур наряду с привычными вертикальными командными линиями [91, с. 67-99].

Анализ концепции сетецентрической войны показывает, что ее основная идея лежит не в новых формах и способах ведения боевых действий, а в изменении принципов управления войсками и оружием. Точнее говоря, это новый способ организации управления как реальный инструмент повышения боевых возможностей разнородных сил и средств за счет синергетического эффекта. При иерархической системе управления в ходе взаимодействия между двумя одноранговыми элементами в работу включается вся

иерархическая цепочка, вплоть до общего для обоих элементов лица, принимающего решение. Сетевая организация допускает непосредственное взаимодействие двух одноранговых элементов. В этом случае потенциальная эффективность сети линейно увеличивается с ростом числа ее элементов и экспоненциально – с ростом числа связей между ними (пропорционально квадрату их числа). Однако при внедрении сетевой системы управления иерархическая структура не упраздняется, а добавляются новые связи между одноранговыми элементами. Эти связи призваны повысить скорость циркуляции информации внутри системы, но не заменить собой существующую иерархическую систему управления [83, с. 294-295].

Логично, что в таких условиях все более или менее организованные криминальные структуры переносят и будут далее организовывать деятельность своих формирований по сетевому принципу. Можно прогнозировать, что в недалеком будущем традиционные преступные группы, которые можно наблюдать сейчас, станут редкостью, а со временем, вероятно, исчезнут вовсе. Это отражение естественного процесса развития криминальной среды. Подобным образом, исчезли стихийные группы так называемых «рэкетиров», которые повсеместно «крышевали» торговые точки в 1990-х годах на заре зарождения рыночной экономики. Последующее ее развитие обусловило «отмирание» указанных примитивных форм и переход криминала к более высокоорганизованной деятельности. В настоящее время происходит очередной этап ее трансформации в сетевые структуры, что относится ко всем линиям – организованная и наркопреступность, экстремизм и терроризм, киберпреступность и т.д.

На этом фоне подавляющее большинство опрошенных сотрудников (свыше 90%) оперативных подразделений ОВД не знают, что означает сетевой характер современной преступности .

Учитывая изложенное, возникает необходимость проактивного (упреждающего) поиска более адекватных и эффективных подходов организации работы правоохранительных органов, прежде всего оперативных подразделений ОВД. В этом смысле целесообразно обратиться к сфере военного дела, которое в последнее время по понятным геополитическим причинам развивается бурными темпами, значительно обгоняя другие области.

Прежде всего, представляют исключительный интерес принципы ведения вышеупомянутых сетецентрических войн, которые, по всей видимости, стали организационной основой всех современных боевых технологий.

Термин «сетецентризм» впервые появился в американской компьютерной литературе как термин для объединения отдельных электронных вычислительных машин в единую сеть. Позднее идея сетецентризма была взята на вооружение армией США. Принцип сетецентрического управления был позаимствован из сферы бизнеса, в частности, из организации предпринимательской деятельности компании розничной торговли Walmart. Авторы концепции сетецентрической войны

рассматривали эту компанию как самосинхронизирующуюся, саморегулируемую, рассредоточенную сеть магазинов, располагающую сведениями о происходящем движении товаров и торговых операциях в реальном масштабе времени. При этом управление движением товаров в компании осуществлялось по горизонтальной информационной сети, а не по вертикальной системе управления [83, с. 137].

Очевидно, что такая организация деятельности практически повторяет модель, на которую переходят современные высокоорганизованные преступные формирования. Соответственно, в противодействии им нужны адекватные подходы, один из которых базируется на идеях военного теоретика Джона Вардена.

Анализируя врага как систему, он разработал модель ранжирования стратегических «центров тяжести» противника в форме пяти концентрических колец (рисунок 1).



Рисунок 1 – Стратегические «центры тяжести» противника по Дж. Вардену.

Согласно данной модели, в пределах каждого кольца существует один или несколько «центров тяжести», представляющих собой «узел силы и движения» для данного кольца. При этом, если он разрушен или нейтрализован, то эффективное функционирование кольца прекращается, причем последствия этого будут оказывать влияние на всю систему (внутреннее или внешнее кольцо). Для определения ключевых узлов внутри каждого кольца Дж. Варден предлагает дальнейшее разбиение каждого из них на пять «субколец»: руководство, критические объекты и т.д., каждое из которых, при необходимости, еще раз делится на пять колец, пока не будет получена действительная картина будущих целей [95].

В настоящее время теория Дж. Вардена широко применяется при выборе стратегических целей при планировании военных операций. Кольца Вардена вошли в военные документы вооруженных сил ряда западных государств, а разработанная Дж. Варденом теория легла в основу концепции сетецентрической войны [83, с. 300].

Этот подход напоминает вышеизложенный подход А.С. Овчинского о том, что структуры криминальных связей было предложено классифицировать по четырем основным типам: очаг, «ансамбль», центр и сеть. В чем же смысл структурного анализа? Чем он может быть полезен оперативно-розыскной аналитике? С позиции возможности получения реактивной информации понятно, что «узкие места» криминального бизнеса, имеющего структуру «ансамбль» – это связи между отдельными звеньями. Если сами звенья «ансамбля», как правило, достаточно законспирированы или труднодоступны, то оперативно значимую информацию удается получать «на стыках» отдельных звеньев при их взаимодействии. Основа расчетов должна базироваться на теории разрушения систем, имеющих сетевую структуру с определенным запасом резервных возможностей. Исследования таких систем проводились в 1930-1940-е годы как американскими, так и советскими учеными. Согласно этой зависимости, когда частота отказов отдельных элементов составляет 11%, вероятность разрушения всей системы равна 50%. При частоте отказов 25% вероятность разрушения системы составляет уже 81%. Если же частота отказов отдельных элементов стремится к 50%, то вероятность гибели всей системы составляет 100%. Можно привести множество примеров систем самой разной природы, жизнеспособность которых подчиняется этой математической зависимости. Расчет показывает, что, если в системе будет поражено 50% ее узлов, то она не сможет функционировать. В природе не существует систем, способных выдерживать разрушение половины своих составных частей. Но если и четверть элементов будет выключена, то вероятнее всего (81%), что система не сможет существовать без коренной перестройки. Так, во времена эпидемий чумы в средние века, когда число заболевших приближалось к четверти населения, все оставшиеся жители покидали пораженный болезнью город [8, с. 71-73; 79, с. 15-16].

Учитывая точку зрения А.С. Овчинского, изложенная модель ранжирования вполне может быть адаптирована и для правоохранительной деятельности, где противником являются высокоорганизованные сетевые криминальные структуры, которые и составляют главный базис преступности на той или иной территории. В такой интерпретации в графическом выражении модель их «центров уязвимости» может выглядеть следующим образом (рисунок 2).



Рисунок 2 – Предлагаемая модель ранжирования «центров уязвимости» высокоорганизованных криминальных формирований

Следуя подходу Дж. Вардена, каждый из указанных «центров уязвимости» анализируется на наличие «субколец». Например, структура подконтрольных сфер высокоорганизованных криминальных формирований, как правило, неоднородна и зависит от конкретной территории. В стандартном варианте это: незаконный оборот наркотиков, оружия, контроль за крупными объектами бизнеса, нелегальная миграция и др. В свою очередь незаконный оборот наркотиков подразделяется на синтетические (ЛСД, экстази и др.) или растительного происхождения (зарубежные героин и кокаин, либо отечественные гашиш и марихуана). Каждая из этих сфер имеет свое руководство, свою критическую инфраструктуру, вовлеченных лиц и т.д. [91, с. 315].

Таким образом, предлагаемая ступенчатая модель ранжирования «центров уязвимости» способна дать действенный механизм для опережающей разведывательно-поисковой (проактивной) работы правоохранительных органов, прежде всего оперативных подразделений ОВД. Когда четко видна цель и стоящие задачи, то гораздо проще спланировать и провести мероприятия по их достижению.

Сеть любого значимого размера имеет как сердцевину (ядро), так и периферию. Ядро состоит из плотных сетевых связей среди группы индивидуумов или малых организаций, которые обеспечивают управление и определяют направления деятельности всей сети. Члены ядра сети должны иметь связывающие механизмы, которые позволяли бы обеспечить высокий уровень доверия и надежность взаимоотношений. Сплачивание может достигаться различными путями – через этническую общность, семейственность, исторические или другие связи. Оно имеет важное

значение для ядра сетевой структуры. Периферия не так сплочена, у нее более свободные отношения и менее крепкие сплачивающие механизмы [96].

Такая характеристика типичной сетевой структуры, в том числе криминальной, дает для оперативных подразделений координаты наиболее оптимальных «точек входа» в нее. Это – периферия, включающая в себя прежде всего подконтрольные структуры и их персонал. Однако на практике они в большинстве случаев остаются «невидимыми» для оперативных работников, так как не представляют интереса. К тому же имеет место извечная «боязнь» затрагивать экономические и финансовые источники существования преступных групп, прикрываемая дежурным тезисом, что это компетенция службы экономических расследований.

Поэтому разработка сетевых криминальных структур традиционно начинается разработкой их рядовых членов, и ими же в большинстве случаев ограничивается, что позволяет удовлетворить формальным критериям по количеству уголовных дел.

Как уже отмечалось выше, это классический пример преобладающей в настоящее время реактивной модели деятельности оперативных подразделений ОВД.

Но в ней не учитывается то принципиальное обстоятельство, что современное противоборство с внутренним и международным криминалитетом носит ассиметричный характер. Структурно организованной деятельности преступных формирований, террористических и экстремистских организаций, их действиям по дискредитации правоохранительных органов, по подрыву основ государственности необходимо противопоставлять более совершенное информационно-аналитическое, информационно-технологическое и информационно-психологическое обеспечение правоохранительной деятельности. Должны применяться как технологии процессуального (в рамках правового поля), так и непроцессуального использования оперативно-розыскной информации, если изменение правовых норм отстает от стремительно обостряющейся криминальной ситуации. Противоборство с противником, имеющим разветвленную сетевую организацию, требует получения информации в реальном масштабе времени. Это дает возможность мгновенно принимать решения и упреждающе реагировать не только на противоправные действия, но и на замыслы и планирование тех или иных деструктивных акций [8, с. 78].

Вместе с тем при практическом использовании предложенной выше модели ранжирования «центров уязвимости» высокоорганизованных криминальных формирований следует постоянно учитывать важные аспекты.

Так, по мнению Р.В. Арзуманяна, при декомпозиции и анализе системы противника на основе теории Дж. Вардена следует обращать внимание на следующие три фактора. Во-первых, даже если анализ системы противника корректен, ключевое правило теории о первоочередном выборе в качестве цели руководства системы не обязательно является корректным. Руководство

не всегда является самой важной целью. Другие кольца (или связи между ними) могут и зачастую содержат гораздо более важные «центры тяжести». Теория Джона Вардена не отрицает этого, но указывает, что в большинстве случаев цели во внешних кольцах должны быть выбраны так, чтобы влиять на расчет показателя «затраты – выгоды» именно для руководства системы, так как именно оно определяет политический курс, который необходимо изменить [97].

Между тем, в практике работы оперативных подразделений ОВД РК преимущественно присутствует ошибочный подход, что привлечение к ответственности лидера преступной группы и наиболее активных участников автоматически приведет к ее разобщению. Как правило, после этого считается, что цель ОРМ достигнута, дело оперативного учета прекращается как успешно реализованное и сдается в архив.

Однако, вышеизложенная характеристика сетевых структур показывает, что здесь нет прямой зависимости. Без устранения 50 % их организации они способны к восстановлению, тем более, если экономическая и финансовая основа осталась нетронутой.

Такое углубленное понимание сущности сетевых структур организованной преступности (в широком смысле, включающем сюда же и наркопреступность, экстремизм и терроризм, а также деструктивную деятельность) открывает перед оперативными подразделениями ОВД совершенно иные подходы. Они заключаются в смещении акцента с безальтернативного варианта уголовного преследования и упорного (часто безрезультативного) поиска процессуальных доказательств на выработку мер по разрушению инфраструктуры криминальных формирований.

Такой подход полностью соответствует предназначению ОРД ОВД и придаст ей реальный проактивный характер.

Во-вторых, отмечает Р.В. Арзуманян, теория Дж. Вардена дает ключ к пониманию потенциальной роли информационно-психологических, экономических и других нелетальных воздействий на руководство противника в составе общей операции. Она показывает, что поражение системы противника может быть достигнуто исключительно через информационно-психологическое воздействие на руководителей системы, через навязывание своей системы ценностей или снижение воли к сопротивлению [97, с. 414].

Такой подход дополняет предыдущий; он является абсолютно новым и непривычным для науки и практики ОРД ОВД, до сих пор воспринимающих криминальную среду только через призму уголовного преследования. Но объективные реалии сегодняшнего дня заставляют оперативно пересматривать устоявшиеся взгляды и адаптироваться к внешним изменениям, трансформируя свое внутреннее отношение к ним. Ведь разрушить действующую криминальную структуру, не сводя всю работу только к уголовным делам – это идеальный вариант реализации принципа экономии уголовных репрессий и, в конечном итоге, наиболее эффективная

форма организации государственной политики противодействия преступности.

При этом в данной деятельности можно и нужно применять нестандартные методы – информационно-психологическое воздействие, управляемый хаос и др., осуществляемые в рамках различных оперативных комбинаций и тактических операций. Они способны создать благоприятные условия, при которых фигуранты будут вынуждены проявлять свои криминальные действия, что позволит привлекать к ответственности не только непосредственных исполнителей преступлений, но и членов иных звеньев сетевой структуры.

По нашему убеждению, информационно-психологическое воздействие на интересующий контингент имеет не меньшие (а, возможно, и большие) возможности в деле реального разрушения преступных структур, нежели уголовное преследование. Поэтому ниже будут рассмотрены такие методики прикладного характера применительно к ОРД ОВД.

В-третьих, теория Дж. Вардена имеет дело с односторонним действием, предпринимаемым против пассивного противника. Таким образом, игнорируются циклы «действие-реакция» и сопутствующие им факторы конфликтного взаимодействия систем. При этом Дж. Варден утверждает, что если нападающая сторона имеет заведомо более быстрый цикл управления, то это фактически исключает возможность реакции противника на стратегическом уровне управления [97, с. 415].

Говоря простыми словами, если оперативные работники, вооружившись знанием о сетевых структурах и владея проактивными методиками оказания зашифрованного (незаметного) воздействия на них различными способами (в том числе, а может и преимущественно, психологическими), окажутся в этой сфере быстрее разрабатываемых фигурантов, то они выполнят свою задачу по их разобщению.

Однако этот фактор работает и в обратную сторону. Тогда оперативные подразделения будут запаздывать, действовать «вторым номером», то есть останутся в реактивной модели.

Таким образом, современный глобализирующийся мир требует качественно нового подхода к проблемам принятия решений. Все более настойчиво ставится вопрос о сетевой природе управления: переходе от жестко иерархизированной вертикальной системы управления (где четко разделены центральное ядро, в котором принимаются решения, и периферия, обязанная эти решения беспрекословно выполнять) к запараллеленной, или распределенной, т.е. сетевой системе, когда полномочия по принятию решений делегируются от центрального ядра к структурным подразделениям [91, с. 67-99].

Выделяются два механизма, с помощью которых можно усилить сетецентрический характер деятельности оперативных подразделений ОВД

Первый – это развитие горизонтальных связей между ними на уровне район – район, город – город, область – область. Другими словами, это

координация действий прежде всего между соседними подразделениями; иногда и не только с ними, а с находящимися дальше.

Состояние такой координации зависит от многих факторов, основным из которых является дальновидность руководителей как самих органов, так и их оперативных подразделений. Хотя проблем в этой сфере достаточно, все же горизонтальная координация в определенной степени отработана, особенно в случаях совершения резонансных преступлений, когда всем соседям направляются ориентировки с описанием их обстоятельств, приметами подозреваемых лиц, похищенного имущества и т.д.

Это тоже элемент сетецентризма, возникший когда-то как логичный ответ на межрегиональный характер преступлений.

Вместе с тем эффективность подобной координации зависит от нескольких факторов:

– добросовестности оперативных работников, которым поручено провести мероприятия по отработке ориентировки, поступившей из другого органа;

– уровня их профессионализма – степени оперативного перекрытия обслуживаемой территории, чтобы своевременно ориентировать свои источники на поиск соответствующей информации;

– загруженности этих оперативных работников своими собственными делами; очевидно, что они не будут жертвовать ими ради выполнения «чужих» показателей.

Таким образом, горизонтальные связи данной сети зависят от мотивации конкретных лиц, которая носит не постоянный характер.

Напомним из вышеизложенного, какая мотивация присутствует у сетевых структурных элементов криминальных формирований. Это – выгода, материальная или моральная, но все-равно определенный мобилизующий компонент. Однако он обычно отсутствует в координации действий смежных оперативных подразделений ОВД, где ставка делается на сознательность, которая также является сугубо субъективным фактором.

Кроме того, очевидно, что количество штатных оперативных работников на порядок (а может, на несколько) меньше, чем контингент, нуждающийся в постоянном оперативном освещении. К примеру, в территориальных подразделениях УБОП один сотрудник может быть закреплен за преступной группой в несколько десятков членов. Соответственно, он физически не в состоянии охватить их всех наблюдением.

Значит, сетевую структуру необходимо выстраивать на мотивационной основе с привлечением внештатных участников. Сразу необходимо оговорить, что это не конфиденциальные помощники, которые также являются необходимым элементом сетевой структуры. Их рассмотрение относится к сведениям, относящимся к государственным секретам, и не может быть изложено в настоящем исследовании. Отметим лишь, что там во многом присутствуют проблемы, аналогичные приведенной выше координации оперативных подразделений ОВД по горизонтали.

Речь идет о внештатных участниках, оказывающих содействие на добровольной и гласной основе. Вопреки возможному пессимизму такие желающие тоже есть, о чем свидетельствуют обращения на блог Министра внутренних дел РК [98].

Возникает закономерный вопрос: какую мотивацию можно предложить таким внештатным участникам будущей сетевой структуры оперативных подразделений ОВД?

Материальный аспект можно отбросить сразу, так как такие отношения не подпадают под нормы Закона РК об ОРД, согласно пункту 5 статьи 23 которого на получение вознаграждения имеют право лишь конфиденциальные помощники [24].

Не полагаются такие выплаты и согласно Закону РК «Об участии граждан в охране общественного порядка». Согласно пункту 3 статьи 1, его действие не распространяется на правоотношения, возникающие в связи с ОРД [99].

Остается моральная мотивация, что на первый взгляд выглядит нереально. Однако мировой опыт показывает, что итоги такого сотрудничества внештатных сетевых структур с правоохранительными органами приносят более чем реальные результаты.

При этом некоторые из таких структур формировались на протяжении многих лет и сейчас могут представлять серьезную силу на международной арене, в зависимости от того, как государства и правительства будут контактировать с ними.

Наглядным примером является сетевая группировка, действующая на просторах Интернета (в том числе, в закрытых его сегментах, таких как Darknet); она называет себя Anonymous («Анонимус»).

Первые упоминания о хакерах, выбравших себе название «Анонимус», начали появляться в 2003 году. Тогда на площадках были замечены небольшие объединения интернет-активистов (которые сами себя называли «хактивистами»), устраивавших свои акции, носившие достаточно локальный и бытовой характер. Основными объектами их деятельности на тот момент были другие интернет-ресурсы, куда они совершали свои хакерские набеги, а также разные скандальные деятели интернета. По своей сути они являются «цифровыми анархистами», выступающими против притеснения свободы слова в интернете, цензуры и препятствий в распространении контента. Именно поэтому с обычных сайтов «Анонимус» быстро переключился на правительственные ресурсы, порталы корпораций и религиозных организаций, банковские структуры и прочие системообразующие, аффилированные с государством службы. Особенность движения заключается в его децентрализации – исторически сложилось, что на просторах интернета действуют разрозненные группы активистов, именующих себя анонимами [94].

Как было отмечено выше, это является характерным признаком любой сетевой структуры – децентрализация и частое отсутствие единого центра руководства и управления.

Известность к ним пришла в 2008 году после войны, объявленной последователям церкви саентологии в США. Саентологи требовали удалить из интернета интервью с одним из своих адептов – Томом Крузом. В 2010-х годах группировка укрепила свои позиции борцов с консервативными режимами, выступив на стороне протестующих во время «арабской весны» в ряде арабских стран. Окончательная «политизация» группировки произошла после того, как на основателя WikiLeaks Джулиана Массажа составили уголовное дело. «Анонимус» считали себя идейными продолжателями его дела, поэтому незамедлительно подвергли «цифровому остракизму» платежные системы PayPal, VISA, MasterCard и другие, которые заморозили донаты для WikiLeaks. Кроме того, пострадали правительственные сайты Швеции, ресурсы банка PostFinance, личные данные многих фигурантов судебного процесса. Кроме того, «Анонимус» взламывал ресурсы, распространявшие детскую порнографию, и сливал в открытый доступ данные пользователей этих сайтов [100].

Получается, помимо заявленных политических целей, «Анонимус» инициативно осуществлял общественно полезную деятельность, противодействуя организованным формам преступности.

При этом, если оперативники ограничены политикой, в рамках которой без доказательных аргументов, исков и постановлений у них нет права на доступ и анализ данных, то для «Анонимус» такие формальности не помеха [101].

В данном случае эта группа представляла для правоохранительных органов и специальных служб идеальное сетевое звено, которому можно доверить «деликатные» поручения в условиях, когда нет законных оснований действовать государственным органам. Такую возможность они не упустили.

Известны случаи, когда специальная программа с нелегальных сайтов скрыто отправляла на сервера спецслужб данные о посетителях. При этом последовательность событий, предшествовавших громким арестам, иногда складывается в интересную схему, в рамках которой хакеры «громко» и вовремя взламывают именно те ресурсы, в которых заинтересованы правоохранители. К примеру, в 2014 году «Анонимус» вывели из строя более 10 тыс. сайтов крупного Darknet-провайдера Freedom Hosting II. На всех вскрытых ресурсах безымянный диверсант оставил сообщения о том, что все пароли и явки скопированы с целью передачи в руки правоохранительных органов, таким образом отомстив за распространение детского порно. Ряд специалистов полагают, что успех «Анонимус» мог обеспечить слив информации изнутри: на это указывают масштабность цели и короткие сроки проведения операции, как если бы атакующие изначально знали узлы, между которыми шел обмен данными [101].

Очень похоже, что опытом зарубежных коллег воспользовались и российские правоохранители. По имеющейся информации, они инициировали конкурентную борьбу между различными Интернет-площадками в Darknet за передел рынка наркобизнеса, использовав их друг

против друга. Таким образом, были устранены Darknet-сервисы R2D2, AmberRoad, Malina и RuTor [102].

При этом «Анонимус» не единичное явление в киберпространстве.

Например, существует некоммерческая организация Open Briefing, которая называет себя «первой в мире разведслужбой гражданского общества». Она ставит своей целью сбор, анализ и распространение ключевой информации в интересах правозащитных групп, агентств гуманитарной помощи и других общественных организаций и гражданских активистов [103].

Это то, что известно о всемирно известных сетевых организациях. Кроме того, на уровне отдельных стран или даже их регионов не исключено существование аналогичных структур, занимающихся локальными вопросами. Наибольшую перспективу здесь представляют журналистские сообщества, прежде всего освещающие криминальную тематику и специализирующиеся на расследованиях.

Как правило, это достаточно грамотные люди, владеющие приемами поиска интересующих сведений в современном информационном пространстве, в отличие от многих оперативных работников.

Привлечение их к сотрудничеству как временные или постоянные сетевые звенья оперативных подразделений ОВД способно дать перспективные результаты.

Такое предложение в своей диссертации выдвигал А.К. Сысоев, когда обосновывал две модели такого сотрудничества. При первой модели оперативный аппарат (с санкции соответствующего руководителя) инициирует контакт с организациями типа «Анонимус», при этом не скрывая своей принадлежности к правоохранительной структуре, и предлагает им взаимовыгодный сетевой альянс. В случае принятия такого предложения оперативный аппарат получит в свое распоряжение серьезные ресурсы организации, которая, в свою очередь, может быть заинтересована в официальной реализации имеющейся информации в отношении киберпреступников. При второй модели контакт оперативного аппарата с такими структурами может устанавливаться в процессе внедрения под соответствующей легендой, например, имитируя желание вступить в хакерское ополчение, чтобы помогать в разоблачении педофилов, коррупционеров, сбытчиков наркотиков и т.д. [104].

Естественно, рассматривая предложение А.К. Сысоева применительно к казахстанским реалиям, сложно представить, каким образом в настоящих условиях оперативные подразделения ОВД смогут на равных выстраивать взаимоотношения с аналогами «Анонимуса», даже действующими на местном уровне, из-за несоответствия уровня технологической подготовки. Это перспектива завтрашнего дня.

А вот сотрудничество с журналистским сообществом – это элемент сетевой организации, которую можно внедрить уже сейчас. Главное в таком подходе – здесь присутствует та самая мотивация, причем не материальная.

Это выгода. Оперативный работник получает в свое распоряжение дополнительные источники информации, которых не надо учить действовать. А журналисты получают доступ к некоторому объему оперативных данных, которых нет в открытом доступе, так как они находятся в закрытых базах, либо в голове оперативника.

Таким образом, получается взаимовыгодный симбиоз на сетевой основе.

Естественно, подобное сотрудничество должно строго контролироваться руководителями оперативных подразделений на предмет излишней утечки оперативной информации, могущей привести к расшифровке проводимых ОРМ или нарушению прав и свобод личности [105].

На этом фоне существует еще одна сфера, которая может кардинально помочь в деле создания проактивной сетецентрической структуры оперативных подразделений ОВД.

Это область так называемой частной детективной деятельности, которая в Казахстане до сих пор не урегулирована, хотя многочисленные попытки предпринимались.

Впервые необходимость разработки закона о частной сыскной деятельности была поднята ещё в 2003 году. В 2006 году подготовленный законопроект прошёл стадию голосования в Мажилисе Парламента, однако его принятие было отклонено Сенатом. Кроме того, данный вопрос находился в центре внимания первого президента Н.А. Назарбаева, который в рамках мероприятий по совершенствованию деятельности правоприменительных органов поручил подготовить данный закон. В 2012 году эта тема вновь получила развитие, когда в своём ежегодном Послании народу Казахстана Н.А. Назарбаев вновь акцентировал внимание на важности принятия закона. Так же Министерство внутренних дел Республики Казахстан сообщило, что разработка документа продолжается. Принятие этого закона, по мнению представителей МВД, способствовало бы обеспечению профильной деятельностью многих сотрудников оперативно-следственных подразделений правоохранительных и специальных органов, которые вышли на пенсию. Кроме того, предполагалось, что принятие закона позволит создать рынок новых услуг, таких как розыск без вести пропавших лиц, возврат утраченного имущества и предоставление юридической помощи физическим и юридическим лицам.

Однако, несмотря на явную перспективность закона о частной детективной деятельности, даже его разработка, не говоря о принятии, по ряду причин «тормозилась». Каковы эти причины, и кто это делал?

Любопытные версии озвучивают казахстанские журналисты.

Некоторые эксперты видят причины в нежелании государственных служащих, чиновников высокого ранга создать такие условия для детективов, когда они сами могут стать объектом их расследований. Поэтому разработанный законопроект оказался «беззубым». В нем были всего две статьи, определяющие особые возможности частного детектива, и одна, описывающая его права. Ему позволялось проводить индивидуальную

беседу и осуществлять запрос справок, характеристик, иных документов у физических или юридических лиц и создавать общественные объединения. Любые другие мероприятия, включая съемку скрытой камерой, признаны недопустимыми в рамках частного сыска, что делает бессмысленной саму работу детектива в современных условиях [106].

В развитых же странах работа частного детектива уважаема, востребована и заключается она далеко не только в слежке за неверными супругами. Это и розыск людей, в том числе пропавших, в том числе детей. Это и розыск имущества. Это и проведение расследований. Это и проверка благонадёжности. И многое-многое другое. При этом частные детективы работают практически всегда эффективнее полиции [107].

Возможно, и в этом тоже была одна из причин того, что частная детективная деятельность в Казахстане до сих пор не узаконена, хотя она давно регламентируется в ряде стран ЕАЭС.

Так, например, в России Закон «О частной детективной и охранной деятельности в Российской Федерации» был принят в марте 1992 года и позволяет гораздо более широкий спектр действий частных детективов.

Согласно статье 5 «Действия частных детективов», в рамках частной сыскной деятельности допускаются следующие действия: проведение устных опросов граждан и должностных лиц, но исключительно с их согласия, сбор справочной информации, изучение предметов и документов на основании письменного согласия их владельцев, а также внешний осмотр зданий, помещений и других объектов. Кроме того, в целях предоставления услуг разрешено осуществление наблюдения для сбора необходимой информации.

Также допускается использование технических средств, таких как видеозапись, аудиозапись, фото- и киносъёмка, при условии, что их применение не наносит вреда жизни и здоровью граждан, а также окружающей среде. Все действия, связанные с использованием указанных средств, должны строго соответствовать требованиям законодательства Российской Федерации [108].

Также широк круг их компетенции, которые указаны в статье 3 этого же Закона. В целях частного сыска разрешается предоставление следующих услуг:

1) сбор сведений по гражданским делам на договорной основе с участниками процесса;

2) изучение рынка, сбор информации для деловых переговоров, выявление некредитоспособных или ненадежных деловых партнеров;

3) установление обстоятельств неправомерного использования в предпринимательской деятельности фирменных знаков и наименований, недобросовестной конкуренции, а также разглашения сведений, составляющих коммерческую тайну;

4) выяснение биографических и других характеризующих личность данных об отдельных гражданах (с их письменного согласия) при заключении ими трудовых и иных контрактов;

5) поиск без вести пропавших граждан;

6) поиск утраченного гражданами или предприятиями, учреждениями, организациями имущества;

7) сбор сведений по уголовным делам на договорной основе с участниками процесса. В течение суток с момента заключения контракта с клиентом на сбор таких сведений частный детектив обязан письменно уведомить об этом лицо, производящее дознание, следователя или суд, в чьем производстве находится уголовное дело;

8) поиск лица, являющегося должником в соответствии с исполнительным документом, его имущества, а также поиск ребенка по исполнительному документу, содержащему требование об отобрании или о передаче ребенка, порядке общения с ребенком, требование о возвращении незаконно перемещенного в Российскую Федерацию или удерживаемого в Российской Федерации ребенка или об осуществлении в отношении такого ребенка прав доступа на основании международного договора Российской Федерации, на договорной основе с взыскателем [108].

Аналогичный закон принят в Кыргызстане в 1996 году [109], его содержание в целом аналогичному российскому.

Учитывая существующие в Республике Казахстан в настоящее время законотворческие тенденции, в обозримом будущем ожидается возврат к рассмотрению законопроекта о частной детективной деятельности.

В разрезе внедрения принципа сетецентризма в деятельность оперативных подразделений ОВД его нормы могут предоставить еще один, возможно, самый перспективный элемент сетевой структуры.

Как правило, частными детективами станут лица, ранее работавшие в следственно-оперативных подразделениях правоохранительных органов и специальных служб, то есть лица, изначально знакомые с основами ОРД. Кроме того, определенная корпоративная солидарность благоприятствует установлению рабочих взаимовыгодных отношений с ними со стороны действующих оперативных работников.

Ну и главное – здесь будет присутствовать нематериальная заинтересованность обеих сторон в продуктивном диалоге. Оперативные подразделения получают дополнительный объем интересующей информации, на который не нужно расходовать собственные усилия и ресурсы. Частным детективам выгодно изначально иметь положительное отношение с оперативными работниками, так как именно на ОВД будет возложена обязанность по проверке кандидатов в частные детективы для решения вопроса о выдаче соответствующей лицензии на такую деятельность [105, с. 21].

В настоящее время такого основания для проведения ОРМ в Законе РК об ОРД пока нет. Но логично, что необходимость подобной нормы появится в рамках приведения законодательства в соответствие после принятия Закона о частной детективной деятельности по аналогии с охранной, которая в Законе РК об ОРД прописана в пункте 2 статьи 10 [24].

В то же время частная детективная деятельность не идентична охранной. В силу родственности ее с ОРД при ее осуществлении достаточно высока вероятность сознательного или неосознанного нарушения прав и свобод личности. Соответственно, требования к частной детективной деятельности должны быть повышенными. Оперативные подразделения должны осуществлять ОРМ не только для решения вопроса о выдаче лицензии на занятие частной детективной деятельностью, но и о её лишении в случае таких нарушений.

В этой связи, учитывая активизацию законотворческой работы по проекту соответствующего закона, целесообразно параллельно пункт 2 статьи 10 «Основания проведения оперативно-розыскных мероприятий» Закона РК об ОРД дополнить абзацем следующего содержания:

«- о выдаче или лишении лицензии на занятие частной детективной деятельностью;».

Мы считаем, что такая норма будет способствовать повышению мотивации частных детективов для их тесного взаимодействия с оперативными подразделениями ОВД. Это создаст благоприятные условия для получения последними дополнительной информации о лицах и фактах, представляющих оперативный интерес.

В итоге, институт частных детективов может стать наиболее действенным звеном в сетецентрической структуре, создаваемым оперативными подразделениями ОВД в противодействии преступности.

Кроме того, легенды журналистов или частных детективов будут идеальным прикрытием для работы таких негласных оперативных служб ОВД, как Седьмой департамент или служба «Р» (криминальная разведка).

Как отмечают В.Р. Григорьев и Л.О. Шуркин, чтобы эффективно действовать в сложном и нестабильном мире, необходимо принимать во внимание контекст (как ближайший, так и достаточно широкий) изучаемых явлений и событий. «Думай глобально, а действуй локально!» – вот лозунг сегодняшнего дня. Решая задачи информационного противоборства, необходимо понимать способы интеграции и взаимосогласованного, гармоничного развития различных сложноорганизованных структур [91, с. 67-99].

К таким структурам можно отнести как современную преступность (в широком смысле), так и правоохранительные органы, в частности МВД как самый большой из них. Отсюда следует, что в рамках противодействия преступности система МВД должна действовать как на более высоком стратегическом (проактивном), так и на тактическом уровнях.

Однако проблема профессионального сознания подавляющего большинства нынешних оперативных работников и их руководителей заключается в том, что они не стремятся и, соответственно, не умеют мыслить в стратегических форматах. Их конечные цели максимально конкретизированы – выявить и раскрыть отдельное преступление, не разбираясь особо, каковы его глубинные (стратегические) причины и условия.

Соответственно, такой подход способствует их сохранению и постоянному воспроизводству новых криминальных явлений. И этот процесс даже выгоден действующей парадигме правоохранительной деятельности, так как демонстрирует яркую и эффектную, но не эффективную работу оперативных подразделений ОВД.

Поэтому их важнейшей задачей является постепенная поступательная переориентация сознания на приоритетность проактивных методик, основанных на сетецентрических подходах, изложенных выше.

Обобщая теоретические, организационные и правовые аспекты принципа сетецентризма как организационной основы проактивного подхода к осуществлению ОРМ, можно сделать следующие выводы:

1. Система МВД еще до конца не осознала факт перехода современной преступности на сетевую структуру и ошибочно выстраивает противодействие ей на устаревших представлениях о ней, чем в значительной степени обусловлена неожиданность многих совершаемых резонансных уголовных правонарушений.

2. Успешность такого противодействия заключается в применении адекватных подходов, соответствующих структуре и динамике криминогенной ситуации, прежде всего основанных на сетецентрическом принципе работы оперативных подразделений ОВД.

3. Это принцип образует организационную основу их деятельности, а методическую базу составляют приемы и способы, предусматривающие информационно-психологическое воздействие на отдельных фигурантов и их группы с целью склонения к желаемой модели поведения.

Рассмотрению этих вопросов посвящен следующий подраздел настоящего исследования.

§ 2.3 Информационно-психологические операции в системе проактивного подхода

12 октября 2022 года Указом Президента Казахстана К.-Ж.К. Токаева были внесены серьезные изменения в военную доктрину. Помимо традиционных мероприятий по повышению боевого потенциала и укреплению обороноспособности, впервые упомянуты принципиально новые виды вооруженных сил, такие как кибервойска и подразделения информационно-психологических операций (PSYOP) [110].

Какие причины повлияли на включение PSYOP в военную доктрину Казахстана?

Таких обстоятельств несколько. Прежде всего, это события января 2022 года в Казахстане – масштабные протесты на социальной почве во многих регионах, сопровождавшиеся погромами и нападениями на сотрудников правоохранительных органов. Анализ этих событий показал, что определяющее воздействие на их активизацию оказало как раз проведение PSYOP, причем в большинстве случаев из-за рубежа [111].

В Казахстане до последнего времени о PSYOP было известно немного, и широко данная тема не обсуждалась. Видимо, это было обусловлено тем обстоятельством, что априори они считались одним из методов ведения боевых действий в отношении противника. А Казахстан провозглашает себя миролюбивым государством и воевать ни с кем не планирует.

Однако события января 2022 года в Казахстане (масштабные социальные протесты во многих регионах, сопровождавшиеся погромами и нападениями на сотрудников правоохранительных органов) показали, что даже в отношении стабильных государств не исключено применение принципов PSYOP, в том числе из-за рубежа [111].

В общем виде PSYOP можно характеризовать как спланированную передачу информации разным аудиториям граждан, с целью повлиять на их самочувствие, мотивы, критическое мышление, так, чтобы это в свою очередь повлияло на деятельность правительств, организаций, групп или индивидов. Наиболее известные виды методов информационно-психологического воздействия – это пропаганда и дезинформация [110].

По мере развития средств массовой информации, информационных технологий и техники информационное противоборство в мире становится всё более масштабным и результативным. Массированное использование информационных ресурсов, превысивших по своим объемам все мыслимые пределы, позволяет управлять общественным мнением вплоть до изменения системы ценностей широких масс населения [111].

Информационно-психологическое противоборство имеет давнюю историю. Оно возникло одновременно с появлением вооруженного противоборства как составная часть вооруженной борьбы в виде психологического средства ослабления боевой мощи противника и поднятия боевого духа своих войск. В настоящее время информационно-психологическое противоборство выделилось в самостоятельную форму борьбы, которая может вестись как без непосредственного применения военного насилия, так и в сочетании с военной силой [75].

Вместе с тем подобное определение информационно-психологического противоборства не вполне применимо к сфере противодействия преступности, так как оно полностью относится к военной сфере. Это не значит, что в правоохранительной сфере нет такого противоборства; просто оно специфично, о чем более детально будет изложено ниже.

В то же время в связи с тем, что технологии PSYOP еще не адаптированы под потребности уголовной юстиции, здесь и далее нам придется регулярно касаться военной сферы и пытаться трансформировать ее положения под рамки настоящего исследования.

Кроме того, становится все более очевидным критическое влияние PSYOP на стабильное функционирование государств, что наглядно демонстрирует геополитическая обстановка, сложившаяся сейчас в мире на фоне конфликта на Украине. В таких условиях развитие PSYOP в военной сфере является закономерным и обоснованным.

Аналогичный пример показывает конфликт в секторе Газа.

Министерство общественной дипломатии Израиля будет закрыто, министерство информации распущено за провальную информационную работу, начиная с момента террористического рейда ХАМАС 7 октября 2023 года. Данное министерство очевидным образом не справилось с координацией медийной деятельности и не наладило нормальные коммуникации государства и населения страны с международным сообществом. По итогу ХАМАС, Палестина и арабы в целом подчистую переиграли Израиль в информационной войне. Они склонили на свою сторону мнение общественности даже в Евросоюзе и в Америке [113].

Таким образом, обладая мощной армией, мотивированными солдатами и мобилизованным населением, Израиль, тем не менее, проигрывает информационную войну в глазах мирового сообщества. Причем его состояние напоминает шахматную ситуацию цугцванга, когда любой последующий ход только ухудшает положение.

В то же время возникает резонный вопрос: если такие операции столь эффективны на войне, почему бы теорию психологических операций не развить и не использовать столь же широко в правоохранительной деятельности, которая тоже является сферой конфликта между государством и криминалом?

И если в военно-политической сфере целевое информационное воздействие на противника воспринимается неоднозначно (с учетом зачастую диаметрально противоположных геополитических аспектов), то проведение PSYOP правоохранительными органами несет очевидную общественную пользу.

Если подходить к PSYOP как к пропаганде и дезинформации, то в противодействии преступности в той или иной мере они используются и сейчас, но носят другое название. Например, государственные программы профилактики правонарушений основываются на пропаганде законопослушного поведения граждан, а дезинформация широко практикуется в ОРД. Такие мероприятия, как оперативное внедрение или имитация преступной модели поведения, полностью построены на дезинформации криминальных структур, и это повсеместно признано общественно полезной практикой.

Вместе с тем практическая деятельность идет преимущественно путем совершенствования организационных и тактических основ таких мероприятий; при этом разработка целевых психологических моделей воздействия на подучетный контингент незаслуженно обойдена вниманием.

Поэтому, несмотря на очевидную аналогию подходов, теория и практика PSYOP в правоохранительной сфере должного развития пока не получили, во всяком случае в Казахстане. Не обнаружены подобные исследования открытого характера и в других странах постсоветского пространства, за исключением российского опыта.

Например, А.С. Овчинский достаточно давно говорит об информационно-психологическом воздействии организованной преступности, экстремизма и терроризма на различные слои населения, что

представляет серьезную угрозу. Он прямо называет такое воздействие информационными войнами, которые могут быть развязаны с различными целями, как локальными – изменения расстановки политических сил в обществе, так и глобальными– геополитическими, направленными на достижение мирового господства в той или иной сфере [43].

Отмечается, что лидеры преступных сообществ и террористических организаций все больше в своей практике стали применять научный подход: привлекать для работы профессиональных психологов, психотехников, профессиональных системных аналитиков, информационщиков, оперативных разработчиков из научной элиты и специальных служб [114].

В этом свете логично, что правоохранительные органы (прежде всего оперативные службы) должны противопоставить таким угрозам адекватную систему PSYOP, имеющую свои теоретические и практические основы.

Одним из таких элементов является применение теории управляемого хаоса. Ее основы были заложены примерно в 500 году до нашей эры китайским полководцем Сунь-Цзы в своем «Трактате о военном искусстве». В нем говорится, что приоритетными в борьбе с противником являются информационные действия, посредством которых необходимо добиться у противника беспорядка и хаоса, что будет способствовать победе [115].

Вместе с тем, несмотря на давность таких рекомендаций, в деятельности правоохранительных органов Казахстана подобные весьма перспективные подходы противодействия преступности используются не системно, лишь в работе отдельных полицейских подразделений благодаря профессиональному инстинкту, оперативной смекалке и творческому подходу некоторых оперативных работников.

Мы считаем, что в нынешних условиях качественного реформирования современной преступности, возрастания степени ее организованности, транснационального и технологического характера применение PSYOP способно поднять ОРД на качественно иной, проактивный уровень, позволяющий упреждать особо опасные криминальные проявления.

Тем более, что определенные методики таких психологических операций известны, они могут быть алгоритмизированы и лечь в основу деятельности оперативных служб. Как отметил А.Б. Рудаков, это может быть:

– разжигание противоречий и недоверия внутри организованных преступных групп, между преступными группами и сообществами;

– информационное стравливание их между собой;

– склонение их руководителей к сотрудничеству с правоохранительными органами;

– культивирование, запуск и управление «слуховыми вирусами» в криминальной среде;

– дискредитация в глазах общественного мнения организованной преступности как явления, так и конкретных лидеров;

– гласная и негласная работа со средствами массовой информации (СМИ)для нейтрализации конкретных преступных групп;

– организация конфликтов между ними, создание внутренней

обстановки нервозности, взаимного недоверия и подозрительности;

– организация мероприятий маскировочного характера («дымовая завеса») с последующим распространением нужных «слуховых вирусов» [114, с. 27-28].

Указанные мероприятия укладываются в теорию управляемого хаоса применительно к криминальным структурам. Данный принцип применим и в сфере противодействия религиозному экстремизму, который является для Казахстана серьезной угрозой общественной безопасности.

Практический опыт показал, что экстремистские организации построены по сетецентрическому принципу, объединяющему сообщество первичных ячеек («халок»), состоящих, как правило, из пяти членов. Старшим в ячейке является «амир», которому беспрекословно подчиняются все ее участники; связь с «амиром» вышестоящего уровня осуществляется только через него. Такая внутренняя структура обладает высокой степенью защиты, затрудняющей проникновение в нее полицейских агентов [115].

Но если посмотреть на нее через призму теории управляемого хаоса, то именно «амир» первичной ячейки может стать наиболее уязвимым ее звеном, так как несет полную ответственность за всю ее деятельность – за внутреннюю конспирацию, соблюдение установленных религиозных правил, регулярность собраний, координацию с вышестоящим «амиром», сбор финансовых средств и т.д. По каждому из этих направлений можно планировать мероприятия по инициированию управляемого хаоса.

Так, можно «вбрасывать» рядовым членам ячейки информацию о том, что другие участники (или сам «амир») негласно пренебрегают основными религиозными правилами: втайне употребляют алкоголь, сигареты, наркотики; часто нарушают регулярность молитв без уважительной причины, имеют подозрительные связи с правоохранительными органами и др. порицаемые действия.

Действенным может оказаться распространение «слуховых вирусов» о финансовой нечистоплотности активных членов или «амира» ячейки – тратах собираемых средств на свои личные нужды.

Учитывая повышенную конспирацию деятельности ячеек, распространение подобных «слуховых вирусов» способно вызвать рост подозрительности ее участников друг к другу и, соответственно, понизить или парализовать ее функционирование.

Результаты конкретных оперативно-розыскных мероприятий подтверждают эффективность такого подхода [115, с. 24].

Если же применять теорию управляемого хаоса одновременно и параллельно относительно всех известных экстремистских ячеек, можно воздействовать на всю организацию в целом или на ее отдельные части. В результате, можно добиться того, что все их основные усилия будут направлены на лихорадочную проверку «слуховых вирусов», приостановление действующих и задействование резервных каналов связи, «заморозку» подготавливаемых экстремистских или террористических актов. Как результат, угроза общественной безопасности может быть

значительно снижена или отсрочена, что дает оперативным работникам дополнительное время.

В то же время, как и любая перспективная методика, применение PSYOP в ОРД имеет «побочные» эффекты. Одной из наиболее проблемных является возможная неконтролируемая эскалация насилия, инициированная неумелыми или непродуманными психологическими действиями оперативных работников. Например, при подозрении в сотрудничестве с правоохранительными органами криминальные структуры или экстремистские группы могут прибегать к насильственным актам, вплоть до физического устранения подозреваемого. Это неизбежное условие любой активной деятельности в данной опасной среде, в связи с чем планируемые операции должны тщательно анализироваться с целью минимизации таких последствий [116, с. 26].

Итак, информационно-психологическое противоборство – процесс, отражающий различные уровни противодействия конфликтующих сторон, осуществляемого информационными и психологическими средствами для достижения политических и военных целей. Такая широкая трактовка рассматриваемого феномена позволяет охватить информационно-психологические акции, осуществляемые:

– на разных уровнях (стратегическом, оперативном и тактическом);
– как в мирное, так и в военное время;
– как в информационной, так и в духовной сфере;
– как среди своих военнослужащих, так и среди войск противника [117].

Данный подход применим и к правоохранительной деятельности. Здесь тоже можно разделить стратегический, оперативный и тактический уровни. Например, к стратегическому относятся оперативно-профилактические мероприятия, проводимые в масштабе всей страны, такие как «Правопорядок», «Мигрант», «Скотокрад» и др. В их преддверии проводится широкая разъяснительная работа, которая имеет серьезное влияние на криминальные структуры, которые в ожидании этих мероприятий, как правило, приостанавливают свою деятельность.

Оперативный уровень информационно-психологического воздействия на сферу и инфраструктуру преступности охватывает какой-либо регион или крупный населенный пункт в связи с проведением аналогичных мероприятий в меньшем масштабе, либо в связи с совершением резонансного преступления (например, вооруженный конфликт криминальных групп). В этом случае также их деятельность приостанавливается. В последнем случае иногда по каналам связи, установленным между оперативными работниками и руководителями преступных групп, на последних оказывается целевое психологическое воздействие с целью выдачи участников конфликта и использованного ими оружия.

Что касается тактического уровня, то это традиционная ежедневная работа оперативных подразделений с подучетным контингентом с целью предупреждения готовящихся и раскрытия совершенных уголовных

правонарушений, в процессе которой на этих лиц также оказывается определенное психологическое воздействие.

Это происходит постоянно, вне зависимости от того, мирное ли время или военное. Более того, в военное время интенсивность психологического воздействия на подучетный контингент должна усиливаться.

При этом такое воздействие не ограничивается только ими. В эту сферу входит широкий круг лиц, попадающих в орбиту ОРД. Прежде всего, это конфиденциальные помощники, а также свидетели, очевидцы, иные лица, обладающие необходимой информацией.

В системе информационно-психологического противоборства, осуществляемого в военных целях, можно выделить:

– информационную войну;
– психологическую войну.

Информационная война – борьба сторон за достижение информационного превосходства над противником в своевременности, достоверности, полноте получения информации, скорости и качестве ее переработки и доведения до исполнителей [117].

Эта война включает в себя такие направления деятельности, как:

–добывание необходимой информации;

–переработка полученной информации;

–защита информационных каналов от проникновения противника;

–своевременное и качественное доведение информации до потребителей;

–дезинформация противника;

–вывод из строя или нарушение функционирования систем добывания, переработки и распространения информации противника;

–уничтожение, искажение, хищение информации у противника;

–разработка более эффективных, чем у противника, средств работы с информацией.

Средствами ведения информационной войны могут быть:

– средства информационно-технического оружия;
– средства подавления информационных систем противника, вхождения в них в целях воздействия на циркулирующую информацию;
– средства пропагандистского вмешательства [117].

Категория «войны» неприменима к сфере противодействия преступности. Во-первых, в военной сфере активные действия информационной войны осуществляются преимущественно против населения (граждан) другой страны, в отношении которых отсутствуют многие обязательства. В правоохранительной сфере «противник» - свой гражданин, обладающий комплексом неотъемлемых прав, нарушать которые без веских оснований нельзя. Во-вторых, информационная война является частью общей военной стратегии, направленной в том числе на физическое уничтожение части армии противника, чего не допускает уголовная юстиция.

В то же время такие направления, как получение и обработка информации, а также дезинформация, достаточно широко распространены в ОРД ОВД.

Вторым компонентом военной сферы информационно-психологического противоборства является психологическая война – борьба между государствами и их вооруженными силами за достижение превосходства в психологической и духовной сфере, а также за превращение полученного преимущества в решающий фактор достижения победы над противником. При таком подходе информационные возможности, наряду с чисто психологическими акциями, выступают средством решения психологических задач. Рассматривая атакующие аспекты информационно-психологического противоборства, можно сформулировать следующую цель воздействия. Цель информационно-психологического противоборства – установление контроля над стратегически важными ресурсами страны-противника за счет управления людьми, заставив население страны-жертвы поддерживать агрессора, действуя вопреки своим интересам, не задействуя имеющиеся социально-психологические защитные механизмы [118].

Средствами осуществления психологической войны являются психологические операции. Это проводимая в мирное или военное время плановая пропагандистская или психологическая деятельность, рассчитанная на иностранные враждебные, дружественные или нейтральные аудитории с тем, чтобы влиять на их отношение и поведение в благоприятном направлении для достижения как политических, так и военных целей [117].

Как видно из определения, психологические операции представляют собой скоординированную пропагандистскую деятельность и психологические действия.

При этом под пропагандой понимается систематическое, целенаправленное распространение с помощью средств связи и информации определенных идей с целью оказания влияния на мнения, чувства, состояния и отношения или поведение объектов воздействия с тем, чтобы достичь прямых или косвенных выгод для своей страны [83, с. 589].

Отсюда, видимо, следует, что PSYOP – это последовательная совокупность определенных действий, осуществляемых в разовом или многократном порядке.

В военной сфере разовые мероприятия психологической войны представляют собой кратковременные целенаправленные действия специальных подразделений или отдельных специалистов, которые отличаются ограниченным характером и осуществляются в ограниченных (локальных) масштабах [119].

По нашему мнению, применительно к ОРД ОВД такими разовыми мероприятиями являются оперативные комбинации, каждая из которых направлена на решение отдельной задачи – установить круг криминальных связей объекта оперативного интереса, найти к ним подход, приобрести источник информации и т.д.

К тому же оперативные комбинации осуществляются оперативными работниками часто. Их опрос показал, что все они в той или иной степени проводят сами либо видят со стороны их проведение . То есть сама по себе комбинационность, являющаяся неотъемлемым элементом информационно-психологических операций, им знакома, что подтверждают результаты изучения дел оперативного учета, где в 25% случаев она присутствовала или хотя бы планировалась .

Говоря об адаптации опыта военной сферы под потребности правоохранительной деятельности, выше упоминалось о том, что определенное психологическое воздействие на подучетный контингент на разных уровнях осуществляется и в настоящее время.

Это отметили в своих ответах более половины опрошенных респондентов , хотя по изученным делам эта доля составила лишь 15% .

Вместе с тем какой-либо чёткой системы такой работы, а тем более её научного обоснования, в Казахстане пока не существует. Поэтому применение технологий PSYOP в основном осуществляется интуитивно и хаотично.

В этой связи адаптация их к теории и практике ОРД ОВД является актуальной задачей ввиду очевидной перспективности.

Если обратиться к истории, то поворотным пунктом в развитии как теории пропаганды на противника, так и совершенствования практики применения психологии для разложения войск противника в больших масштабах, подрыва морального состояния народа в стране противника явилась Первая мировая война. Этот не только количественный, но и большой качественный скачок был обусловлен появлением материально-технических средств для размножения листовок миллионными тиражами, авиации для быстрой доставки печатной продукции адресату и, наконец, распространением грамотности среди большинства населения стран, принимавших участие в войне [120].

Впервые понятие «психологическая война» использовал британский военный историк Дж. Фуллер в 1920 году при анализе психологических проявлений этой тяжелой войны. В широкий обиход этот термин был введён П. Лайнбарджером в работе «Психологическая война», изданной в 1948 году, где был обобщён собственный опыт и военно-психологическая обработка нацистов в проведении информационно-психологической войны во время Второй мировой войны. Психологическая война в то время использовалась в качестве вспомогательного оружия и полезной составной части стратегии, способствующей одержанию победы над противником при помощи пропагандистских мероприятий, психических операций, распространения слухов и т.д. [121].

Само понятие PSYOP впервые было использовано в 1945 году американским военным деятелем, контр-адмиралом Э. Захариасом в планах США по разработке войны с Японией [122].

Конечно, в те годы возможности PSYOP были ограничены существовавшими тогда «скромными» возможностями по распространению

информации. Но возникновение и развитие новых информационных технологий, появление Интернета и социальных сетей ускорили эти процессы.

Символической точкой отсчета революционных преобразований в этой области стал тщательный анализ американским военным руководством опыта по достижению информационного превосходства на поле боя, полученного в ходе операции «Буря в пустыне» (1991), ставшей последней «классической» и первой крупной информационно-психологической операцией в современной военной истории. Результатом анализа стала опубликованная на страницах американской военной печати работа бывшего командующего командованием учебных и научных исследований по строительству сухопутных войск генерал-майора Гленса Отиса. В материалах указывалось: «Из операции «Буря в пустыне» можно извлечь много уроков. Некоторые из них новые, некоторые старые. Один урок, тем не менее, является поистине фундаментальным. Природа войны коренным образом изменилась. Та сторона, которая выиграет информационную кампанию, победит. Мы продемонстрировали этот урок всему миру: информация является ключом к современной войне в стратегическом, оперативном, тактическом и техническом отношениях» [123].

В XXI в. в ходе информационной революции ведущие государства мира перешли к ведению информационных войн, в которых ставка делается на стратегическое информационное противоборство, PSYOP при этом являются не просто одним из компонентов способа ведения войны, а приобретают полностью самостоятельное значение [112, с. 26-38]. Это эффективное оружие, направленное на лишение противника воли к сопротивлению, чтобы отказаться от военной силы [57, с. 70-74].

Хотя понятие PSYOP было сформулировано сравнительно недавно, в середине прошлого века, практика информационного воздействия на военного противника осуществлялось задолго до нашей эры. Общеизвестна история военной хитрости греков в ходе осады и последующего захвата Трои (XII век до н.э.), когда был применен метод «троянского коня». Как правило, широкой общественности известен лишь финальный этап этого события, хотя ему предшествовала серьезная подготовка, показавшая высокий уровень интеллекта греков.

В предыдущие годы греками была создана в Трое разветвлённая сеть высокопоставленных «агентов влияния», в том числе один из них по имени Синон. Именно он после появления статуи огромного коня стал убеждать набожных защитников крепости, что это – подарок богини Афины, и поэтому надо снести крепостную стену, ввести «коня» в Трою и хранить как святыню. Однако это было еще не все. Против переноса «деревянного коня» в Трою резко возражал жрец Лаокоон, видевший в нем очередное коварство греков, которое принесет городу большое несчастье. Но хитроумные греки предвидели подобный исход, и недоверчивый жрец был физически ликвидирован специальной группой ранее засланных в город лазутчиков. Это и решило судьбу Трои [124].

С тех далеких времен арсенал методов PSYOP значительно расширился и сейчас активно используется различными странами в геополитической, геоэкономической, военной и других стратегически важных сферах.

Так, еще в 2010 году правительство США заключило договор с компанией «HBGary Federal» на разработку компьютерной программы, которая может создавать многочисленные фиктивные аккаунты в социальных сетях для влияния на общественное мнение по спорным вопросам. По мнению специалистов, с февраля 2011 года эта программа активно используется и распространяется. Она также может быть применена для наблюдения за общественным мнением [125].

Еще раньше ВВС США заказали разработку «Persona Management Software» (программы по управлению персонажами), которую можно использовать для создания и управления фиктивными аккаунтами на сайтах социальных сетей, чтобы создавать впечатление, будто существует общепринятое мнение по спорным вопросам. Персонажи могут производить впечатление, что они происходят почти из любого места в мире, и могут взаимодействовать посредством обычных онлайн-сервисов и платформ социальных сетей [126].

На этом фоне очевидно, что современная международная обстановка имеет сложный характер, который в значительной степени влияет и на Казахстан. Динамичные процессы, протекающие в мировой геополитике (прежде всего, вооруженный конфликт между Россией и Украиной), обусловили необходимость соответствующей реакции на них путем вышеуказанного изменения военной доктрины.

Данная мера своевременна и в определённой степени запоздала: она отражает признание того факта, что сфера PSYOP фактически уже давно используется другими странами.

В военно-политической сфере целевое информационное воздействие на противника вызывает неоднозначную реакцию, что связано с часто противоположными идеологическими установками. В то же время использование PSYOP правоохранительными органами демонстрирует очевидную общественную пользу.

Если рассматривать PSYOP как элементы пропаганды и дезинформации, то эти методы в определенной степени уже применяются в борьбе с преступностью, хотя и под иными названиями. К примеру, государственные программы профилактики правонарушений основываются на пропаганде законопослушного поведения, а дезинформация активно используется в оперативно-розыскной деятельности (ОРД). Такие действия, как оперативное внедрение или имитация криминальной деятельности, полностью базируются на дезинформации преступных структур и общепризнаны полезной практикой.

Однако на практике основное внимание уделяется совершенствованию организационных и тактических аспектов подобных мероприятий, тогда как разработка целевых психологических моделей воздействия на подучетный контингент остается без должного внимания.

При этом, большинство опрошенных оперативных работников (свыше 65%) считают правомерным применение методов информационной войны и создание управляемого хаоса в преступных формированиях .

С учетом изложенного, несмотря на очевидную схожесть подходов, теория и практика PSYOP в правоохранительной деятельности на данный момент не получили достаточного развития, особенно в Казахстане. Аналогичные исследования в открытых источниках не обнаружены и в других странах постсоветского пространства, за исключением упомянутого опыта Российской Федерации.

Таким образом, назрела острая необходимость выработки методик информационно-психологического воздействия на криминальные структуры и их участников с целью разобщения и последующей нейтрализации.

Как уже отмечено выше, отдельные элементы PSYOP давно используются правоохранительными органами в рамках так называемых оперативных комбинаций. Они представляют собой сочетание комплекса негласных мероприятий, направленных на то, чтобы вынудить преступников действовать по тому плану, который выработали полицейские.

В то же время изучение практики такой деятельности показывает, что целевое информационно-психологическое воздействие при оперативной комбинации используется редко, хотя, в сущности, оно должно являться ее «сердцевиной». Первопричиной такой ситуации служит то обстоятельство, что основы PSYOP не изучаются полицейскими как в процессе обучения в ведомственных учебных заведениях (полицейских академиях), так и в рамках последующей специальной подготовки в процессе практической работы.

Между тем определенные методики таких психологических операций известны. Они могут быть алгоритмизированы и лечь в основу учебной программы сотрудников правоохранительных органов Казахстана.

Такой подход направлен на создание хаоса в криминальной структуре и последующее управление им в целях решения конкретных задач. В то же время теория управляемого хаоса в настоящее время рассматривается преимущественно применительно к геополитике и геоэкономике.

С. Манн, один из ведущих исследователей теории управляемого хаоса, анализировал её в контексте сложных неравновесных нелинейных систем, таких как общество, культура, экономика, политика, история, экология, международные отношения и другие. Согласно его концепции, подобные системы следуют принципу самоорганизующейся критичности, предполагающему естественную эволюцию к критическому состоянию. В таком состоянии даже незначительное воздействие может инициировать цепную реакцию, затрагивающую множество элементов системы. В качестве примера Манн приводил распад СССР и вызванные этим глобальные геополитические изменения.

Теория управляемого хаоса, по мнению С. Манна, даёт возможность осознать, что задача состоит не в жёстком контроле и абсолютной стабилизации систем, а в создании условий для мягкого, контролируемого изменения, способствующего развитию. Основная идея состоит в том, чтобы

не ждать, пока критическое состояние приведёт к катастрофическим последствиям, подобным внезапному сходу снежной лавины. Гораздо рациональнее заранее предвидеть этот момент и управляемо инициировать изменения с минимальными потерями, когда система ещё не достигла полной критической массы и остаётся относительно предсказуемой [127].

На этом фоне очевидно, что сфера противодействия преступности также относится к указанным С. Манном сложным системам, к которым вполне могут применяться положения теории управляемого хаоса.

Как отмечает А. Бартош, в теории управляемого хаоса особую значимость имеет способность любой сложной структуры в режиме повседневного функционирования контролировать и удерживать хаос в определенных рамках. Вместе с тем в другом режиме, например, в период искусственно созданного обострения – само это удержание посредством положительной обратной связи способствует лавинообразному нарастанию действия хаоса, что в конечном итоге может привести к распаду системы [128].

Какими могут быть средства реализации PSYOP? Если рассматривать сферу военного дела, технологии которого адаптируются для ОРД ОВД, то там все выглядит достаточно четко.

Например, С.И. Макаренко и М.С. Иванов относят такие средства к информационному оружию и дают его виды. Одним из них является средства психологического воздействия, дезинформации и пропаганды, к которым относятся:

– воздействие посредством СМИ, средства пропаганды, средства создания или модификации виртуальной реальности;

– средства имитации голосов операторов систем управления (например, систем управления воздушным движением) и видеоизображения конкретных людей с их голосом (руководителей государств, лидеров партий и др.);

– средства модификации информации, хранимой в базах данных информационных систем противника;

– средства ввода в информационные системы противника ложной информации и данных (целеуказания, мест доставки грузов и др.);

– средства дезинформации охранных систем;

– средства модификации данных навигационных систем, систем точного времени и др. [83, с. 541].

Перечисленные средства психологического воздействия в таком виде неприменимы в сфере противодействия преступности. Но, адаптируя некоторые их них, можно получить перспективные варианты. Например, вместо средств имитации голосов операторов систем управления можно успешно использовать технологию так называемых дипфейков (deep – глубинный, fake – подделка).

С помощью различных компьютерных программ (Zao, Reface, FaceSwapLite, DeepFaceLab и др.) можно создавать поддельное изображение (в том числе видео) реального человека. Для этого достаточно иметь

несколько фотоснимков и фрагмент голосовой речи интересующего лица. Программы позволяют также имитировать и голос [129].

Что касается контингента организованной преступности, наркобизнеса и религиозного экстремизма, то в оперативных учетах ОВД имеется достаточное количество их фото- и видеоматериалов. Основываясь на них, можно изготавливать высококачественные дипфейки (фото- и видеоизображения интересующих фигурантов), на которых они представлены якобы контактирующими с оперативными работниками либо с членами конкурирующих группировок в укромных местах (городские пустыри, лесопосадки, заброшенные здания и т.д.). Такие фото- или видеоматериалы могут стать серьезным компрометирующим фактором в отношениях между руководителями и активными участниками криминальных формирований, наркогруппировок, экстремистских и террористических организаций.

Если же дополнить такие визуальные материалы аудиозаписями якобы телефонных переговоров фигурантов с представителями правоохранительных органов либо конкурирующих группировок, то это серьезно усилит подозрения.

Если же использовать подобные фото-, видео- и аудиоматериалы с предварительно озвученными «слуховыми вирусами», то можно добиться реальной дезорганизации внутри структуры интересующей криминальной группы. Умело сочетая имеющиеся материалы и используя их каждый в свое время, можно негласно управлять нарастающим хаосом в ней с целью парализации (а в идеале - остановки) преступной деятельности.

Как отмечено выше, это и является главной целью PSYOP.

В то же время, как и любая перспективная методика, применение PSYOP и управляемого хаоса в ОРД имеет «побочные» эффекты. Одной из наиболее проблемных является возможная неконтролируемая эскалация насилия, инициированная неумелыми или непродуманными психологическими действиями оперативных работников. Например, при подозрении в сотрудничестве с правоохранительными органами криминальные структуры или экстремистские группы могут прибегать к насильственным актам, вплоть до физического устранения подозреваемого. Это неизбежное условие любой активной деятельности в данной опасной среде; в связи с чем планируемые операции должны тщательно анализироваться с целью минимизации таких последствий.

Для этого предназначена вторая часть технологии PSYOP – собственно психологическая составляющая. Для ее эффективного применения необходимо овладеть базовыми навыками и умениями психологической науки.

Сам термин «психологические операции» указывает на то, что для достижения целей подрывной деятельности широко применяются выводы психологической науки, которые направлены, в первую очередь, на изменение психологических состояний противника [117].

В то же время для их применения в сфере ОРД нет необходимости полностью погружаться в психологию. Необходимо выделить и сосредоточиться на отдельных методиках, предназначенных для завоевания доверия с целью управления действиями и поведением объектов оперативного интереса.

Речь идет о нейролингвистическом программировании (НЛП).

Нейролингвистическое программирование (НЛП) зародилось в США в начале 1970-х годов благодаря совместной работе Джона Гриндера, ассистента профессора лингвистики Университета Калифорнии в Санта-Круз, и Ричарда Бэндлера, студента психологии того же университета. Бэндлер также проявлял глубокий интерес к психотерапии, что способствовало их исследовательской деятельности. Вместе они занялись изучением профессиональных методов трёх выдающихся психотерапевтов: Фрица Перлза, новатора в области психотерапии и основателя гештальт-терапии; Вирджинии Сатир, талантливого семейного терапевта, известного способностью разрешать сложнейшие семейные конфликты, которые многим другим специалистам казались неразрешимыми; и Милтона Эриксона, признанного на мировом уровне мастера гипнотерапии.

Бэндлер и Гриндер изначально не ставили целью создание новой школы психотерапии. Их интерес был сосредоточен на выявлении паттернов (моделей и шаблонов), которые применялись выдающимися терапевтами, и на их адаптации для передачи другим. Вместо того чтобы углубляться в теории, они сосредоточились на разработке практических моделей терапии, демонстрировавших свою эффективность и доступных для освоения. Несмотря на значительные различия в подходах и индивидуальности трёх терапевтов, чьи методы они изучали, Бэндлер и Гриндер обнаружили удивительно схожие ключевые паттерны в их работе. Эти паттерны они систематизировали, улучшили и превратили в стройную и универсальную модель, которая нашла применение в областях, таких как эффективная коммуникация, трансформация личности, ускоренное обучение и повышение качества жизни.

Нейролингвистическое программирование включает в себя три ключевые концепции, отражённые в самом названии. Часть «нейро» подчёркивает основополагающий принцип: всё поведение человека начинается с неврологических процессов восприятия через зрение, слух, обоняние, вкус, осязание и другие ощущения. Именно через органы чувств мы познаём окружающий мир, извлекаем смысл из полученной информации и строим на её основе свои действия. Наша неврология объединяет как невидимые мыслительные процессы, так и заметные физиологические реакции на события и идеи, которые представляют собой взаимное отражение на физическом уровне. Это подчёркивает единство тела и разума, формирующее целостную природу человеческого существа.

Часть «лингвистическая» указывает на важность языка, который помогает нам структурировать свои мысли и поведение, а также является основным инструментом взаимодействия с окружающими.

«Программирование» в свою очередь акцентирует внимание на способах, с помощью которых мы систематизируем свои идеи и поступки, чтобы достигать конкретных целей и желаемых результатов [130].

Хотя основоположники НЛП создавали свои методики прежде всего в медицинских целях, результатами воспользовались и многие другие, прежде всего специальные службы, где умение находить общий язык с людьми и управлять ими является одной из главных задач.

Естественно, что тактика применения таких психологических методов, применяемых разведывательными структурами, носит закрытый характер. Но определенные их аспекты рано или поздно становятся гласными и ложатся в основу различных психологических курсов и тренингов.

Одним из ярких примеров является Институт НЛП, созданный в России под руководством одного из наиболее опытных тренеров НЛП – Михаила Пелехатого. По некоторым сведениям, он является учеником Ричарда Бендлера. Высшее образование получил в Высшей школе КГБ СССР, а затем в Академии внешней разведки России. В прошлом – профессиональный разведчик [131].

М. Пелехатый вместе с коллегами творчески адаптировали идеи основоположников НЛП применительно к сфере бизнес-разведки и деловых переговоров. При этом основа всех методик осталась неизменной – вхождение в контакт с целью завоевания доверия и управления поведением интересующих лиц [132].

В рамках настоящего исследования не представляется возможным полностью рассмотреть методики НЛП, применимые при использовании PSYOP в ОРД. Вместе с тем целесообразно очертить некоторые контуры такой работы для оперативных подразделений ОВД.

Эта деятельность может проводиться на двух уровнях – применение методов НЛП оперативными работниками в отношении: 1) конфидентов; 2) объектов оперативного интереса.

В случае с конфидентами цель заключается в их дополнительном психологическом мотивировании на качественное выполнение поставленных оперативных задач. Для этого они могут обучаться некоторым методам НЛП в ограниченном объеме, необходимом для этого. Главное предназначение данного подхода состоит в том, чтобы конфидент, находясь в доверительном контакте (прямом или опосредованном) с фигурантом, оказал зашифрованное воздействие на него – передал какую-то информацию, высказал мнение о связи фигуранта, поделился смутными подозрениями в отношении кого-либо, негласно распространил дипфейк и т.д.

Помимо конфидента, оказывать необходимое воздействие на фигуранта может и оперативный работник как непосредственно, так и через третьих лиц из числа его окружения. При этом может доводиться та же информация, что и через конфидента, но в иной интерпретации, чтобы не расшифровать его. Для фигуранта создается видимость, что сведения поступают из разных независимых источников, что повышает для него их достоверность.

Главная цель таких мероприятий – вызвать у фигуранта и его окружения сначала состояние неуверенности и подозрительности друг к другу, а затем усиливать их до организационного коллапса (управляемого хаоса).

Для этого НЛП дает конкретные методики установления контакта с интересующими лицами и последующего завоевания у них доверия. На их основе могут строиться алгоритмы деятельности конфидента и оперативного работника.

В подсознании любого человека сидит мысль, что полностью он может доверять только лишь себе. Соответственно, завоевание доверия зависит от того, в какой степени он видит в другом человеке самого себя. Поэтому НЛП в качестве первого шага предлагает подстройку к интересующему человеку. Есть несколько ступеней подстройки:

–к внешнему виду (рост, вес, одежда и обувь, головной убор, очки и т.д.);

–к позе (сидя, стоя, нога на ногу и т.п.);

–к тональности разговора (громко, средне, тихо);

–к дыханию [130].

При подстройке нельзя копировать оригинал, чтобы она не воспринималась как передразнивание. При соблюдении этих условий между людьми (например, между конфидентом и фигурантом) возникает определенное чувство единения, называемое в психологии раппортом. Именно он рождает необходимое доверие [131].

Завоевание доверия является главным подготовительным этапом для последующего разворачивания всех вышеназванных мероприятий по осуществлению PSYOP.

Как видно, эти и некоторые другие проблемные вопросы дают широкий простор и для научных исследований данной сферы ОРД. Разработка «слуховых вирусов» по различным направлениям криминальной деятельности (организованная преступность, наркобизнес, религиозный экстремизм и др.), методика их внедрения в окружение объектов оперативного интереса, выбор психологических методов контроля и управления конкретной ситуацией – вот неполный перечень актуальных тем для теории и практики ОРД.

Кроме того, использование технологий PSYOP автоматически создает далеко идущие перспективы в таком важном и актуальном институте теории и практики ОРД, как оперативно-розыскная психология. К сожалению, приходится констатировать, что в отличие от сегодняшнего дня в советское время она активно изучалась, разрабатывались конкретные методические рекомендации для построения моделей поведения между различными участниками ОРД: оперативниками и конфидентами, конфидентами и фигурантами, оперативниками и фигурантами, оперативниками друг с другом и т.д. Отдельные аспекты оперативно-розыскной психологии дошли до наших дней (в частности, выбор тактических способов ввода конфидентов в оперативную разработку), но целостный подход к этой теме не сохранился. Поэтому вышеизложенные методы НЛП могут стать основой для восстановления и развития этого направления ОРД.

Отсюда понятно, что предлагаемые в настоящем исследовании тезисы в некоторых случаях носят постановочный характер и могут стать темами самостоятельных монографических изысканий.

Таким образом, теория PSYOP имеет далеко идущие перспективы. Перестройка работы оперативных служб на ее принципы в корне поменяет ее характер и придаст новый импульс оперативно-розыскной профилактике как одной из организационно-тактических форм ОРД.

К сожалению, анализируя работу оперативных подразделений ОВД в настоящее время, приходится констатировать, что оперативно-розыскная профилактика сейчас зачастую оказывается невостребованной. Задачи предупреждения и пресечения уголовных правонарушений, регламентированные статьей 2 Закона об ОРД [20], во многом стали носить декларативный характер.

По различным объективным и субъективным обстоятельствам сложилась такая ситуация, что оперативно-розыскная профилактика «выпала» из поля зрения как практических, так и научных работников. Более подробно о данной проблеме высказались К.С. Лакбаев и М.М. Галиханов в ходе участия в Международной научно-практической конференции в г. Москве, посвященной памяти известного ученого – специалиста в сфере ОРД А.Ю. Шумилова. Ими отмечено, что причиной сложившегося положения является ментальная «зацикленность» всей системы уголовной юстиции на количественных статистических цифрах законченных уголовных дел. Это же является показателем оценки деятельности всех правоохранительных и судебных органов. Тем самым сложился традиционный репрессивный подход к противодействию преступности, когда выгоднее дождаться реализации криминального замысла, чем предупредить совершение уголовного правонарушения заблаговременно. Между тем профилактика силами, средствами и методами ОРД является наиболее эффективным инструментом экономии уголовных репрессий, так как может воздействовать на истоки будущих криминальных событий задолго до их формирования. В этой связи вышеуказанными авторами была предложена система оценки результатов оперативно-розыскной профилактики, с упором на качественные критерии [132].

Использование технологий PSYOP способно породить ещё одно перспективное направление – блокирование (остановка) криминальной деятельности. Оно может стать логичным дополнением к двум другим – предупреждению и пресечению; при том, что они, как правило, осуществляются в реактивном режиме. Блокирование же, по определению, изначально предполагает инициативную заблаговременную (проактивную) работу по приостановке криминальной деятельности на различных стадиях с помощью инновационных информационно-психологических методов.

Об этом же говорит и А.С. Овчинский. По его мнению, информационное противоборство в ОРД означает не только выявление преступных замыслов, но и воздействие на них. Решается задача ликвидации криминальных угроз, которые сформировались в информационных сферах или непосредственно в

сознании потенциальных преступников как организаторов или заказчиков преступлений, так и их исполнителей [8, с. 20-21].

Принципиальное отличие блокирования от предупреждения и пресечения состоит в следующем. Если последние начинаются после получения информации о подготавливаемом или совершаемом уголовном правонарушении (пункт 1 статьи 10 Закона об ОРД), то блокирование возможно и на более ранних стадиях. Оно может иметь место после возникновения преступного умысла с целью его приостановки и недоведения до стадии подготовки. Более того, в некоторых случаях блокирование может осуществляться для недопущения формирования и возникновения самого умысла.

Тем самым, теория и практика ОРД ОВД может пополниться еще одним перспективным направлением оперативно-розыскной профилактики, которое имеет собственные предмет исследования и методологию, основывающуюся на рассматриваемом институте PSYOP.

В более широком смысле – это еще один действенный механизм реализации принципа экономии уголовных репрессий, что в конечном счете является одной из целей уголовной политики государства.

Таким образом, основываясь на вышеизложенном, можно попытаться сформулировать понятие «информационно-психологических операции» (PSYOP) в ОРД ОВД, под которыми предлагается понимать совокупность оперативных комбинаций по использованию оперативно-розыскной информации и оказанию скрытого психологического воздействия на объект оперативного интереса и (или) его связи для создания ситуации управляемого хаоса с целью решения задач ОРД.

Таким образом, технологии PSYOP в сочетании с теорией управляемого хаоса могут стать серьёзным инструментом противодействия преступности в Казахстане.

Адаптируя геополитический подход к данной проблеме [133], можно обозначить основные принципы такой деятельности:

– обязательное использование достижений новых информационных технологий;

– комплексное воздействие на всех известных руководителей и участников криминальных групп с целью создания перманентного управленского хаоса;

–формирование «агентов влияния» среди низовых ячеек криминальных структур и вышестоящих уровней, которые будут формировать их планы действий в пользу правоохранительных органов.

Эти и многие другие проблемные вопросы дают широкий простор и для научных исследований данной сферы ОРД. Разработка «слуховых вирусов» по различным направлениям криминальной деятельности, методика их внедрения в окружение объектов оперативного интереса, выбор способов контроля и управления ситуацией – вот неполный перечень актуальных тем для теории и практики ОРД.

Изложенные тезисы во многом носят постановочный характер. Теория PSYOP имеет далеко идущие перспективы. Перестройка работы оперативных служб на ее принципы в корне поменяет ее характер и придаст новый импульс оперативно-розыскной профилактике как одной из организационно-тактических форм ОРД. Появляется еще одно ее возможное направление (наряду с предупреждением и пресечением) – блокирование (затруднение) криминальной деятельности.

В более широком смысле – это еще один действенный механизм реализации принципа экономии уголовных репрессий, что в конечном счете является одной из целей уголовной политики государства [116, с. 26].

Таким образом, обобщая теоретические, организационные и правовые аспекты информационно-психологических операций и теории управляемого хаоса как элементов проактивного подхода к осуществлению ОРМ, можно сделать следующие выводы:

1. Развитие военных технологий информационно-психологических операций дает возможность адаптировать их к правоохранительной сфере для более успешного противодействия преступности.
2. Применение в рамках информационно-психологических операций технологий управляемого хаоса против криминальных структур может стать серьезным инструментом возрождения и развития оперативно-розыскной профилактики.
3. Необходима целевая подготовка сотрудников оперативных подразделений ОВД для использования этих проактивных технологий в своей деятельности, что должно сопровождаться специальной психологической подготовкой.

Эти перспективные методики следует органично дополнять техническими средствами, речь о которых пойдет в следующем подразделе.

§ 2.4 OSINT и БПЛА как инструменты проактивного подхода

Данную проблему Глава государства К.-Ж.К. Токаев поднимал еще в сентябре 2020 года, когда отмечал, что реальность стремительно меняется, и чем больше силовые структуры будут полагаться на передовые методы работы, тем больше у них шансов вписаться в контекст международной практики [135].

Добиться этого можно только за счет глубокого понимания сущности процессов, происходящих в тех сферах, где потенциально возможно возникновение указанных угроз и вызовов. В свою очередь, это достигается инфильтрацией правоохранительных органов в их инфраструктуру, что является основным предназначением ОРД ОВД.

Виды такого проникновения могут быть разными, начиная от негласной деятельности конфиденциальных помощников до применения специальных программных продуктов мониторинга Интернета.

В последние годы, ввиду бурного развития новых информационных технологий и практически поголовного вовлечения населения в цифровую среду, особый интерес представляет такое направление ОРД, как разведка из открытых источников – OSINT (open-source intelligence).

Разведка на основе открытых данных активно применялась еще во время Второй мировой войны в Британии и США: специальные подразделения прослушивали трансляции противника. Ее целью является сбор информации о человеке или организации из открытых источников и ее последующий анализ. Как отмечают специалисты лаборатории Касперского, в настоящее время методы OSINT наиболее активно используются во внешней политике и в сфере информационной безопасности. Так, злоумышленники могут использовать OSINT для выявления перспективных мишеней и слабых мест в защите потенциальной жертвы, подготовки к целевым атакам [136].

Вместе с тем разведка из открытых источников весьма перспективна и в правоохранительной деятельности, так как позволяет получить значимый объем информации об объектах оперативного интереса без осуществления интрузивных (затрагивающих права личности) методов. Соответственно, каких-либо специальных разрешений (санкций) на это не требуется.

Серьезное преимущество дает OSINT при выявлении и проверке лиц и фактов, представляющих оперативный интерес, по линии протестных акций и деструктивной деятельности. Как правило, они не имеют отношения к привычно криминальной среде, и в базах данных ОВД на них ориентирующая информация отсутствует. Но в глобальной сети такие фигуранты обычно проявляют повышенную активность, так как это их основное поле деятельности [137].

В то же время в деятельности оперативных подразделений ОВД методы OSINT применяются не везде и не в полной мере, что обусловлено отсутствием четкой и понятной методологии их проведения. В основном такая работа ограничивается стандартной проверкой глобальной сети с использованием общеизвестных поисковиков, таких как Google, причем на каком-то одном языке (русском или казахском).

На этом фоне более половины (55%) опрошенных сотрудников оперативных подразделений ОВД ответили, что в их практической деятельности даже такая проверка осуществляется редко .

Что касается изученных дел оперативного учета, то там эта доля еще ниже и не превышает 20% .

Однако, OSINT включает в себя гораздо более широкий спектр возможностей.

Например, из открытых источников можно получить сведения о записях в блогах интересующих лиц, социальных сетях и других интернет-сообществах с их участием, а также о доступных Интернет-портах, что представляет значительный оперативный интерес для оперативных подразделений по всем направлениям. Кроме того, там же можно найти интересующую информацию о записях публичных заявлений, докладов,

конференций, статей в специализированных журналах по определенной тематике [136].

Это полезно через призму противодействия деструктивной деятельности на политической или социальной основе.

Мониторинг сети Интернет не ограничивается подразделениями по противодействию экстремизму и терроризму. Аналогичные функции прописаны и для подразделений криминальной полиции, по борьбе с организованной преступностью и по противодействию наркопреступности.

Но для этого нужно разработать и внедрить в работу оперативных подразделений ОВД четкие методики использования специализированных программных продуктов, способных обеспечить получение требуемой информации.

В спектре таких технологий можно выделить Shodan и Thingful.

Shodan – это поисковая система, которая целенаправленно индексирует все подключенные к интернету вычислительные устройства (веб-камеры, маршрутизаторы, серверы, новомодные девайсы для IoT – Интернета вещей и т.д.) и позволяет находить их с помощью различных поисковых запросов и фильтров [138].

Применительно к ОРД ОВД данная программа раскрывает широкие возможности, так как она позволяет найти в сети интернет-устройства, которые используют фигуранты и иные объекты оперативного интереса в открытых сегментах сети.

Аналогичными возможностями обладает программа Thingful. Ее версия Umbrellium осуществляет поиск людей и нахождение их устройств в определенный момент времени с помощью геолокации [139].

Обычно оперативным подразделениям для этого необходимо проведение комплекса специальных ОРМ, которые должны предварительно санкционироваться прокурором, что зачастую представляет сложность с точки зрения обоснования перед ним целесообразности их проведения.

К тому же этот процесс требует определенного времени, что в условиях динамики современных событий часто делает эти СОРМ не актуальными.

Преимуществом таких продуктов является отсутствие необходимости такой бюрократической волокиты, особенно если использовать их будут не оперативные подразделения, а их сетевые звенья в виде журналистов или в будущем частных детективов.

Но есть некоторые специфические особенности при проведении мероприятий с применением подобных программных продуктов.

Во-первых, наиболее эффективные их версии, как правило, являются платными. Эту проблему можно решить за счет использования средств, выделяемых для финансирования ОРД.

Во-вторых, проведение разведки из открытых источников на основе таких информационных технологий требует усиленных мер безопасности, так как серверы и сайты, которые исследуются с помощью Shodan или Thingful, часто содержат вирусы-трояны. Поэтому при работе с ними также

должны использоваться такие методы защиты, как виртуальные машины, прокси-серверы и VPN [139].

Виртуальная машина – это компьютерный файл (обычно его называют образом), который действует как обычный компьютер. Она может работать в качестве отдельной вычислительной среды (часто для запуска другой операционной системы) или даже как целая система, как это часто реализуется на рабочем компьютере, которым пользуются несколько человек. Виртуальная машина отделена от остальной части системы, то есть программное обеспечение виртуальной машины не может вмешиваться в работу операционной системы главного компьютера. Виртуальная машина мало чем отличается от физических компьютеров – ноутбука, смартфона или сервера. У нее есть центральный процессор, память, диски для хранения файлов и возможность подключения к Интернету [140].

Прокси-сервер – это дополнительное звено между пользователем и интернетом. Это посредник, который отделяет его от посещаемого сайта и создает условия, при которых сайт думает, что прокси – это и есть реальный человек. Все за счет того, что прокси подменяет IP-адрес, а трафик проходит через дополнительный сервер, на котором организованы дополнительные механизмы защиты данных [141].

VPN, или виртуальная частная сеть, создает частное сетевое подключение между устройствами с помощью Интернета. Сети VPN используются для безопасной и анонимной передачи данных по публичным сетям. Принцип их работы заключается в маскировании IP-адресов пользователей и шифровании данных, в результате чего пользователи, не имеющие разрешения на получение таких данных, не смогут их прочесть [142].

Таким образом, указанные технологии создают дополнительную защиту от несанкционированного проникновения в компьютер, предназначенный для постоянной работы. Кроме того, это позволяет работать в сети без риска быть идентифицированным со стороны объектов оперативного интереса.

Кроме того, в условиях регулярно возрастающего объема в глобальной сети, невозможно обойтись без специализированных программных продуктов поисковой направленности. Специалисты приводят следующие наиболее подходящие для этого инструменты:

1. Maltego – графический анализ ссылок. Это инструмент OSINT, предназначенный для поиска данных о людях, компаниях. Работает на платформах «Windows», «Linux» и «Mac». Ключевая особенность программы в том, что она определяет соотношения между данными, создает графическое отображение данных [143].

На графиках и диаграммах можно просматривать до 1 млн объектов. «Maltego» автоматизирует поиск, что позволяет пользователям одним кликом выполнить несколько запросов. Поиск ведется среди записей DNS (система доменных имен, которая служит для поиска и идентификации доменов в Интернете), поисковых систем, социальных сетей. После сбора информации приложение формирует связи, которые обнаруживают скрытые

соотношения между именами, адресами e-mail, компаниями, сайтами и пр. Этой программе доверяют многие, потому что «Maltego» предлагает более 58 направлений источников данных из разных областей [144].

2. Cobwebs – набор взаимосвязанных инструментов. Он предлагает четыре программных продукта OSINT с разнообразным функционалом в сфере расследования. Это решение отличается тем, что продукты работают во взаимосвязи между собой, при этом важно исследовать возможности каждого продукта. Платформа позволяет отслеживать онлайн-активность, собирать и анализировать информацию из доступных источников данных. Поисковая система построена на базе искусственного интеллекта для автоматизированных интернет-расследований [145].

Решение для анализа угроз предназначено для извлечения целевых данных посредством алгоритмов машинного обучения искусственного интеллекта. Уникальная технология помогает собирать и анализировать огромные объемы данных для выявления киберугроз в режиме реального времени. Защищенный помощник аналитика. В работе используется браузер «Lynx», обеспечивающий безопасный просмотр для ручного сбора и анализа данных [144, с. 6-12].

3. Phonelnfoga – инструмент OSINT для поиска по номеру телефона. Это продвинутая программа, позволяющая анализировать телефонные номера и собирать нужную информацию. На первом этапе происходит сбор стандартных данных (страна, оператор, тип линии). После этого в поисковых системах специалисты находят след, по которому можно вычислить владельца. Основные возможности «Phonelnfoga»:

– проверка действительности номера телефона;
– сбор стандартной информации;
– выполнение разведки OSINT, используя API, телефонные справочники, Google Hacking и поисковики;
– сканирование группы телефонных номеров [150].

В то же время использование подобных перспективных программ для эффективной OSINT затруднено недостатком бюджетного финансирования. Так, подавляющее большинство опрошенных сотрудников оперативных подразделений ОВД (более 95 %) отметили, что в их службах такие программные продукты не применяются в связи с их отсутствием .

По изученным уголовным делам не представилось возможным установить такую долю в связи с тем, что в их материалах не конкретизируется, какие информационные системы были использованы в ходе расследования . В общей массе могут в основном учитываться факты проверки фигурантов дел по базам данных МВД, что не вполне укладывается в понятие OSINT.

Следует отметить, что OSINT не ограничивается только поиском интересующей информации в глобальной сети. Это лишь ее часть, так называемая пассивная разведка, когда осуществляется сбор необходимых сведений и наблюдение за фигурантами. Есть и активная разведка, когда

помимо этого, с ними устанавливается контакт с целью оказания определенного воздействия [136].

В этом смысле серьезную перспективу для проактивного осуществления ОРМ представляет собой такой элемент новых информационных технологий, как социальная инженерия.

Под ней понимается искусный метод управления психологией человека без использования технических приемов взломов для получения персональной информации или доступа к чему-либо [145, с. 86].

Говоря о социальной инженерии, обычно имеются в виду такие криминальные факты, как интернет-мошенничество, которое широко распространилось в последнее время. Но этот метод может применяться и для более масштабных угроз общественной безопасности. Здесь опять можно возвратиться к событиям января 2022 года и предшествовавшему им периоду.

Как отметил Глава государства К.-Ж.К. Токаев, в этот период сплочённость казахстанского общества методично расшатывалась, в том числе посредством акций протеста, согласно профессионально разработанным сценариям. В этом ряду находятся и беспорядки в Жамбылской области, различные провокации на межэтнической почве и другие конфликты. Конспиративно шла подготовка конкретных исполнителей радикальных мер [34].

Очевидно, что все эти весьма опасные протестные проявления являются итогом целенаправленного воздействия методов социальной инженерии.

В то же время ее феномен не окрашен однозначно в криминальный оттенок. Более того, ее методы можно с успехом использовать в деятельности оперативных подразделений ОВД, прежде всего, в рамках активной разведки из открытых источников.

Как отмечалось выше, она подразумевает установление и поддержание в Интернете зашифрованных контактов с объектами оперативного интереса с целью склонения к нужной линии поведения.

Учитывая, что на текущий момент накоплен значительный объем информации о методах психологического воздействия преступников на своих жертв с применением социальной инженерии, целесообразно обобщить данный опыт и определить наиболее действенные способы. В этом также помогут методики информационно-психологических операций, рассмотренные выше.

Конкретные методики для их применения оперативными подразделениями ОВД зависят от линии работы. По линии противодействия организованной преступности это могут быть модели активности в глобальной сети, отражающие специфику незаконного оборота оружия, нелегальной миграции, наркопреступности и т.п.; по линии деструктивных религиозных течений – процессы рекрутинга новых членов через Интернет; по линии экстремизма на политической почве – выявление и воздействие на очаги формирования протестных настроений.

В этой связи формируется двухступенчатая модель OSINT, предлагаемая к внедрению в деятельность оперативных подразделений ОВД:

1) первая ступень – пассивная разведка из открытых источников, в результате которой выявляются лица и факты, представляющие оперативный интерес;

2) вторая ступень – активная разведка, целью которой будет направленное информационно-психологического воздействие на них (с применением методов социальной инженерии) для снижения или полной нейтрализации преступного потенциала либо протестной активности [137, с. 105].

С учётом сложных процессов, происходящих в политической, социально-экономической и криминальной сферах, именно такие проактивные элементы ОРД ОВД востребованы в настоящее время.

В этом смысле перспективными элементами OSINT являются виртуальная и дополненная реальность, а также их сочетание.

Виртуальная реальность представляет собой подобие окружающего мира, искусственно созданного с помощью технических средств и представленного в цифровой форме. Создаваемые эффекты проецируются на сознание человека и позволяют испытывать ощущения, максимально приближенные к реальным [146].

Дополненная реальность (AR – augmented reality) – это интерактивная версия реальности, обогащенная цифровыми изображениями, звуками и другими сигналами с помощью специальных технологий. AR-системы основаны на трех принципах: объединении цифровой и физической реальности, взаимодействии в реальном времени и точном 3D-разграничении реальных и виртуальных объектов. На основе виртуальной и дополненной реальности созданы технологии смешанной реальности (создает интерактивные цифровые элементы с привязкой к физическим объектам) и расширенной реальности (объединяет все типы технологий, воздействующих на органы чувств) [147].

Технологии виртуальной и дополненной реальности могут дать ощутимый эффект в совокупности с еще одной технологией. Возможно, многие жители Казахстана, особенно крупных городов, обратили внимание на периодически появляющиеся на улицах автомашины с эмблемой Google, которые на небольшой скорости осуществляют мобильную съемку окружающего пейзажа и местных достопримечательностей. Эти фото и записи затем прикрепляются к ресурсам Google карт для наглядной демонстрации той или иной локации. Для их просмотра разработаны различные приложения.

Одно из них – Google Street View позволяет увидеть определенную локацию в объемном масштабе [148].

Естественно, что такими записями охвачена не вся территория городов и не все достопримечательности, но процесс продолжается, и база все время пополняется. В крупных городах видеофиксацией охвачены уже многие локации.

Использование таких технологий будет весьма актуально при подготовке различных ОРМ (наблюдение за фигурантами, подбор возможных мест для конспиративных встреч, задержание с поличным и т.д.).

При этом поиск и нахождение конкретных мест, особенно в урбанизированном ландшафте, можно поручить ИИ, который встроен в технологии виртуальной реальности. Более того, ему можно задать перечень параметров, по которым он сможет выстроить перспективную картину места будущих ОРМ: схему наиболее оптимальных путей подхода и отхода; наличие и расположение камер видеонаблюдения; места возможной стоянки автотранспорта; наиболее подходящие точки для организации наблюдения; степень загруженности дорог в промежутке времени планируемых ОРМ; плотность людского потока в этот период; расположение магазинов, кафе и ресторанов с выходом во двор или в подъезд жилых домов; наличие уличных торговцев и т.д.

Многие из этих важных факторов для подготовки ОРМ можно уже сейчас получить из общедоступного приложения 2ГИС, которое включает в себя геолокацию многих городов Казахстана.

Преимущества таких программных продуктов заключаются в том, что их применение позволяет значительно высвободить ресурсы и время оперативных работников, чтобы использовать их для более важных дел.

Как отмечает А.С. Овчинский, автоматизация такой аналитической работы требует создания поисковых процедур, когда объект поиска находится и идентифицируется в информационном пространстве, например, по его связям и окружению. В аналитической деятельности по выявлению возможных криминальных угроз все в большей мере начинают использоваться алгоритмы инициативной обработки потоков разнородных данных, составляющих оперативно-розыскную информацию [8, с. 28].

Здесь также говорится о насущной необходимости проактивной (упреждающей) работы в сфере аналитической деятельности. Учитывая постоянно возрастающие объемы информации, поступающие в оперативные подразделения ОВД, уже следует прорабатывать вопросы о внедрении в нее ИИ на основе нейросетей для автоматической обработки сведений.

Это большое количество сообщений о преступлениях и правонарушениях, о событиях, им сопутствующих, и о ситуациях, провоцирующих противоправные реакции, бытовые, корыстные или «идейные» преступления. Фоновую информацию составляют заявления граждан, обращающихся со своими проблемами в правоохранительные органы, контролирующие инстанции и службы безопасности. Важнейшим сегментом информации для оперативных аппаратов являются сведения о перемещении лиц на железнодорожном, воздушном, автодорожном, морском и речном транспорте. Наряду с «транспортными» базами данных фоновой информацией при решении оперативных задач являются сведения о лицах, пересекающих границы государства, о потоках мигрантов, об иностранных гражданах, прибывающих на заработки. Не меньший интерес могут представлять данные о денежных переводах, валютных операциях,

коммерческих сделках, изменениях на рынке недвижимости, смене владельцев предприятий, концернов, корпораций. Все большие объемы фоновой информации поступают с многочисленных камер видеонаблюдения [8, с. 28].

В России пропускные пункты на вокзалах и аэропортах крупных городов сейчас оснащают программно-аппаратными комплексами, позволяющими производить идентификацию лиц по биометрическим признакам, например, производить портретную идентификацию на основании имеющихся ресурсов оперативно-розыскной информации. Далее уже можно принимать меры оперативного реагирования для задержания разыскиваемых лиц или включать алгоритмы прогнозирования вероятного развития криминальной ситуации при аналитических исследованиях, направленных на обеспечение безопасности тех или иных массовых мероприятий. Неисчерпаемым источником информации, которая образует «рабочий фон» ОРД, являются сообщения средств массовой информации и сетевые коммуникации. В этом же ряду стоит мониторинг телефонных переговоров и электронных сообщений, радиоэфира, операций и сделок в различных сегментах Интернета [8, с. 29].

В Казахстане объём подобной информации весьма значителен, обработать ее вручную невозможно, поэтому использование новых информационных технологий – веление сегодняшнего дня.

Это же относится и к внедрению последних достижений науки и техники, таких как беспилотные летательные аппараты (БПЛА, дроны, коптеры).

Многие привыкли к тому, что беспилотник – это коптер с электродвигателем, фактически игрушка, которую можно просто купить. В то же время моделисты давно используют и более серьезные аппараты с размахом крыла полтора-два метра и высотой полета в несколько сотен метров, оснащенные двигателями внутреннего сгорания и запасом топлива, который позволяет летать на сотню и более километров по автономной программе. Такие аппараты массово используются и в коммерческих целях. Например, для контроля посевов, для точечного внесения удобрений на поля, для контроля за выпасом домашних животных – сегодня овец уже пасут с помощью дронов. Кроме того, они применяются транспортными, нефтяными компаниями или компаниями электросвязи для контроля за линиями электропередач. В месте старта такого аппарата выставляются координаты места, куда он должен прилететь, ставится датчик, чтобы аппарат держал определенную высоту полета, таймер, чтобы он в определенное время отцепил полезную нагрузку. А такой нагрузкой может быть что угодно: и удобрения, и бомбы [150].

Дроны уже давно используются преступниками как средство для совершения преступлений.

Так, в Великобритании в 2015 году в уголовном деле фигурировал коптер. Грабители перед совершением преступления провели тщательную

рекогносцировку объекта при помощи коптера, оснащённого видеокамерой [150].

В 2017 году летящий из России на территорию Финляндии беспилотник заметили в окрестностях города Лаппеенранта. Позднее представители финской погранслужбы обнаружили недалеко от населенного пункта упавший дрон, к которому был прикреплен пакет с 45 блоками сигарет. В ходе расследования в лесу было обнаружено еще два пакета с 15 блоками. Такая высокотехнологичная контрабанда обусловлена тем, что стоимость сигарет в Финляндии в несколько раз выше, чем в России [151].

В 2016 году в США были зарегистрированы беспилотники, которые могут вооружаться практически любыми видами стрелкового оружия, вплоть до гранатометов весом до 10 кг. Был преодолен главный побочный эффект такого применения – мощная отдача – за счет уникальной системы стабилизации [152].

Весьма опасным оружием кибертеррористов может стать комбинация беспилотного летательного аппарата (дрона) и мобильного самодельного взрывного устройства. В будущем дроны могут быть оснащены генерируемой на борту сетью Wi-Fi, автономной навигацией и иными технологиями, позволяющими обнаруживать и поражать цели без вмешательства человека [153].

В настоящее время в деятельности международных террористических организаций произошли настолько заметные изменения, что не принимать их в расчет нельзя. Технологии террора обогатились прежде всего за счет беспилотных летательных аппаратов [154].

Хотя в Казахстане подобные опасные проявления применения БПЛА еще не регистрировались, но преступления с их использованием уже совершаются.

Так, в начале сентября 2020 года сотрудники павлодарской колонии совместно с военнослужащими Нацгвардии перехватили дрон, который приземлился на территории учреждения. К нему был прикреплен пакет, в котором находилось два сотовых телефона, две сим-карты и шнур для зарядки. В истории тюремной системы Казахстана это был первый случай, когда перехвачен дрон с запрещенными предметами [155].

Определенные меры в этом направлении предпринимаются. В частности, в связи с возрастающей возможностью противоправного использования БПЛА при массовых мероприятиях или нарушения режима содержания в местах изоляции и лишения свободы, в январе 2020 года МВД РК издан приказ, которым установлены нормы оснащения ОВД техническими средствами нейтрализации БПЛА. Так, на отряд специального назначения «Сункар», на каждое подразделение специального назначения «Арлан», на каждый специальный отряд быстрого реагирования и на каждое учреждение уголовно-исполнительной системы должны приобретаться такие средства по 2 комплекта и сроком на 7 лет [156].

Вместе с тем, не отрицая нужности и своевременности таких мер, выскажем мнение, что это лишь одна часть решения проблем, реакция на ее

появление. Такой реактивный подход означает пассивную выжидательную позицию, запоздало реагируя на изменения оперативной обстановки вместо того, чтобы идти в опережающем режиме.

Речь идет о комплексном использовании как средств нейтрализации дронов, так и об использовании самих БПЛА в инициативном (проактивном) режиме, в том числе в ходе осуществления ОРМ.

О состоянии в этой сфере говорят результаты опроса сотрудников оперативных подразделений ОВД. Так, свыше 60% из них либо не встречали факты применения дронов в ОРМ, либо это было иногда. Причем во всех случаях это были мероприятия по розыску без вести пропавших лиц , что подтверждается изучением дел оперативного учета .

При этом возникает ряд вопросов, требующих своего решения.

Прежде всего, это нормативное регулирование применения дронов, начиная от закупки и заканчивая методикой их использования в различных ситуациях. В настоящее время ведомственные приказы МВД по этим вопросам находятся в стадии разработки. Из-за этого практика применения БПЛА (пока отрывочная и субъективная) показывает целый ряд проблемных вопросов.

Например, из-за отсутствия единых стандартов и норм оснащения ими подразделений ОВД в разных регионах приобретаются различные марки и модели с отличающимися техническими данными. Главной целью их использования в настоящее время является наблюдение за массовыми мероприятиями или протестными акциями. Конечно же, основным критерием при их приобретении является стоимость. Однако зачастую характеристики оснащения наиболее доступных дронов не дают наблюдать за интересующими событиями длительное время, либо оптика не позволяет отчетливо идентифицировать участников и интересующих фигурантов.

Аналогичные проблемы возникают при осуществлении мероприятий по розыску без вести пропавших лиц или похищенного скота. Так, в теплое время года тепловизор часто не может определить человека или животное на фоне прогретой земли, а в морозы поиски быстро прекращаются из-за быстрой разрядки аккумуляторов.

Такая практика обусловлена тем, что вопросы использования БПЛА в правоохранительной деятельности в целом и в ОРД ОВД в частности, с учетом их технических характеристик, не исследованы в научном плане [157].

К тому же функционирование БПЛА далеко не везде законодательно урегулировано, потому нельзя точно сказать, будет ли считаться таковым преступление, совершенное частным лицом с помощью дрона, например, слежка. Он может настигнуть человека, где угодно за каким-либо занятием [158].

В этой связи актуально рассмотреть некоторые аспекты правового и организационного обеспечения применения дронов при проведении ОРМ. Прежде всего необходимо проанализировать их перечень, изложенный в

статье 11 Закона РК об ОРД [24], и выделить из них те, в процессе которых использование БПЛА наиболее целесообразно.

Взять, к примеру, такое общее ОРМ, как применение технических средств для получения сведений, не затрагивающих охраняемые законом неприкосновенность частной жизни, жилища, личной и семейной тайны, а также тайну личных вкладов и сбережений, переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений. С точки зрения применения дронов данное ОРМ идентично другому – наблюдению, то есть визуальному контакту с объектом оперативного интереса.

Логично, что основное содержание данных ОРМ при использовании дронов заключается в получении фото- и видеоинформации об этом объекте на протяжении определенного промежутка времени. Кроме того, при подключении навигационной системы дополнительно можно отслеживать его геолокацию.

Заметим, что согласно нормам Закона об ОРД, оба этих ОРМ относятся к общим, то есть не требующим санкции прокурора. Соответственно, их результаты, полученные с использованием БПЛА, вполне легитимны и могут в дальнейшем использоваться как для подготовки следственных действий, так и иных ОРМ.

Однако на практике впоследствии могут возникать серьезные проблемы с точки зрения их законности.

Смоделируем ситуацию. В процессе розыска без вести пропавших лиц в поле зрения видеокамеры коптера случайно попадает эпизод совершения преступления на территории частного дома, огороженного высоким забором (или иной территории, защищаемой конституционными нормами о неприкосновенности жилища). Естественно, что оператор БПЛА начинает концентрироваться на этом. Очевидно, в данном случае имеет место негласный видеоконтроль лица или места, то есть специальное ОРМ, обозначенное в пункте 3 статьи 11 Закона РК об ОРД [24], которое требует санкции прокурора. При этом пункт 7 статьи 12 этого же Закона, регламентирующий последующее получение санкции прокурора, может быть, не применим по следующим основаниям:

– первоначально оно проводилось как общее ОРМ, не требующее санкции;

– в норме речь идет исключительно о тяжких и особо тяжких преступлениях, а также о деяниях, подготавливаемых и совершаемых преступной группой. Таким образом, здесь «выпадают» преступления небольшой и средней тяжести.

Кроме того, подобные ситуации создают для БПЛА уникальную правовую ситуацию, когда одно действие, по существу, может объединять сразу три ОРМ (два общих и одно специальное). И здесь же возникает вопрос: как нормативно урегулировать «переход» из одного режима в другой?

Мы предполагаем, что эта проблема сможет создать серьезные препятствия в процессе использования подобных материалов ОРМ с использованием БПЛА как поводов и оснований для начала досудебного

расследования, согласно статье 184 Уголовно-процессуального кодекса РК. Очевидно, что любой адвокат будет оспаривать такие материалы как полученные незаконным путем, причем его позиция формально будет юридически обоснована.

В дальнейшем, когда дроны широко начнут применяться в деятельности оперативных подразделений ОВД, подобные ситуации могут приобрести массовый характер и способствовать уходу преступников (особенно представителей организованного криминалитета) от ответственности.

С учётом этого, в целях правового урегулирования данной коллизии, предлагается дополнить статью 12 Закона об ОРД пунктом 6-1 следующего содержания:

«В случае возникновения угрозы жизни, здоровью и собственности физических и юридических лиц разрешается применение технических средств для негласного аудио- и(или) видеоконтроля лица или места, с последующим вынесением в течении 12 часов постановления, утвержденного руководителем органа, осуществляющего оперативно-розыскную деятельность, с уведомлением прокурора и последующим получением санкции в течении двадцати четырех часов с момента вынесения постановления» [157, с. 173].

Подобный подход позволит урегулировать возможные правовые коллизии, связанные с использованием БПЛА при осуществлении указанных ОРМ.

Прогнозируя их будущее масштабное использование в оперативно-розыскной практике, также можно с уверенностью предположить их применение при осуществлении и иных ОРМ, обозначенных в Законе об ОРД:

1) поиск и отождествление личности по приметам [24].

Оно может проводиться в форме патрулирования в местах массового скопления людей на культурных мероприятиях, на близлежащих территориях к вокзалам, аэропортам, крупным торговым центрам и т.д. Вместе с тем здесь эффективное применение дронов возможно при выполнении нескольких основных условий: наличие видеоаппаратуры высокого разрешения, бесперебойной сети высокоскоростного обмена данными (к примеру, стандарта 5G), сопряжения с базой данных разыскиваемых лиц и специальной программы распознавания лиц (или иных примет, таких как походка);

2) преследование лица, готовящего, совершающего или совершившего преступление, и его задержание [24].

Данное ОРМ может быть логичным продолжением поиска и отождествления разыскиваемой личности по приметам. Другой вариант – когда установлено местонахождение подозреваемого, начато его преследование и одновременно подключается дрон. Особенно эффективно его применение может быть в массиве частной жилой застройки, при обилии складок местности, относительно невысокой растительности (кустарники, камыши), либо в гористой местности;

3) осуществление с участием понятых личного досмотра задержанных лиц, изъятия находящихся при них вещей и документов, могущих относиться к преступной деятельности, а также досмотра жилых помещений, рабочих и иных мест, досмотра транспортных средств [24].

Здесь БПЛА могут использоваться для визуального обследования высотных зданий и сооружений, где могут проживать или работать задержанные лица;

4) проведение операций по захвату вооруженных преступников [24]. В этом случае методика применения дронов объединяет все вышеприведенные действия.

БПЛА может использоваться и для проведения такого специального ОРМ, как негласное проникновение и (или) обследование места [24]. Очевидно, что необходимость в нем не может возникать спонтанно, как при переходе наблюдения в негласный аудио- или видеоконтроль лица или места. Поэтому применение дронов для этого должно в обязательном порядке санкционироваться прокурором.

Следует также отметить, что для различных ОРМ необходимо подбирать разные виды беспилотников. К примеру, для розыска без вести пропавших лиц и похищенного скота на обширных территориях более всего подходят программируемые БПЛА, или GPS-дроны, которые в автоматическом режиме обследуют их, фиксируя видеоизображение на свой носитель. После возвращения оператор просматривает запись на предмет обнаружения следов разыскиваемых объектов. При этом необходимо учитывать вышеизложенные требования к техническим характеристикам беспилотника (качество видеокамеры и тепловизора, емкость аккумулятора и др.).

Как правило, программируемые БПЛА не особо сложны в управлении, так как основное время они действуют в автономном режиме.

Совсем иные качества дронов необходимы при осуществлении таких ОРМ, как преследование подозреваемых лиц или задержание вооруженных преступников. Здесь наиболее эффективны управляемые беспилотники, или FPV-дроны.

Аббревиатура FPV образована от слов First Person View (вид от первого лица). Такой беспилотник, в отличие от GPS-дронов, рассчитанных на стабилизированную аэросъемку, позволяет вести трансляцию в режиме реального времени с камеры FPV-дрона на монитор, очки или шлем со встроенным приемником. Опытные операторы могут залетать буквально в окна зданий – на данный момент это самые эффективные инструменты разведки позиций противника [159].

Сложность в применении FPV-дронов заключается в том, что ими можно управлять только в ручном режиме. Соответственно, оператор должен овладеть таким навыком и постоянно его поддерживать.

Кроме того, БПЛА требуют регулярного технического обслуживания и ухода для обеспечения их правильной и безопасной работы. Это может быть дорогостоящим, трудоемким и сложным для неопытных пользователей [160].

А значит необходимо ставить их использование в ОРД ОВД на надежную организационную основу. Прежде всего, следует определить наиболее актуальные направления и среднюю потребность их применения по ним. Отсюда рассчитать нормы оснащения беспилотниками подразделений, предусмотрев комплекты запасных элементов питания, оснащение съемным оборудованием оптимального качества – тепловизорами, устройствами сброса грузов (лекарств, продуктов для разыскиваемых в горах и т.д.), камерами с различным разрешением, динамиками (поддержание связи с разысканными).

Параллельно нужно создавать ведомственные программы и методики подготовки специалистов БПЛА с уклоном на специфику отраслевых служб – общеуголовная, организованная, нарко- и киберпреступность, экстремизм и терроризм и т.д.

В соседней России работа по внедрению беспилотной авиации в деятельность правоохранительных органов уже началась. Так, глава МВД России Владимир Колокольцев в октябре 2022 года сообщил, что в центральном аппарате министерства введены должности специалистов по робототехнике и БПЛА [161].

Очевидно, что и робототехника в настоящее время может серьезно повысить эффективность деятельности правоохранительных органов.

Так, оснащенные искусственным интеллектом роботы-полицейские «заступили на службу» в аэропорту Нарита в Японии летом 2022 года. Их высота составляет 1,2 м, внешне они напоминают небольшое транспортное средство. Их искусственный интеллект может мгновенно анализировать изображение, которое фиксируют установленные камеры. Они также оснащены динамиками и могут при необходимости обратиться к пассажирам с той или иной просьбой или призвать к соблюдению порядка [162].

Летом 2023 года после пяти лет испытаний в Сингапуре началось развёртывание парка полицейских роботов. Машины высотой 1,7 м будут применяться для обеспечения кордонов и оповещения прохожих в случае инцидентов – это позволит обеспечить порядок до приезда основных полицейских сил [163].

Подобные тенденции являются велением времени, так как технический прогресс развивается динамично. То, что еще недавно казалось фантастикой, сейчас воплощается в реальность. Это касается и использования дронов в правоохранительной деятельности.

Корпорация Amazon несколько лет назад оформила патент на миниатюрные дроны для патрульных полицейских. Он получил название UAVA (Unmanned Aerial Vehicle Assistant), что переводится как «беспилотный летательный аппарат-ассистент». Дрон-коп будет входить в стандартную полицейскую амуницию патрульного ипо команде будет подниматься в воздух для выполнения его команд. Оснащенный видеокамерой, он сможет заглянуть туда, куда живому сотруднику заходить опасно, и тем самым избавит полицейских от неоправданного риска. Такжедрон сможет участвовать в преследовании преступников: имея

поддержку с воздуха, догнать нарушителя гораздо легче, а сам он, находясь в поле зрения беспилотника, имеет меньше шансов незаметно ускользнуть. Кроме этого, полицейский дрон сможет зависать над улицей или автомобилем, пока патрульный проверяет документы у подозрительных личностей. Безнаказанно совершить нападение на сотрудника правопорядка в таком случае гораздо труднее, ведь видео нападения тут же будет отправлено в полицейский участок [164].

Очевидно, что в этом свете перспективы использования БПЛА в ОРД ОВД имеют серьезный потенциал и способны придать оперативной работе импульс не меньше, чем практика применения специальных технических средств, например, прослушивание телефонных переговоров, внедренная несколько десятилетий назад и давшая резкий скачок в раскрываемости преступлений.

Со временем беспилотники могут стать столь же привычным средством ОРД и войти в реестр признанных научно-технических средств с описанием их тактико-технических характеристик, сферы применения и сроков эксплуатации.

Пока же вопросы, связанные с их широким внедрением в Казахстане, находятся в процессе регулирования.

Реальное число дронов в Казахстане неизвестно, поскольку их ввоз в РК не ограничен. Нет необходимости в разрешении, если вес беспилотника не превышает 250 граммов. Более тяжёлые беспилотники, помимо разрешения, необходимо ещё и поставить на учёт. На август 2022 года в Авиационной администрации было зарегистрировано около 500 аппаратов. Для запуска дрона в густонаселенном районе города или посёлка теперь необходимо пройти обучение. По новым правилам на курсах владельцы беспилотных летательных аппаратов должны изучить структуру воздушного пространства. Также инструкторы объясняют им, как правильно готовиться к полёту. Без обучения получить разрешение на эксплуатацию устройства не получится. Однако есть исключения. Документ не нужен, если съёмку планируется проводить в развлекательных целях и вдали от густонаселённого района. При этом дрон запрещается поднимать выше 50 метров. Если полёт выполнен без документов, его владельцу грозит штраф. Для физических лиц его размер составляет 10 МРП [165].

Нормативно установлены и другие ограничения для беспилотной авиации:

– в контролируемом воздушном пространстве истинная высота (расстояние по вертикали от поверхности земли до высоты полета) планируемого полета не превышает 50 м;

– в неконтролируемом воздушном пространстве истинная высота (расстояние по вертикали от поверхности земли до высоты полета) планируемого полета не превышает 200 м;

– полет выполняется за пределами густонаселенных районов населенных пунктов, в которых расположены многоэтажные жилые здания (микрорайоны, жилые комплексы, жилые массивы, гостиничные комплексы),

административные здания (здания государственных органов, многоэтажные бизнес-центры и офисные помещения), культовые здания (церкви, мечети), государственные учреждения, торговые объекты (торгово-развлекательные центры, рынки, ярмарки), концертные залы, спортивные сооружения, развлекательные сооружения, организации образования, здравоохранения, транспортные сооружения (вокзалы, станции, порты), включая прилегающую к ним открытую территорию;

– полет выполняется за пределами запретных и опасных зон, зон ограничения полетов, зон ограничения полетов беспилотных воздушных судов, зон воздушного пространства для полетов беспилотных воздушных судов;

– маршрут (планируемая траектория) полета проходит за пределами 8 км от контрольной точки аэродрома;

– БПЛА не перевозит грузы, не сбрасывает или не разбрызгивает что-либо во время полета;

– БПЛА не эксплуатируется ближе 50 м по горизонтали от любого человека (за исключением человека, управляющего беспилотным воздушным судном), другого транспортного средства, здания или сооружения во время взлета и посадки;

– БПЛА не эксплуатируется ближе 100 м по горизонтали от любого человека (за исключением человека, управляющего беспилотным воздушным судном), другого транспортного средства, здания или сооружения во время полета;

– БПЛА не эксплуатируется во всех случаях ближе 150 м по горизонтали от массового скопления людей и (или) транспортных средств [165].

Это общие требования, устанавливаемые для гражданских эксплуатантов БПЛА. Что касается сферы правоохранительных органов и специальных служб, то указанные ограничения к ним не относятся, однако такие пользователи должны пройти углубленную подготовку в целях соблюдения мер безопасности в процессе полетов.

Это обусловлено тем, что БПЛА оцениваются как объекты повышенной опасности. Они могут воздействовать на гражданские воздушные суда, перевозящие пассажиров. Если выполняются полеты в районы аэродрома, то попадание дрона в двигатель воздушного судна приведет к серьезным инциденту и, возможно, даже к авиационному происшествию, катастрофе с человеческими жертвами. Плюс беспилотник при любых отказах превращается в камень, который падает с неба с определенным ускорением и может нанести ущерб здоровью граждан. Поэтому в перспективе в Казахстане планируется контролировать дроны через системы дистанционной идентификации [165].

Аналогичный опыт имеется в других странах. Так, Британская ассоциация пилотов (BALPA) отстаивает необходимость программирования дронов по автоограничению воздушного пространства для осуществления полетов. Речь идет об установке на них геоблокировки и GPS-трекеров,

которые содержат координаты тысяч аэропортов по всему миру. Они не позволяют войти в эти районы. Если коптер приближается к границе заблокированной зоны (в радиусе от 2 км от крупного аэропорта), то в автоматическом режиме его высота полета будет ограничена 10 м [167].

Таким образом, использование БПЛА в ОРД ОВД, являясь перспективной технологией противодействия преступности, в то же время требует приложения значительных ресурсов для полноценного внедрения в деятельность оперативных подразделений: организационных, правовых, технологических, методических и обучающих.

Данная проблематика может стать предметом самостоятельного научного исследования.

Таким образом, завершая рассмотрение теоретических, организационных и правовых аспектов новых информационных технологий как сферы реализации проактивного подхода к осуществлению ОРМ ОВД РК, можно сделать следующие выводы:

1. Современный криминальный мир сразу берет на вооружение динамично развивающиеся информационные технологии, опережая правоохранительные органы, действующие в реактивном режиме.

2. Чтобы успешно противодействовать этим процессам, оперативным подразделениям ОВД необходимо перестроить свою работу на проактивный режим и начать активно использовать в своей деятельность аналогичные технологии: OSINT, виртуальная и дополненная реальность, а также их сочетания.

3. Серьезный эффект в этой деятельности способно дать использование различных комбинаций БПЛА, применяемых для выявления, предупреждения и пресечения уголовных правонарушений.

ЗАКЛЮЧЕНИЕ

Проведённое исследование теоретических, организационных и правовых аспектов проактивного подхода к осуществлению ОРМ позволяет сформулировать следующие выводы:

1. Главной проблемой действующей модели деятельности оперативных подразделений ОВД является инерционность и косность мышления подавляющего большинства их руководителей и сотрудников.

Поэтому первоочередной задачей внедрения нового «проактивного» подхода является изменение сложившейся парадигмы за счет широкого обучающего процесса, проводимого как в стенах ведомственных вузов при формировании будущего профессионального ядра, так и в рамках последующей служебной подготовки непосредственно по месту работы.

Другого пути кардинального изменения баланса сил в противодействии современным криминальным формированиям не существует. Уже сейчас оперативные подразделения ОВД серьезно отстают от них не только в техническом обеспечении, но что самое критичное – в мотивации оперативных работников в поиске эффективных методов такого противодействия.

«Корень» системных проблем, исследованных в настоящей монографии, лежит в искаженном понимании на всех уровнях конечных целей ОРД ОВД. Ошибочные критерии оценки деятельности оперативных подразделений ОВД, замкнутость на количественных показателях дел оперативного учета, конфидентов, проведенных ОРМ и т.д., без привязки к их качеству закономерно приводят к «отмиранию» оперативно-розыскной профилактики как одного из центральных институтов теории и практики ОРД. Тем самым вместо устранения причин и условий, способствующих развитию преступности, неосознанно культивируется ее постоянное воспроизводство.

Более того, действующая модель попустительствует безнаказанному существованию особо опасных ее форм, аналогичных ИДМ-преступности.

2. Особую актуальность приобрели экстремистские проявления на почве периодически активизирующейся протестной активности различных слоев населения на различной почве. Опыт показал, что адекватно противодействовать таким процессам можно только за счет опережающей работы, которую может обеспечить «проактивный» подход к организации деятельности оперативных подразделений ОВД.

На это направлены предложенные в настоящем исследовании принципы такого подхода, выработанные с учетом самого зарубежного передового опыта как в сфере правоохранительной службы, так и военного дела.

Структурно «проактивный» подход включает в себя несколько самостоятельных элементов, первым из которых является аналитическая работа, направленная на выявление тенденций развития криминогенных процессов, происходящих на обслуживаемой территории. Здесь требуется отход от формализма при определении информационных потребностей и последующей выработке прогнозных оценок. Следует четко осознавать, что

формализм здесь приведет к неверному формулированию и реализации всех мер реагирования и, следовательно, цель достигнута не будет.

Адекватный прогноз должен дополняться упреждающими мерами по контролю за негативным развитием оперативной обстановке. Изощренные и латентные способы совершения уголовных правонарушений высокоорганизованными криминальными формированиями в большинстве случаев препятствуют принятию к ним мер уголовно-правового реагирования. В этой связи необходимо использовать альтернативные пути, предусматривающие применение иных форм воздействия, в том числе психологического.

Здесь тоже потребуется объемная обучающая программа подготовки руководителей и оперативных работников специфическим методам и приемам, уже имеющимся и успешно используемым правоохранительными органами зарубежных стран.

Одновременно необходимо в корне пересмотреть и нормативно зафиксировать новые критерии оценки работы оперативных подразделений ОВД, основанные на качественных показателях деятельности каждого конкретного сотрудника.

Очевидно, что это потребует серьезной перестройки сознания как руководителей, так и сотрудников оперативных подразделений, что само по себе является сложной задачей. Вместе с тем реалии современной оперативной обстановки наглядно показывают, что стандартные «реактивные» методы противодействия преступности уже не соответствуют уровню существующих и потенциальных вызовов и угроз общественной безопасности Казахстана.

3. Не вызывает сомнений, что формирование будущих схем и моделей криминальной деятельности будет неизбежно включать новые информационные технологии – искусственный интеллект на основе нейросетей, большие данные (Big Data), deepfake и т.д.

Эти технологии уже активно распространяются за рубежом и уже пришли в Казахстан. Логично, что готовиться к их появлению лучше заблаговременно, чтобы успеть выработать организационно-тактические и правовые основы противодействия им.

В этом смысле переход к «проактивной» организации работы оперативных подразделений ОВД создает адекватную модель, когда они будут готовы не только реагировать на них в режиме реального времени, но и опережать за счет применения аналогичных технологий, позволяющих заранее спрогнозировать возможные схемы и способы совершения уголовных правонарушений.

В настоящее время использование искусственного интеллекта на основе нейросетей, технологий больших данных и deepfake может показаться чем-то оторванным от реальной практики оперативных подразделений ОВД. Но динамичное ускорение новых информационных технологий и их использование криминальным миром неизбежно поставят вопросы адекватного противодействия этим процессам.

Поэтому уже сейчас необходимо ставить эти вопросы и пытаться адаптировать свою работу под реалии современной и будущей оперативной обстановки, создавая алгоритмы адаптации к ним привычных ОРМ.

4. Здесь не надо начинать работу «с нуля». В сфере военного дела достаточно давно известны практические рекомендации, которые используют в настоящее время вооруженные силы развитых стран. Эти подходы можно с успехом использовать и в правоохранительной деятельности, изменив их под специфику противодействия преступности, которая в настоящее время все больше приобретает сетевой характер.

Основная идея таких рекомендаций заключается в аналитическом сегментировании структуры криминальных формирований и применении к каждому элементу отдельного метода воздействия. Их спектр может быть широк – от привычного уголовного преследования до психологических операций, от экономических мер до социального реагирования. Рамки подобных «проактивных» шагов ограничены только творческими способностями оперативных работников и их руководителей.

Кроме того, самим оперативным подразделениям ОВД необходимо переходить на сетевую организацию своей деятельности за счет привлечения на горизонтальном уровне к проведению ОРД иных структур, подобных журналистским сообществам.

5. Сформировав собственную сетевую структуру, можно гораздо более успешно реализовывать адресное информационно-психологическое воздействие на интересующих фигурантов и их группировки. Для этого необходимо развивать теоретическую и практическую базу таких целевых операций, вырабатывать организационные и тактические приёмы применительно к конкретным оперативно-розыскным ситуациям.

Применение таких методов требует не только грамотного планирования и анализа, но и тщательного обучения и подготовки сотрудников правоохранительных органов, которое должно включать в себя специализированное обучение сотрудников, разработку строгих этических норм и правил, проведение психологических исследований и оценок рисков. Так как методы PSYOP является новшеством в правоохранительной деятельности, необходимо наладить сотрудничество с экспертами и консультантами, имеющими опыт в области информационно-психологических операций, чтобы обеспечить качественное выполнение поставленных задач [168].

Весьма перспективно использование в информационно-психологических операциях положений теории управляемого хаоса как эффективного метода парализации преступной активности фигурантов. Тем самым их криминальный потенциал можно снизить до нуля временно или навсегда. Это наиболее предпочтительный путь экономии уголовных репрессий, который можно реализовать только в рамках ОРД ОВД.

6. Приметой последнего времени становится возрастающая интеллектуализация преступной деятельности, когда уголовные правонарушения совершаются с применением новых информационных

технологий. Широкое распространение в настоящее время получили кибермошенничество, преступления с использованием «интернета вещей», криптовалют и т.д.

Такая тенденция требует адекватных мер противодействия со стороны оперативных подразделений ОВД. Прежде всего это расширение альтернативных методов сбора оперативно-розыскной информации за счет разведки из открытых источников. Методика подобного сбора известна и широко применяется зарубежными правоохранительными органами и специальными службами – OSINT.

Вместе с тем разведка из открытых источников оперативными подразделениями ОВД РК вынужденно осуществляется в сильно урезанном виде ввиду отсутствия финансирования для приобретения специализированных программ сбора и систематизации данных.

Тем не менее необходимо последовательно двигаться к повсеместному внедрению OSINT и разработке чётких алгоритмов её осуществления.

То же самое относится и к использованию при проведении ОРМ БПЛА. Эта сфера пока не обеспечена ни в правовом, ни в организационном, ни в тактическом плане, поэтому внесенные предложения призваны в значительной степени восполнить эти пробелы.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Мы извлекли необходимые уроки – Президент Казахстана о январских событиях (8 января 2023 года) // https://www.inform.kz/ru/my-izvlekli-neobhodimye-uroki-prezident-kazahstana-o-yanvarskih-sobytiyah_a (13.03.2026).
2. Международная платформа действий ООН в целях выполнения Протокола действий о предупреждении и пресечении торговли людьми // https://www.unodc.org/documents/human-trafficking/TIP_Framework_ (13.03.2026).
3. Президент Республики Казахстан К.-Ж.К. Токаев. Справедливое государство. Единая нация. Благополучное общество: послание народу Казахстана // https://www.akorda.kz/ru/poslanie-glavy-gosudarstva (13.03.2026).
4. Каримова Д. Цифровая карта бизнеса и искусственный интеллект – какое будущее ждет Казахстан // https://lsm.kz/tokaev-poruchil-maksimal-no-razvivat-iskusstvennyj-intellekt (13.03.2026).
5. Токаев К.-Ж.К. обвинил отдельных руководителей спецслужб Казахстана в измене долгу // https://www.interfax.ru/world/814702 (13.03.2026).
6. Мусин А.Б. Переход от «реактивной» к «проактивной» модели организации деятельности оперативных подразделений органов внутренних дел // Ғылым – Наука. – 2023. – №3(77). – С. 160-166.
7. Овчинский С.С., Христюк А.В. Приоритетные направления разработки оперативно-розыскной тактики борьбы с организованными преступными группами // Совершенствование деятельности оперативных аппаратов органов внутренних дел в борьбе с опасными проявлениями групповой преступности: сб. науч. тр. – Хабаровск, 1990. – С. 3-15.
8. Овчинский А.С. Оперативно-розыскная аналитика (ответ современным угрозам): монография / Овчинский А.С. – М.: ИД Шумиловой И.И., 2015. – 108 с.
9. УБОП вернут в Казахстане // https://tengrinews.kz (13.03.2026).
10. Глава ДБОП рассказал о воровских сходках, коронации авторитетов и заказных убийствах в РК // https://orda.kz/glava-dbop-rasskazal (13.03.2026).
11. 40 человек задержали в ходе крупной спецоперации в Карагандинской области // https://tengrinews.kz/kazakhstan_news/40-zaderjali-hode (13.03.2026).
12. Латов Ю.В. Экономика вне закона: очерки по теории и истории теневой экономики / Латов Ю.В. – М., 2001. – 284 с.
13. де Сото Э. Иной путь. Невидимая революция в третьем мире / пер. с англ. – М.: Catallaxy, 1995. – 320 с.
14. Бормашенко Э. Мафия: проявленный негатив // Знание – сила. – 1994. – №9. – С. 3-9.
15. Члены экстремистских организаций участвовали в погромах в Казахстане – госсекретарь // https://tengrinews.kz/kazakhstan_news (13.03.2026).

16. Абжекенова Н. На «Хоргосе» «потерялось» 5 млрд. долларов // https://www.caravan.kz/articles/na-khorgose-poteryalos-5-milliardov (13.03.2026).
17. ОПГ Бергея Рыскалиева действовала с момента его назначения на пост акима – гособвинение // https://prg.kz/document/?doc_id=31498579&utm_source=chatgpt.com (13.03.2026).
18. Приговор Бергею Рыскалиеву вынесли в Атырау // https://tengrinews.kz/events/prigovor-bergeyu-ryiskalievu-vyinesli-v (13.03.2026).
19. Сатаева А. Суд приговорил Тохтара Тулешова к 21 году лишения свободы // https://tengrinews.kz/kazakhstan_news/sud-prigovoril (13.03.2026).
20. Основные элементы организации оперативно-розыскной деятельности // https://student-servis.ru/spravochnik/osnovnye-elementy-organizatsii (13.03.2026).
21. Телицын Н.А. К вопросу о формировании понятия оперативного обслуживания объектов и линий работы в деятельности оперативных подразделений органов внутренних дел: исторический и сущностный аспекты // Вестник Белгородского юридического института МВД России им. И.Д. Путилина. – 2022. – №1. – С. 62-68.
22. Калашников К.В. Сущность и понятие оперативного обслуживания объектов (сфер, территорий) // Право и государство: теория и практика. – 2019. – №6(174). – С. 137-140.
23. Галушко В.А., Половников О.Г. Правовой аспект оперативного обслуживания территорий и объектов подразделениями уголовного розыска // Актуальные проблемы раскрытия и расследования преступлений: сб. науч. тр. – Омск, 2013. – Вып. 11. – С. 83-84.
24. Закон Республики Казахстан. Об оперативно-розыскной деятельности: принят 15 сентября 1994 года, №154-XIII // https://adilet.zan.kz/rus/docs/Z940004000_ (13.03.2026).
25. Галиханов М.М. Проблемы правовой регламентации инициативного характера оперативно-розыскной деятельности // Организация и деятельность органов внутренних дел на современном этапе: проблемы и пути решения: матер. междунар. науч.-практ. конф., посв. 30-летию Независимости Республики Казахстан. – Костанай, 2021. – С. 143-148.
26. Приказ Министра внутренних дел Республики Казахстан. Об утверждении системы критериев оценки деятельности полиции: утв. 4 июня 2019 года, №515 // https://online.zakon.kz/Document/?doc_id (13.03.2026).
27. Курс лекций по дисциплине «Основы управления в органах внутренних дел» / сост. А.Н. Медведева. – Костанай, 2021. – 340 с.
28. Бектлеева Д. Преступность как индикатор качества жизни // https://economy.kz/ru/Mnenija/id=178 (13.03.2026).
29. Экс-советник Назарбаева обвинил спецслужбы Казахстана в предательстве // https://www.rbc.ru/politics/07/01/2022 (13.03.2026).

30. Информационный сервис Комитета правовой статистики и специальных учетов Генеральной прокуратуры Республики Казахстан // https://www.qamqor.gov.kz/portal/page/portal/POPageGroup/Services (13.03.2026).
31. Тусупбеков К.Р. Правовой аспект оперативно-розыскной деятельности органов внутренних дел в борьбе с религиозным экстремизмом // Наука и жизнь Казахстана. – 2018. – №4(62). – С. 66-69.
32. Как действовала группа Дикого Армана во время январских беспорядков – Генпрокуратура // https://ru.sputnik.kz/20220620/kak-deystvovala-gruppa-dikogo-armana-vo-vremya-ya (13.03.2026).
33. Российская разведка знала о подготовке беспорядков в Казахстане // https://lenta.ru/news/2022/02/10/narishkinznal/ (13.03.2026).
34. Выступление Главы государства К.-Ж.К. Токаева на заседании Мажилиса Парламента Республики Казахстан «Уроки «трагического января»: единство общества – гарантия независимости» // https://www.akorda.kz/ru/vystuplenie-glavy-gosudarstva-kk-tokaeva-na (13.03.2026).
35. Николаев О.Э. Оперативно-розыскное прогнозирование как один из факторов повышения эффективности оперативно-розыскной деятельности // Юридическая наука. – 2019. – №7. – С. 74-77.
36. Что такое реактивность и проактивность // https://www.itexpert.ru/rus/ITEMS/200810062247/ (13.03.2026).
37. Овчинский А.С. Информационно-психологическая сфера противодействия организованной преступности // https://emag.iis.ru/arc/infosoc/emag.nsf/BPA/2405d357bee499fdc32575be00257650 (13.03.2026).
38. В Минэнерго объяснили рост цен на газ // https://kapital.kz/economic/101629/v-min-energo-ob-yasnili-rost-tsen (13.03.2026).
39. Жанаозен Мангыстауской области. Две стороны медали // https://online.zakon.kz/Document/?doc_id=31059060&pos=4;-70#pos (13.03.2026).
40. «Темная сторона» Интернета. Шпионский скандал вызвал всплеск интереса к анонимным сетям // https://korrespondent.net/business/1583897-temnaya-storona-interneta-shpionskij- (13.03.2026).
41. Витовская Е.С. К вопросу о противодействии преступлениям наркотической направленности, связанным с использованием компьютерных средств // Уголовно-процессуальные и криминалистические чтения на Алтае: проблемы и перспективы противодействия преступлениям, совершаемым с применением информационных технологий: сб. науч. ст. – Барнаул, 2018. – Вып. 15. – С. 58-59.
42. Очень темные дела // https://tgraph.io/Ochen-tyomnye-dela-04-27 (13.03.2026).
43. Иванов А. Даркнет наводняет украденное у ВСУ оружие: разбираемся, сколько оно стоит и когда Европа утонет в крови? //

https://fishki.net/anti/4158989-darknet-navodnjaet-ukradennoe-u-vsu (13.03.2026).

44. Бабаев М.М., Пудовочкин Ю.Е. Феномен риска в контексте профилактической политики (криминальная рискология) // Вестник Санкт-Петербургского университета. – 2019. – №1. – С. 144-145.

45. Бьюкенен Дж. Защита организованной преступности? // https://godfather.moy.su/publ/19-1-0-110 (13.03.2026).

46. Schelling T.C. Economic Analysis and Organized Crime: appendix // In book: Task Force Report: Organized Crime. Annotations and Consultants Paper. Washington, 1967. – P. 114-122.

47. Мусин А.Б. Сущность проактивного подхода к организации оперативно-розыскной деятельности органов внутренних дел // Ғылым – Наука. – 2024. – №4(83). – С. 192-197.

48. Оперативно-розыскная деятельность. – Изд. 2-е, перер. и доп. / под ред. К.К. Горяинова, В.С. Овчинского, Г.К. Синилова. – М., 2004. – 848 с.

49. Кваша Ю.Ф., Матвеев С.Е., Сурков К.В. Оперативно-розыскная деятельность органов внутренних дел: словарь-справоч / Кваша Ю.Ф., Матвеев С.Е., Сурков К.В. – Новгород; М., 1998. – 132 с.

50. Меретуков Г.М., Лунина Е.С., Бирюкова С.Н. Правовые основы поисковой деятельности подразделений, осуществляющих оперативно-розыскную деятельность // Научный журнал КубГАУ. – 2016. – №117. – С. 234-250.

51. Легостаев В.П. Некоторые проблемы определения понятия оперативно-розыскных мероприятий // https://cyberleninka.ru/article/n/nekotorye-problemy-opredeleniya-ponyatiya-operativno-rozysknyh-meropriyatiy (13.03.2026).

52. Шаймуханов А.Д. Размышления о понятии и сущности современного оперативно-розыскного законодательства Республики Казахстан // Вестник Уральского института экономики, управления и права. – 2009. – №3(8). – С. 23-26.

53. Лакбаев К.С. Теоретические и прикладные проблемы правоотношений в оперативно-розыскной деятельности органов внутренних дел Республики Казахстан: дис. … док. юрид. наук / Лакбаев К.С. – Караганда, 2008. – 254 с.

54. Сысалов М.П. Основы оперативно-розыскной деятельности: учеб / Сысалов М.П. – Алматы: Юридическая литература, 2006. – 338 с.

55. Карымсаков Р.Ш., Дусанбекова М.А. Некоторые вопросы прокурорского надзора и контроля за оперативно-розыскной и контрразведывательной деятельностью // https://online.zakon.kz/Document/?doc_id=31641537 (13.03.2026).

56. Классификация поколения войн // http://militera.lib.ru (13.03.2026).

57. Ситнова И.В. Информационно-психологическое воздействие как практика ведения войн четвертого поколения // Власть. – 2018. – №7. – С. 70-75.

58. Аванесов Г.А. Теория и методология криминологического прогнозирования / Аванесов Г.А. – М.: Юрид. лит., 1972. – 334 с.
59. Клейменов М.П. Криминология: учеб / Клейменов М.П. – М.: Норма, 2011. – 448 с.
60. Лунеев В.В. Курс мировой и российской криминологии. Общая часть: учеб / Лунеев В.В. – М.: Юрайт, 2011. – 1003 с.
61. Криминология / под ред. В.Н. Кудрявцева, В.Е. Эминова. – М.: Норма: Инфра-М, 2010. – 800 с.
62. Белкин Р.С. Криминалистика: проблемы сегодняшнего дня. Злободневные вопросы российской криминалистики / Белкин Р.С. – М., 2001. – 240 с.
63. Бугаев К.В. Методология криминалистического прогнозирования (на примере экспертных подразделений ОВД) // Научный вестник Омской академии МВД России. – 2011. – №2(41). – С. 37-42.
64. Васильев А.Н., Яблоков Н.П. Предмет, система и теоретические основы криминалистики: монография / Васильев А.Н., Яблоков Н.П. – М., 1984. – 143 с.
65. Криминалистика / под ред. А.Ф. Волынского, В.П. Лаврова. – Изд. 2-е, перер. и доп. – М., 2015. – 943 с.
66. Литвинов А.Н., Степанюк Р.Л. Прогнозирование и планирование в криминалистике / Литвинов А.Н., Степанюк Р.Л. – М., 2004. – 160 с.
67. Исиченко А.П. Оперативно-розыскная криминология: понятие, объект и предмет // Научный портал МВД России. – 2017. – №4(40). – С. 76-79.
68. Селиванов А.И., Стрельников К.А., Царегородцев И.Ю. Теоретические основы прогнозирования в оперативно-розыскной деятельности // Вестник Академии экономической безопасности МВД России. – 2011. – №2. С. 60-69.
69. Плэтт В. Информационная работа стратегической разведки. Основные принципы // https://coollib.com/b/174077/read (13.03.2026).
70. Беспорядки в Кордае: троим участникам вынесли приговор // https://tengrinews.kz/kazakhstan_news/besporyadki-v-kordae-troim (13.03.2026).
71. Тепляков С.В. Перспективные инновации в МВД России // Актуальные исследования. – 2021. – №4(31). – С. 15-17.
72. Васильев А.П., Абрамов А.Х. Искусственный интеллект на основе нейронных сетей // Academy. – 2018. – №5(32). – С. 15-17.
73. Что такое нейросети и для чего они нужны // https://iks.ru/news/nejroseti-i-dlya-chego-oni-nuzhny (13.03.2026).
74. Закон Республики Казахстан. Об информатизации: принят 24 ноября 2015 года, №418-V // https://online.zakon.kz/Document/?doc_id (13.03.2026).
75. Назван планируемый оператор казахстанской национальной платформы искусственного интеллекта // https://kaztag.kz/ru/news/nazvan-planiruemyy-operator-kazakhstanskoy-natsionalno (13.03.2026).

76. Об искусственном интеллекте: Закон Республики Казахстан от 17 ноября 2025 года № 230-VIII ЗРК // https://adilet.zan.kz/rus/docs/Z2500000230 (30.03.2026).
77. Цифровой кодекс Республики Казахстан: Кодекс Республики Казахстан от 9 января 2026 года № 255-VIII ЗРК // https://adilet.zan.kz/rus/docs/K2600000255 (30.03.2026).
78. Соколова А. Что такое дипфейк. Объясняем простыми словами // https://secretmag.ru/enciklopediya/chto-takoe-dipfeik-obyasnyaem (13.03.2026).
79. Нейросети: как искусственный интеллект помогает в бизнесе и жизни // https://habr.com/ru/post/337870/ (13.03.2026).
80. Ларина Е.С., Овчинский В.С. Кибервойны XXI века: о чем умолчал Эдвард Сноуден / Ларина Е.С., Овчинский В.С. – М.: Книжный мир, 2014. – 352 с.
81. Макаренко С.И. Информационное противоборство и радиоэлектронная борьба в сетецентрических войнах начала XXI века: монография / Макаренко С.И. – СПб.: Наукоемкие технологии, 2017. – 546 с.
82. ChatGPT и друзья: лучшие чат-боты с искусственным интеллектом в 2023 году // https://eternalhost.net/blog/tehnologii/chat-boty-s (13.03.2026).
83. Макаренко С.И., Иванов М.С. Сетецентрическая война – принципы, технологии, примеры и перспективы / Макаренко С.И., Иванов М.С. – СПб., 2018. – 900 с.
84. Указ Президента Республики Казахстан. Об утверждении Концепции правовой политики Республики Казахстан до 2030 года: утв. 15 октября 2021 года, №674 // https://adilet.zan.kz/rus/docs/U2100000674 (13.03.2026).
85. Мусин А.Б. Проактивный подход в оперативно-розыскном прогнозировании // Организация и деятельность органов внутренних дел на современном этапе: проблемы и пути решения: матер. междунар. науч.-практ. конф. – Костанай, 2025. – С. 187-188.
86. Числов А.И., Юзиханова Э.Г. Основы оперативно-тактического прогнозирования // Юридическая наука и правоохранительная практика. – 2012. – №1(19). – С. 92-96.
87. Виды оперативно-тактического прогнозирования // https://all-sci.net/rozyisknaya-deyatelnost-operativno/vidyi-operativno (13.03.2026).
88. Шалбаев А.Ш. О понятии криминальных рисков в оперативно-розыскной деятельности органов внутренних дел Республики Казахстан // Вестник Карагандинской академии МВД РК им. Б. Бейсенова. – 2023. – №1(79). – С. 262-266.
89. Жизнестойкость транснациональных организованных преступных группировок // Борьба с преступностью за рубежом (по материалам зарубежной печати): ежемесяч. информ. бюл. – 2017. – №12. – С. 3-5.
90. Гриняев С.Н. Поле битвы – киберпространство: теория, приемы, средства, методы и системы ведения информационной войны / Гриняев С.Н. – М., 2004. – 426 с.

91. Григорьев В.Р., Шуркин Л.О. Сетецентрические войны с позиции синергетики // Вестник РГТУ. – 2014. – №11(133). – С. 67-100.
92. Мусин А.Б. Сетевой характер современной преступности и перспективные подходы противодействия ей // Вестник Карагандинской академии МВД РК им. Б. Бейсенова. – 2023. – №4(82). – С. 307-313.
93. Самые громкие теракты в истории современного Казахстана // https://www.ktk.kz/ru/news/video/2016/06/06/69931/ (13.03.2026).
94. Приговоренный к 20 годам тюрьмы «Солдат Халифата». Кто он? // https://rus.azattyq.org/a/kazakhstan_terrorist_znaliev_atyrau/28701245 (13.03.2026).
95. Warden J.A. The Air Campaign: Planning for Combat. – Boston, 2011. – 224 p.
96. P.Willians. Особенности многонациональных сетей незаконной наркоторговли // Борьба с преступностью за рубежом: ежемесячный информационный бюллетень (по материалам зарубежной печати). – 1999. – №6. – С. 7-13.
97. Арзуманян Р.В. Кромка Хаоса. Сложное мышление и сеть: парадигма нелинейности и среда безопасности XXI века / Арзуманян Р.В. – М.: Регнум, 2012. – 600 с.
98. О регистрации граждан в качестве общественных помощников: ответ Министра внутренних дел РК от 17 августа 2019 года на вопрос от 26 июля 2019 года №560392 // https://online.zakon.kz/Document/?doc_id (13.03.2026).
99. Закон Республики Казахстан. Об участии граждан в обеспечении общественного порядка: принят 9 июля 2004 года, №590-II // https://online.zakon.kz/Document/?doc_id=1049312&pos=18 (13.03.2026).
100. Сидоров К. «Не забудем, не простим»: хакеры Anonymous – кто они и чем знамениты // https://digitalocean.ru/n/ne-zabudem-ne-prostim (13.03.2026).
101. Борьба с черными рынками интернета больше не обречена на провал / Союз спецслужб и анархистов // https://vz.ru/society/2017/5/10/869595.html (13.03.2026).
102. Очень темные дела // https://tgraph.io/Ochen-tyomnye-dela-04-27 (13.03.2026).
103. Open Briefing // https://wp.wiki-wiki.ru/wp/index.php (13.03.2026).
104. Сысоев А.К. Организационные и правовые основы деятельности оперативных аппаратов органов внутренних дел Республики Казахстан по противодействию преступлениям в сфере высоких технологий: дис. … док. PhD / Сысоев А.К. – Караганда, 2020. – 176 с.
105. Мусин А.Б., Айтуарова А.Б. Применение принципа сетецентризма в оперативно-розыскной деятельности органов внутренних дел Республики Казахстан // Хабаршы Академии КНБ Республики Казахстан. – Алматы, 2024. – №3(49). – С. 18-27.

106. Муминов А. Вас не снимают скрытой камерой. Частным детективам запретят даже то, что можно другим // https://online.zakon.kz (13.03.2026).
107. Чернов И. Почему в Казахстане частный детектив вне закона // https://ratel.kz/outlook/pochemu_v_kazahstane_chastnyj_detektiv_vne_ (13.03.2026).
108. Закон Российской Федерации. О частной детективной и охранной деятельности в Российской Федерации: принят 11 февраля 1992 г., №2487-1 // https://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n (13.03.2026).
109. Закон Кыргызской Республики. О частной детективной и охранной деятельности в Кыргызской Республике: принят 1 июля 1996 года, №35 // http://cbd.minjust.gov.kg/act/view/ru-ru/642 (13.03.2026).
110. Мурат Т. Новая военная доктрина Казахстана простыми словами: что значит увеличить боевой потенциал, что такое проактивная защита, ИПСО и зачем нужны кибер-войска // https://www.caviral.com/v-kazahstane (13.03.2026).
111. Протесты в Казахстане // https://ru.wikipedia.org/wiki/Протесты_в_Казахстане_(2022) (13.03.2026).
112. Касюк А.Я. Информационно-психологические операции: история и современность // Вестник МГЛУ. – 2018. – №1(794). – С. 26-39.
113. Израиль и пропаганда: как проигрываются информационные войны // https://sevastopol.su/news/izrail-i-propaganda-kak-proigryvayutsya (13.03.2026).
114. Рудаков А.Б. Организация информационно-психологического противоборства криминальным сообществам и террористическим организациям // Общество и государство. – 2025. – №1(49). – С. 26-29.
115. Сунь-Цзы. Трактат о военном искусстве // http://loveread.ec/read_book.php?id=63682&p=14 (13.03.2026).
116. Лакбаев К.С., Мусин А.Б. Применение проактивных информационно-психологических технологий в практике оперативно-розыскной деятельности // Шумиловские чтения: сб. матер. междунар. науч.-практ. конф. – М., 2023. – С. 21-27.
117. Караяни А.Г. Информационно-психологическое противоборство в современной войне // http://armyrus.ru/index.php?option=com_ (13.03.2026).
118. Микрюков В. Победа в войне должна быть достигнута еще до первого выстрела // http://nvo.ng.ru/concepts/2016-01-15/10_infowar (13.03.2026).
119. Крысько В.Г. Секреты психологической войны (цели, задачи, методы, формы, опыт) / Крысько В.Г. – Минск: Харвест, 1999. – 448 с.
120. Информационный фронт Первой мировой войны // В кн.: Первая мировая война 1914-1918 годов / под ред. С.К. Шойгу. – М.: Кучково поле, 2017. – Т. 6. – С. 257-289.
121. Лайнбарджер П. Психологическая война. – М.: Воениздат, 1962. – 352 с.

122. Кириченко А.В. Информационно-психологические войны: современные тенденции и технологические возможности // Акмеология. – 2015. – №4. – С. 210-215.
123. Костюхин А., Горбунов Г., Сажин А. Информационные операции в планах ВС США // http://pentagonus.ru/publ/22-1-0-181 (13.03.2026).
124. Тертеров Г. Информационные операции: история и современность // 21-й век. – 2015. – №3(36). – С. 40-49.
125. Сундиев И.Ю., Смирнов А.А. Сетевые возможности и сетевые угрозы: информационные сети в экстремистской и террористической деятельности // Свободная мысль. – 2013. – №5(164). – С. 191-204.
126. Army of Fake Social Media Friends to Promote Propaganda // https://www.computerworld.com/article/2470594/army-of-fake-social (13.03.2026).
127. Манн С. Теория хаоса и стратегическое мышление // https://www.litmir.me/br/?b=280018&p=4 (13.03.2026).
128. Бартош А. Цель и механизмы модели управляемого хаоса // https://nvo.ng.ru/concepts/2013-09-27/6_chaos.html (13.03.2026).
129. Что такое Deepfake: 10 лучших приложений для создания дипфейков // https://blog.eldorado.ru/publications/chto-takoe-deepfake-10 (13.03.2026).
130. О. Коннер Дж., Сеймор Дж. Введение в нейролингвистическое программирование. Как понимать людей и как оказывать влияние на людей / пер. с англ. – Челябинск, 1198. – 280 с.
131. Михаил Пелехатый // https://institutnlp.ru/about/trainers (13.03.2026).
132. Спирица Е., Пелехатый М. Боевое НЛП: техники и модели скрытых манипуляций и защиты от них. – СПБ.: Питер, 2020. – 157 с.
133. Лакбаев К.С., Галиханов М.М. Еще раз об оперативно-розыскной профилактике // Шумиловские чтения – 2022: науч. тр. по матер. междунар. науч.-практ. конф. – М., 2022. – С. 30-35.
134. Митрошенков О.А. Теория управляемого хаоса: использовать себе во благо // Власть. – 2017. – №08. – С. 64-73.
135. Президент Республики Казахстан К.-Ж. Токаев. Казахстан в новой реальности: время действий: послание народу Казахстана // https://baiterek.gov.kz/ru/president-messages/poslanie-glavy (13.03.2026).
136. OSINT // https://encyclopedia.kaspersky.ru/glossary/osint/ (13.03.2026).
137. Мусин А.Б. Разведка из открытых источников как элемент проактивного подхода к противодействию преступности // Преступность XXI века: теория и практика противодействия: матер. 1-й междунар. науч.-практ. конф. – М., 2023. – С. 102-110.
138. Сито для интернета: интересные вещи с Shodan // https://habr.com/ru/companies/ruvds/articles/533890/ (13.03.2026).
139. Thingful // https://haque-co-uk.translate.goog/work (13.03.2026).
140. Что такое виртуальная машина? // https://azure.microsoft.com/ru-ru/resources/cloud-computing-dictionary/what-is-a-virtual-machine (13.03.2026).

141. Что такое прокси-сервер, зачем он нужен и как его настроить // https://timeweb.com/ru/community/articles/chto-takoe-proksi-server (13.03.2026).
142. Что такое VPN // https://aws.amazon.com/ru/what-is/vpn/ (13.03.2026).
143. Топ-10 лучших инструментов OSINT для разведки с открытым исходным кодом // https://softlist.com.ua/articles/top-10-luchshykh (13.03.2026).
144. Дворянкин О.А. OSINT, PENTEST и НЕТСТАЛКИНГ – информационные технологии Интернета // Национальная ассоциация ученых. – 2022. – №84. – С. 6-13.
145. Созаев С.С., Кунашев Д.А. Социальная инженерия, её техники и методы противодействия // Вестник науки. – 2020. – Т. 1, №2(23). – С. 85-88.
146. Виртуальная реальность. Virtual Reality (VR) // https://www.tadviser.ru/index.php(VR,_Virtual_Reality) (13.03.2026).
147. Что такое дополненная реальность, или AR? // https://dynamics.microsoft.com/ru-ru/mixed-reality/guides/what/ (13.03.2026).
148. Google карты // https://www.google.com/intl/ru/streetview/ (13.03.2026).
149. Атака дронов на Хмеймим заставила задуматься о новом виде терактов // https://www.mk.ru/politics/2018/01/09/ataka-dronov (13.03.2026).
150. Коптеры как инструмент грабителей // https://habr.com/ru/post/401205/ (13.03.2026).
151. Российские контрабандисты с помощью дронов доставляли сигареты в Финляндию // https://versia.ru/rossijskie-kontrabandisty-s (13.03.2026).
152. Стреляющие дроны // https://www.youtube.com (13.03.2026).
153. Шмидт Э., Коэн Д. Новый цифровой мир. Как технологии меняют жизнь людей, модели бизнеса и понятие государств / пер. с англ. – М., 2013. – 510 с.
154. Тепляков С.В. Перспективные инновации в МВД России // Актуальные исследования. – 2021. – №4(31). – С. 15-17.
155. Квадрокоптер использовали в качестве курьера в казахстанскую колонию // https://diapazon.kz/news/103427-kvadrokopter-ispolzovali (13.03.2026).
156. Приказ Министра внутренних дел Республики Казахстан. Об утверждении натуральных норм оснащения органов внутренних дел Республики Казахстан техническими средствами нейтрализации беспилотных летательных аппаратов: утв. 15 января 2020 года, №20 // https://adilet.zan.kz/rus/docs/V2000019903 (13.03.2026).
157. Мусин А.Б. Перспективы использования беспилотных летательных аппаратов в оперативно-розыскной деятельности органов внутренних дел // Ғылым – Наука. – 2024. – №1(80). – С. 169-175.
158. Будущее преступлений // https://apparat.cc/world/future-of-crime/ (13.03.2026).

159. Что такое FPV-дроны? // https://aif.ru/techno/gadgets/chto_ (13.03.2026).
160. Что такое дрон? Как он летает? Типы, плюсы и минусы // https://www.propelrc.com/ru/как-работают-беспилотники (13.03.2026).
161. В МВД РФ сообщили о введении должностей специалистов по робототехнике и БПЛА // https://www.gazeta.ru/army/news/2021/08/11/16369340.shtml (13.03.2026).
162. Роботы-полицейские с ИИ «заступили на службу» в японском аэропорту // https://iz.ru/1349156/2022-06-14/roboty-politceiskie-s-ii (13.03.2026).
163. Сингапур начнут патрулировать полицейские роботы // https://3dnews.ru/1088526/singapur-nachnut-patrulirovat-politseyskie (13.03.2026).
164. Полиция будущего: расследование и предотвращение преступлений // https://naked-science.ru/article/nakedscience/policiya-budushchego (13.03.2026).
165. О новых правилах использования дронов // https://24.kz/ru/news/polezno-znat/item/557610-o-novykh-pravilakh (13.03.2026).
166. Приказ и.о. Министра индустрии и инфраструктурного развития Республики Казахстан. Об утверждении Правил использования беспилотных авиационных систем в воздушном пространстве Республики Казахстан: утв. 31 декабря 2020 года, №706 // https://adilet.zan.kz/rus/docs/V2000021969 (13.03.2026).
167. Правила использования дронов в странах мира // https://skymec.ru/pravila-ispolzovanija-dronov-v-stranah-mira/news/ (13.03.2026).
168. Мусин А.Б. Совершенствование методов оперативно-розыскной деятельности и внедрение PSYOP // Организация и деятельность органов внутренних дел на современном этапе: проблемы и пути решения: матер. междунар. науч.-практ. конф. – Костанай, 2023. – С. 129-131.

ПРИЛОЖЕНИЯ

ПРИЛОЖЕНИЕ А



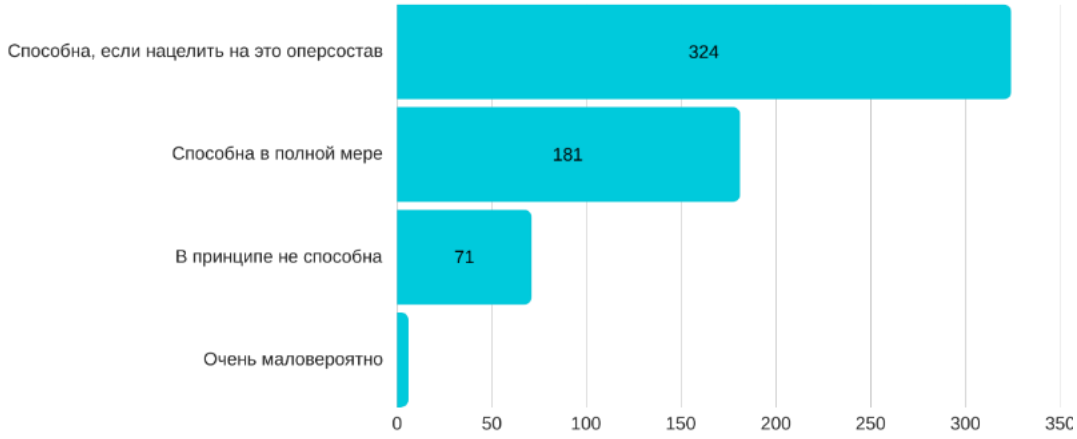




КАКАЯ ЛИНИЯ РАБОТЫ ЯВЛЯЕТСЯ ДЛЯ ВАС ОСНОВНОЙ?



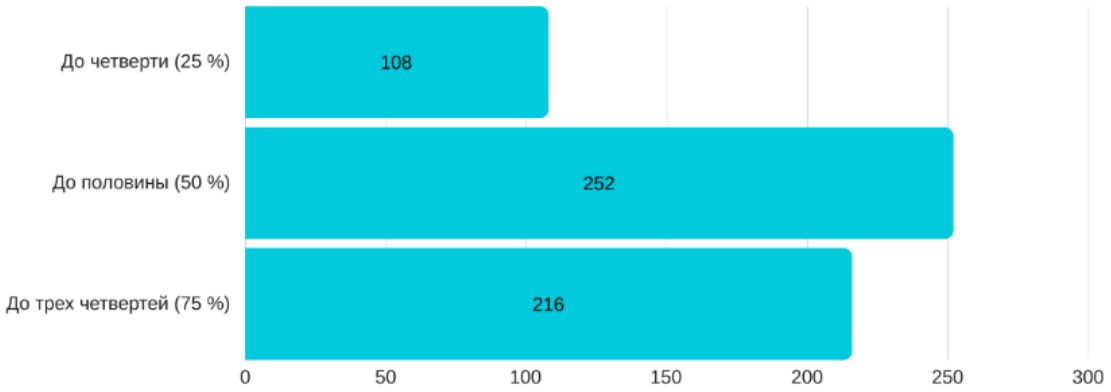
НАСКОЛЬКО СУЩЕСТВУЮЩАЯ ОРГАНИЗАЦИЯ ДЕЯТЕЛЬНОСТИ ОПЕРАТИВНЫХ ПОДРАЗДЕЛЕНИЙ ОВД СПОСОБНА ЗАРАНЕЕ ВЫЯВЛЯТЬ ПРИЗНАКИ ВОЗНИКНОВЕНИЯ УГРОЗ?



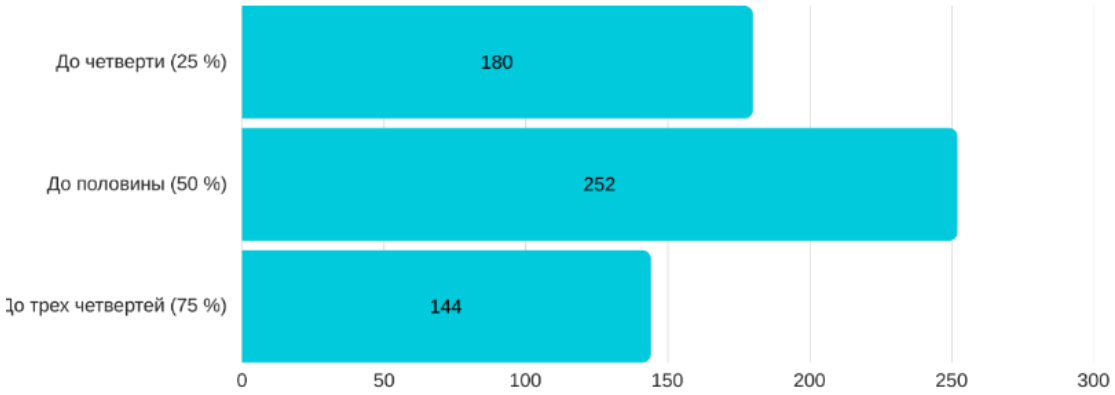
К КАКИМ ПОСЛЕДСТВИЯМ ОБЫЧНО ПРИВОДИТ ПРИВЛЕЧЕНИЕ К ОТВЕТСТВЕННОСТИ РУКОВОДИТЕЛЕЙ ПРЕСТУПНЫХ ГРУПП?



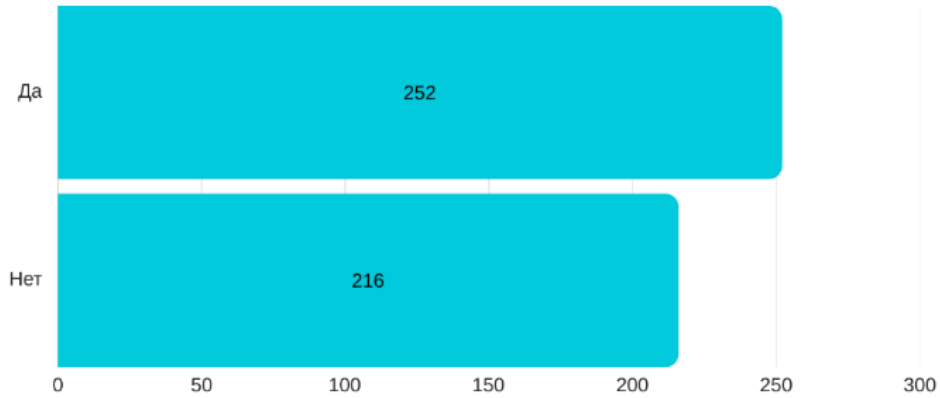
КАК ВЫ СЧИТАЕТЕ, КАКУЮ ДОЛЮ ОТ ОБЩЕГО ЧИСЛА РАСКРЫТЫХ ПРЕСТУПЛЕНИЙ СОСТАВЛЯЮТ РЕЗУЛЬТАТЫ ЛИЧНОГО СЫСКА?



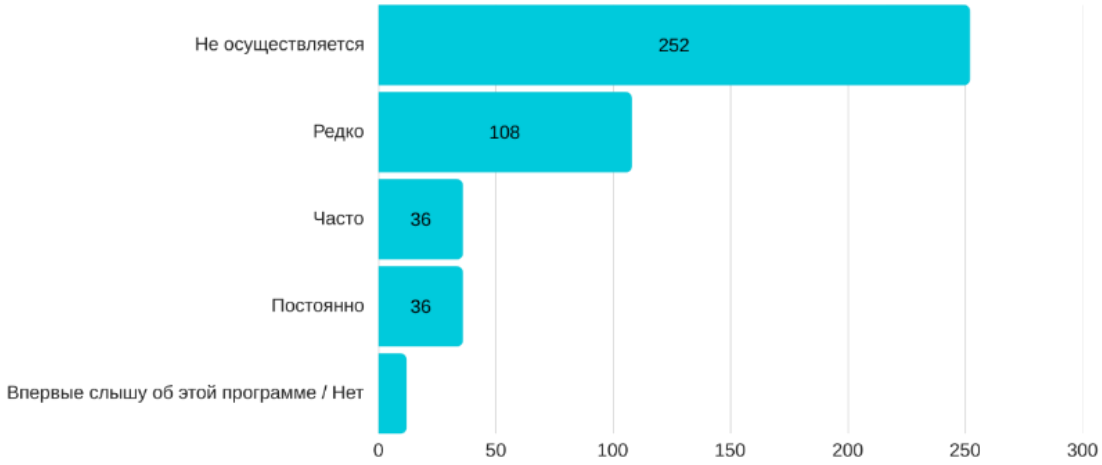
КАК ВЫ СЧИТАЕТЕ, КАКУЮ ДОЛЮ ОТ ОБЩЕГО ЧИСЛА РАСКРЫТЫХ ПРЕСТУПЛЕНИЙ СОСТАВЛЯЮТ РАСКРЫТЫЕ ПО ОПЕРАТИВНЫМ ДАННЫМ?



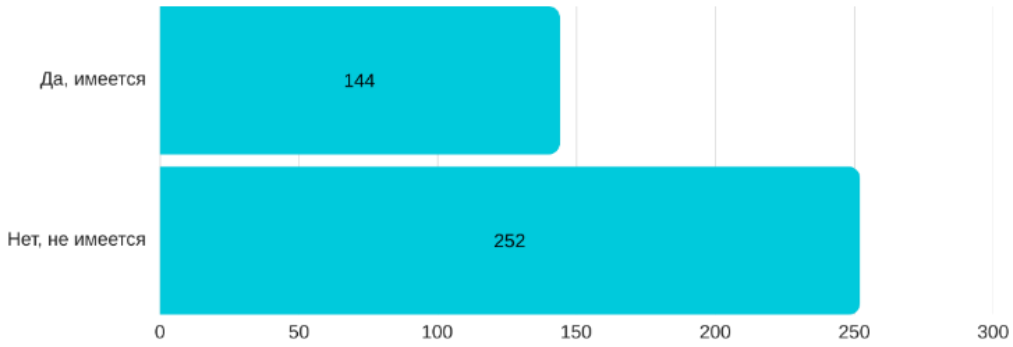
ЗНАЕТЕ ЛИ ВЫ, ЧТО ОЗНАЧАЕТ СЕТЕВОЙ ХАРАКТЕР СОВРЕМЕННОЙ ПРЕСТУПНОСТИ?



КАК ЧАСТО В ПРОЦЕССЕ ПОДГОТОВКИ И ПРОВЕДЕНИЯ ОРМ В ВАШЕМ ПОДРАЗДЕЛЕНИИ ОСУЩЕСТВЛЯЕТСЯ РАЗВЕДКА ИЗ ОТКРЫТЫХ ИСТОЧНИКОВ (OSINT)?



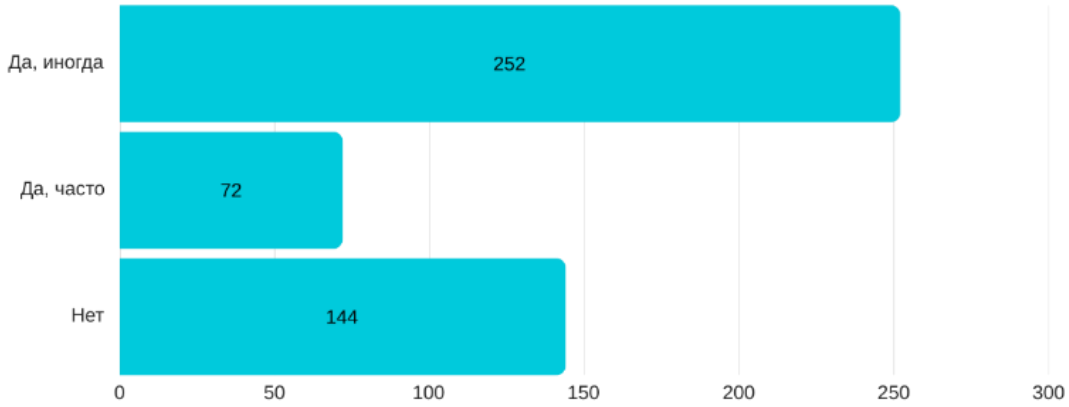
ЕСТЬ ЛИ В ВАШЕМ ПОДРАЗДЕЛЕНИИ ПОИСКОВАЯ ПРОГРАММА ДЛЯ МОНИТОРИНГА ИНТЕРНЕТА С ЦЕЛЬЮ ПОЛУЧЕНИЯ ОТКРЫТОЙ ИНФОРМАЦИИ О ФИГУРАНТАХ?



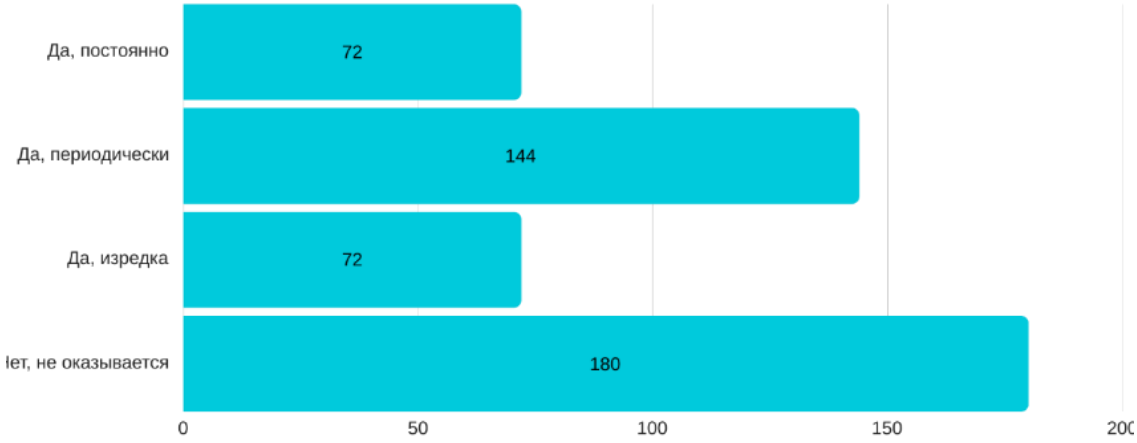
ЕСЛИ БЫЛИ ФАКТЫ ИСПОЛЬЗОВАНИЯ ДРОНОВ, ТО В КАКИХ ЦЕЛЯХ?



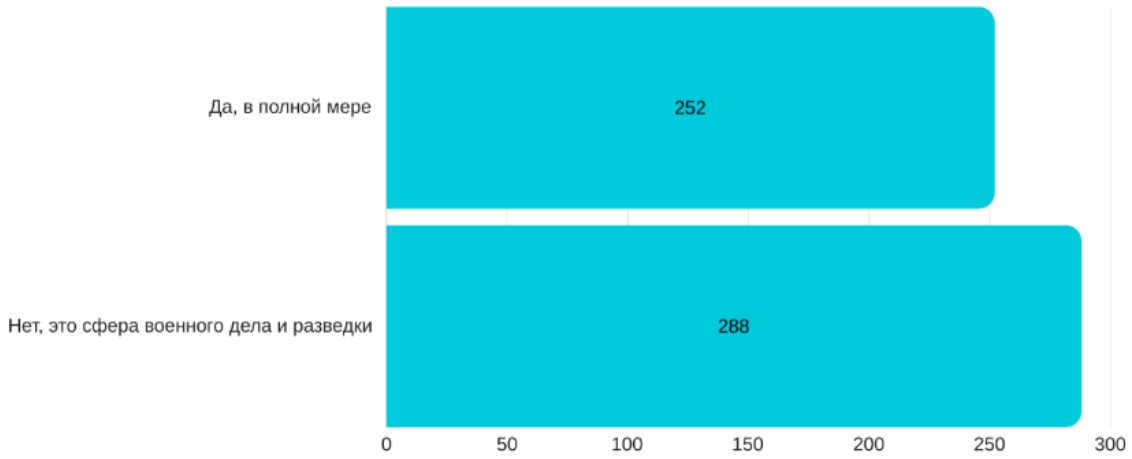
ВСТРЕЧАЛИСЬ ЛИ В ВАШЕЙ ПРАКТИКЕ ПРИМЕНЕНИЕ БЕСПИЛОТНЫХ ЛЕТАТЕЛЬНЫХ АППАРАТОВ (ДРОНОВ, КВАДРОКОПТЕРОВ) ПРИ ОСУЩЕСТВЛЕНИИ ОРМ?



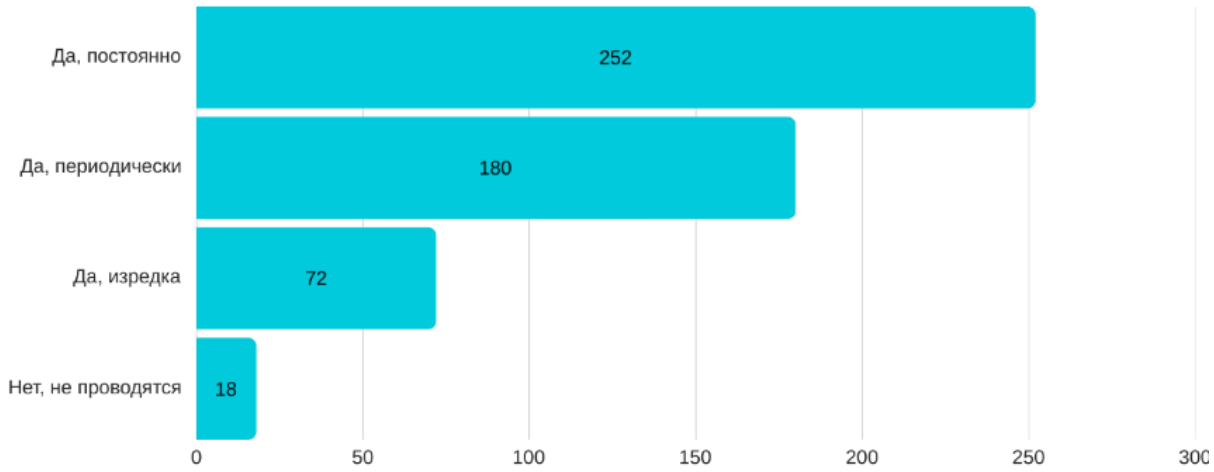
ОКАЗЫВАЕТСЯ ЛИ В РАМКАХ ОПЕРАТИВНЫХ КОМБИНАЦИЙ ЦЕЛЕВОЕ ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКОЕ ВОЗДЕЙСТВИЕ НА ФИГУРАНТОВ?



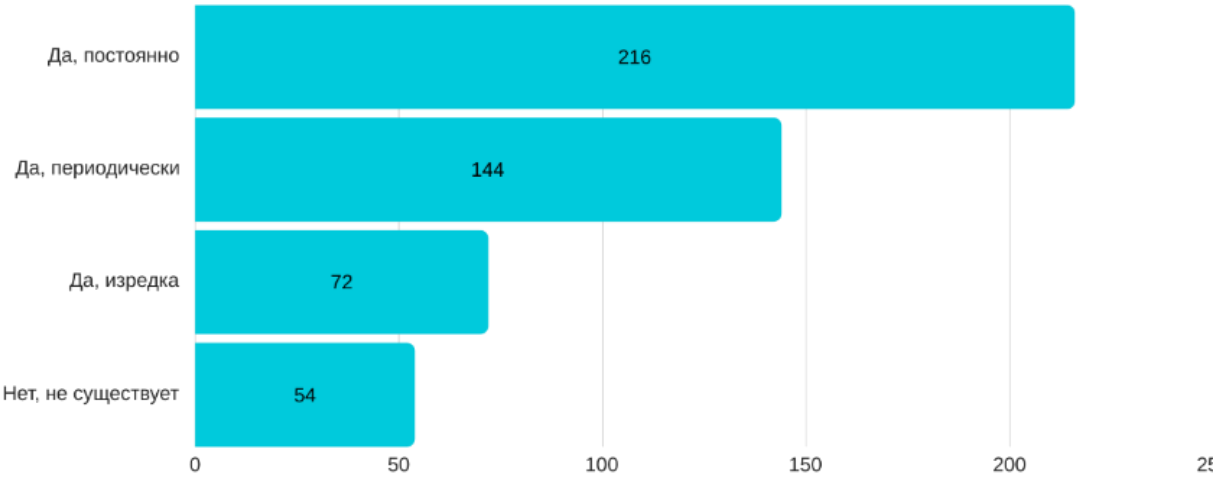
ПРИМЕНИМЫ ЛИ МЕТОДЫ ИНФОРМАЦИОННОЙ ВОЙНЫ И СОЗДАНИЕ УПРАВЛЯЕМОГО ХАОСА В ПРЕСТУПНЫХ ГРУППИРОВКАХ?



НАСКОЛЬКО РАСПРОСТРАНЕНА В ВАШЕМ ПОДРАЗДЕЛЕНИИ ПРАКТИКА ПРОВЕДЕНИЯ ОПЕРАТИВНЫХ КОМБИНАЦИЙ ПРИ ОСУЩЕСТВЛЕНИИ ОРМ?



СУЩЕСТВУЕТ ЛИ В ВАШЕМ ПОДРАЗДЕЛЕНИИ ПРАКТИКА ПРОГНОЗИРОВАНИЯ СЦЕНАРИЕВ РАЗВИТИЯ КРИМИНОГЕННОЙ ОБСТАНОВКИ?



ВАШИ МЫСЛИ ПО ПРОБЛЕМАМ СОВЕРШЕНСТВОВАНИЯ ОРГАНИЗАЦИИ ДЕЯТЕЛЬНОСТИ ОПЕРАТИВНЫХ АППАРАТОВ ОВД В СВЕТЕ ЯНВАРСКИХ СОБЫТИЙ 2022 ГОДА?

1. ОТСУТСТВИЕ МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЙ БАЗЫ, ЗАГРУЖЕННОСТЬ ПОСТУПАЮЩИМИ ТЕЛЕГРАММАМИ, НЕДОСТАТОЧНО ВРЕМЕНИ ДЛЯ РАСКРЫТИЯ И РАЗРАБОТКИ.
2. ВВЕСТИ ДОПОЛНИТЕЛЬНУЮ ШТАТНУЮ ЕДИНИЦУ, ЗАКРЕПЛЕННУЮ ЗА ДАННЫМ НАПРАВЛЕНИЕМ РАБОТЫ. ОСНАСТИТЬ СОТРУДНИКОВ КРИМИНАЛЬНОЙ ПОЛИЦИИ МАТЕРИАЛЬНО-ТЕХНИЧЕСКИМИ СРЕДСТВАМИ.
3. НЕТ ПРОБЛЕМ.
4. БОЛЬШЕ ПОЛНОМОЧИЙ.
5. УВЕЛИЧЕНИЕ ШТАТОВ ОПЕРАТИВНИКОВ, МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОСНАЩЕНИЕ.
6. НУЖНО УСОВЕРШЕНСТВОВАТЬ МЕТОДЫ ОРД, ТАК КАК НЫНЕШНИЕ МЕТОДЫ УСТАРЕЛИ И БОЛЬШИНСТВО ЛИЦ В ПРЕСТУПНОЙ СРЕДЕ ОСВЕДОМЛЕНЫ ТАКТИКЕ ВВЕДЕНИЯ МЕРОПРИЯТИЙ.
7. ВОЗДЕРЖУСЬ.
8. НЕ ЗНАЮ.
9. РАЗРЕШЕНИЕ ПРИМЕНЕНИЯ ОГНЕСТРЕЛЬНОГО ОРУЖИЯ.
10. УВЕЛИЧЕНИЕ ШТАТНОЙ ЧИСЛЕННОСТИ, ТАК КАК ОЧЕНЬ МНОГО СОКРАТИЛИ, ОСОБЕННО НА ТЕРРИТОРИАЛЬНЫХ ПОДРАЗДЕЛЕНИЯХ.
11. ВНЕДРЕНИЯ В ГРУППЫ.
12. БОЛЬШЕ ТЕОРИИ.
13. НЕДОСТАТОЧНОЕ КОЛИЧЕСТВО ОПЕРАТИВНОГО СОСТАВА, ГОНКА ЗА ПОКАЗАТЕЛЯМИ, ГОНКА ЗА ПРОЦЕНТОМ РАСКРЫВАЕМОСТИ ПРЕСТУПЛЕНИЙ, ВЕСЬ ОПЕРАТИВНЫЙ СОСТАВ НАПРАВЛЕН НА ВЫХОД УГОЛОВНЫХ ДЕЛ. РЕЗУЛЬТАТ БЕСКОНЕЧНЫХ СОКРАЩЕНИЙ. В РЕЗУЛЬТАТЕ ЧЕГО НАГРУЗКА ЕЖЕДНЕВНОЙ РУТИНЫ, И ЭТО В КАЖДОМ ОПЕРАТИВНОМ ПОДРАЗДЕЛЕНИИ. НЕКОГДА ЗАНИМАТЬСЯ РАЗРАБОТКАМИ, БЛАГОДАРЯ СОПРОВОЖДЕНИЮ УГОЛОВНЫХ ДЕЛ КАК В ЭЛЕКТРОННОМ, ТАК И В БУМАЖНОМ ФОРМАТЕ, ПРОВОДИТСЯ ДВОЙНАЯ РАБОТА ПО КАЖДОЙ ЗАЯВКЕ. МЫ ЖЕ ЖИВЁМ В 21 ВЕКЕ.
14. БОЛЬШЕ ПРОВОДИТЬ УЧЕНИЙ.
15. НА ПОСТОЯННОЙ ОСНОВЕ ОРИЕНТИРОВАТЬ ЛИЧНЫЙ СОСТАВ И ВСПОМОГАТЕЛЬНЫЙ АППАРАТ.
16. НЕДОСТАТОЧНОЕ ТЕХНИЧЕСКОЕ ОСНАЩЕНИЕ, ФИНАНСИРОВАНИЕ ОПЕРАТИВНОГО АППАРАТА ОВД, ОТСУТСТВИЕ ЦЕЛЕНАПРАВЛЕННОЙ ВЕРБОВКИ АГЕНТУРНОГО АППАРАТА ДЛЯ ВЫПОЛНЕНИЯ ПОСТАВЛЕННЫХ ЗАДАЧ, ЗАКОНОДАТЕЛЬНАЯ НЕЗАЩИЩЁННОСТЬ ОПЕРАТИВНОГО СОТРУДНИКА.
17. УВЕЛИЧИТЬ ЗАРАБОТНУЮ ПЛАТУ ОПЕРАТИВНИКАМ.
18. НА ПОСТОЯННОЙ ОСНОВЕ СОВЕРШЕНСТВОВАТЬ МЕТОДЫ АНАЛИТИЧЕСКОЙ РАБОТЫ И ОРГАНИЗАЦИИ ДЕЯТЕЛЬНОСТИ ОПЕРАТИВНЫХ ПОДРАЗДЕЛЕНИЙ ОВД РК.
19. УВЕЛИЧИТЬ ЗАРАБОТНУЮ ПЛАТУ ОПЕРАТИВНОМУ СОСТАВУ ОВД.
20. НАЧАТЬ СЛЕДИТЬ ЗА ТЕМ, ЧТОБЫ ОПЕРАТИВНЫЕ ПОДРАЗДЕЛЕНИЯ РАБОТАЛИ СОГЛАСНО РЕГЛАМЕНТУ, А НЕ СИДЕЛИ НА РАБОТЕ ДО 12 НОЧИ БЕЗ ВЫХОДНЫХ.
21. ВОПРОСЫ НЕ СООТВЕТСТВУЮТ ТЕМАТИКЕ. ПО МОЕМУ МНЕНИЮ, ОСНОВОЙ СОВЕРШЕНСТВОВАНИЯ ОРД В НАСТОЯЩЕЕ ВРЕМЯ ЯВЛЯЕТСЯ УВЕЛИЧЕНИЕ МОЩНОСТИ ПРИ ПРОВЕДЕНИИ СОРМ.
22. УЛУЧШЕНИЕ МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЙ БАЗЫ (ДРОНЫ, ПРОГРАММЫ БИЛЛИНГА, РАСПОЗНАВАНИЯ).

Мусин Айдар Булатович

ПРОАКТИВНЫЙ ПОДХОД В ОПЕРАТИВНО-РОЗЫСКНОЙ ДЕЯТЕЛЬНОСТИ ОРГАНОВ ВНУТРЕННИХ ДЕЛ РЕСПУБЛИКИ КАЗАХСТАН

Монография

Подписано в печать 05.08.2026.
Формат 60x84/1/16.
Усл. печ. стр. 9,3.
Тираж 500 экз.
Заказ №