

**К ВОПРОСУ О ПОНЯТИИ, СУЩНОСТИ И СОДЕРЖАНИИ
ИНФОРМАЦИОННОГО ПРОТИВОБОРСТВА
ОПЕРАТИВНЫМИ ПОДРАЗДЕЛЕНИЯМИ ПОЛИЦИИ****Пётр Иванович Иванов**

Академия управления МВД России, Москва, Россия, ivanovpi1952@yandex.ru

Аннотация. В настоящей статье на основе изучения и анализа оперативно-розыскного законодательства, научных публикаций, правоприменительной практики и криминогенной ситуации по линии информационного противоборства, осуществляемого силами правоохранительных органов, в том числе оперативными подразделениями полиции, рассматриваются существующие научные позиции специалистов в области теории оперативно-розыскной деятельности по вопросу о понятии, сущности и содержании указанного вида деятельности, который целиком нацелен на оказание открытого или скрытого информационного воздействия. Многие исследователи, характеризуя информационное противоборство в условиях коренных изменений, обусловленных прежде всего цифровой трансформацией, приходят к выводу о том (мы разделяем их мнение), что существует еще и информационно-психологическое противоборство как его неотъемлемая часть. При этом в работе автор сфокусировал свое внимание на поисках новых знаний по проблеме наличия их взаимозависимости и взаимообусловленности.

Ключевые слова: органы внутренних дел, оперативные подразделения органов внутренних дел, информационное противоборство, понятие, сущность и содержание информационного противоборства, факторы, обуславливающие информационное противоборство, совокупность признаков, базовый термин.

Для цитирования: Иванов П. И. К вопросу о понятии, сущности и содержании информационного противоборства оперативными подразделениями полиции // Вестник Уфимского юридического института МВД России. 2024. № 2 (104). С. 88–98.

Original article

**ON THE ISSUE OF THE CONCEPT, ESSENCE AND CONTENT
OF INFORMATION WARFARE BY OPERATIONAL POLICE UNITS****Peter I. Ivanov**Academy of Management of the Ministry of Internal Affairs of Russia, Moscow, Russia,
ivanovpi1952@yandex.ru

Abstract. Based on the study and analysis of operational investigative legislation, scientific publications, law enforcement practice and the criminogenic situation along the line of information warfare carried out by law enforcement agencies, including operational police units, the article examines the existing scientific positions of specialists in the field of theory of operational investigative activities on the concept, essence and content of this type of activity that is entirely aimed at providing open or hidden information impact. Many researchers, characterizing the information warfare in the context of fundamental changes caused primarily by digital transformation, come to the conclusion (we share their opinion) that there is also an informational and psychological confrontation as an integral part of it. At the same time, the author focused his attention on the search for new knowledge on the problem of their interdependence and interconditionality.

Keywords: internal affairs bodies, operational units of internal affairs bodies, information warfare, concept, essence and content of information warfare, factors causing information warfare, set of characteristics, basic term.

For citation: Ivanov P. I. On the issue of the concept, essence and content of information warfare by operational police units // Bulletin of Ufa Law Institute of the Ministry of Internal Affairs of Russia. 2024. No. 2 (104). P. 88–98. (In Russ.)

Введение

Органы внутренних дел и их оперативные подразделения выступают одним из субъектов реализации государственной политики в вопросах информационного противоборства (противостояния), которые в рамках своих полномочий осуществляют противодействие [1, с. 213–220] данной угрозе, создавая тем самым необходимое условие успешности проведения информационной политики [2, с. 26–33]. По мнению большинства специалистов, решающим фактором информационного противостояния является информационный потенциал.

При этом важно учесть одно немаловажное обстоятельство: развитие системы защиты информации ознаменовалось переходом от традиционной формы представления к более широкому пониманию информационной безопасности. Суть нового представления заключается в реализации комплексного подхода к пониманию информационной безопасности как совокупности двух основных направлений: защиты информации и защиты от информации. В свою очередь, защита от информации приобретает стратегический характер, становясь одной из ключевых современных проблем национальной безопасности России. При этом в контексте защиты от информации выделяют три основных направления информационных воздействий: 1) воздействия на информационно-технические системы и средства; 2) воздействия на общество; 3) воздействия на психику человека.

Отметим одну деталь: в понимании ключевых категорий (понятий), связанных с информационным противоборством, среди научных работников в настоящее время возникли определенные расхождения, что подтолкнуло автора настоящей статьи подключиться к обсуждению обозначенной нами проблемы.

Методы

Методологическую базу исследования составили общеправовые принципы ди-

алектики, общенаучные, частные и специальные методы, а также системный подход, обеспечивающие единство, объективность и концептуальную целостность системы информационного противоборства. Использование системно-структурного метода и метода факторного анализа позволило определить его структуру и направление проводимого выборочного изучения. Так, с помощью формально-юридического метода установлены, проанализированы и систематизированы основные источники оперативно-розыскных знаний об организации и тактике осуществления рассматриваемого вида деятельности в интересах противодействия ему, установлено взаимное влияние информационно-психологического и информационного противоборства на формирование научных положений и научно обоснованных рекомендаций по повышению эффективности противодействия им. Логико-юридический метод применялся для исследования нормативных правовых актов, позволивших определить понятие «информационное противоборство», его сущность и содержание. Формально-логический метод способствовал выявлению и систематизации элементов оперативно-розыскного противодействия и определению закономерных связей между ними. Статистический метод обеспечил возможность сбора, анализа и систематизации данных о предупреждении и пресечении различных видов правонарушений, в том числе с использованием оперативно-розыскных сил и средств. Конкретно-социологический метод использован при анкетировании руководителей оперативных подразделений полиции и их сотрудников, изучении отдельных оперативно-служебных документов. Решение задач исследования на основе привлечения обширного спектра теоретического и эмпирического материала предопределило использование разнообразного научного инструментария.

Результаты

В результате исследования сформулировано авторское определение понятия «информационное противоборство» на основе изучения и анализа научной литературы, нормативных правовых актов и правоприменительной практики; определена его сущность и содержание, которое в обобщенном виде представлено через призму комплекса мер, носящих теоретический, правовой, организационный, информационный, тактический и иной характер; разработана научно обоснованная теоретико-методологическая модель исследования информационно-психологического противоборства как одной из функций оперативных подразделений полиции.

Среди новых вызовов и угроз национальной безопасности в настоящее время информационное противоборство на фоне глобализации посредством информационно-телекоммуникационных технологий (сети), включая сеть Интернет, занимает ключевое место, поскольку оно охватывает самые передовые технологии, преследующие одну единственную цель – выигрыш в условиях международного соперничества.

Со своей стороны полагаем, что без предварительного уяснения смысла и содержания рассматриваемого понятия вряд ли удастся найти наиболее оптимальные варианты противодействия. К сожалению, на сегодня среди специалистов теории оперативно-розыскной деятельности (далее – ОРД) органов внутренних дел (далее – ОВД) нет единого мнения на этот счет, что вызывает определенные трудности и сложности в решении указанной задачи.

В системе оперативно-розыскного понятия противодействия и понятийно-категориального аппарата базовым термином является информационное противоборство, которое, на наш взгляд, может быть рассмотрено как в узком, так и в широком смысле.

Одни авторы (Г. Г. Аветисянц, В. И. Борисов, Д. П. Гавра и др.) информационное противоборство рассматривают как нацеленную на получение информационного превосходства и выигрыша в сфере реально-

го бытия форму борьбы социальных субъектов, представляющую собой использование каждым из них информационных и иных ресурсов, специальных средств и методов для воздействия на информационные процессы и информационную среду противостоящего субъекта и защиты собственных информационных процессов и информационной среды [3, с. 10–26].

Из приведенного определения видна сама цель информационного противоборства, а также его стороны, ресурсы, инструменты и объекты воздействия. Автор при его формулировании предусмотрел системообразующие компоненты рассматриваемого вида деятельности, что, на наш взгляд, является большим его достоинством.

В научной литературе существуют и иные подходы к определению понятия «информационное противоборство». Так, например, С. П. Расторгуев утверждает, что «информационное противоборство – это открытое и/или скрытое целенаправленное информационное воздействие систем друг на друга с целью получения определенного выигрыша в материальной сфере» [4, с. 468]. В данном случае автор, на наш взгляд, анализируемый вид деятельности рассматривает в узком смысле слова. Многие исследователи, характеризуя информационное противоборство, приходят к выводу о том, что существует еще и информационно-психологическое противоборство, которое, по их мнению, выступает неотъемлемой частью информационного противоборства. Одним из сторонников этой точки зрения является А. В. Манойло. В частности, он считает, что информационное противоборство есть «соперничество социальных систем в информационно-психологической сфере по поводу влияния на те или иные сферы социальных отношений и установления контроля над источниками стратегических ресурсов, в результате которого одни участники соперничества получают преимущества, необходимые им для дальнейшего развития, а другие их утрачивают» [5, с. 388]. Действия участников информационного противоборства могут носить наступательный (агрес-

сия, война) или оборонительный характер. Указанный подход разделяют многие специалисты [6, с. 92]. Как видим, вышеприведенные определения сформулированы авторами через призму военного искусства. Однако они, как нам представляется, приемлемы и применительно к правоохранительной деятельности, поскольку в них заложены концептуальные основы самого термина.

Другие (В. И. Шайкин [7, с. 272], В. А. Мелешенко [8, с. 74] и др.), говоря об информационном противоборстве, одновременно употребляют такие термины, как «информационная война», «информационно-психологическое противоборство», оценивая при этом как относительно самостоятельные виды деятельности. Со своей стороны полагаем, что сторонники этой точки зрения вполне аргументированно обосновывают свою позицию, и поэтому она, безусловно, имеет право на существование. Разделяя отчасти указанное мнение, хотим подчеркнуть, что информационная война есть составная часть современной геополитики.

Рассуждая о понятии «информационное противоборство», мы стараемся уяснить для себя сущностно-содержательные элементы, а их, на наш взгляд, три:

а) принятие активных целенаправленных действий, затрагивающих различные сферы жизнедеятельности (общество, индивид, коллектив через призму удовлетворения социально-экономических и иных их потребностей). Выборочное изучение научной литературы убедительно показывает, что исследователи основной акцент делают на информационно-психологической сфере, рассматривая ее как действенное средство для влияния на противоборствующую сторону. Такой способ противодействия многократно доказан в его эффективности при достижении планируемой цели. При этом человеческий ресурс считается определяющим (ключевым);

б) совокупность общественных отношений, включая урегулированные нормами различных отраслей права. Эти отношения возникают между двумя субъектами, пред-

ставляемыми в виде относительно самостоятельных систем;

в) наконец, соперничество в интересах получения преимущества чаще всего в материальной сфере, позволяющего становиться субъектом контроля над источниками стратегических ресурсов. Здесь основным двигателем является выигрыш.

Вышеуказанные составные части, взятые вместе, образуют единый деятельностный механизм, основанный на общем методологическом подходе к намеченной цели. Как нам представляется, указанный механизм есть совокупность правовых норм, форм, методов и средств, обеспечивающих эффективность морально-психологического воздействия. Мы полагаем, что в таком виде сталкиваемся со специально сформированной инфраструктурой (организационное построение), располагающей необходимыми ресурсами и средствами. Характеризуя указанный механизм, отметим, что при его реализации отчетливо проявляют себя такие принципы, как единство научно-методических и организационных подходов к выработке осуществляемой в рамках информационно-психологического противоборства политики; принцип инновационности, состоящий в разработке и внедрении прогрессивных научных технологий совершенствования его форм и методов; принцип профессионализации управления, основанный на необходимости повышения профессиональной компетенции задействованных на практическое осуществление специалистов. В системе названных принципов не менее востребованным считается принцип практической направленности, означающий подчиненность названной политики целям и задачам деятельности по информационно-психологическому противоборству.

Чтобы противостоять ему, мы в контексте оперативно-служебной деятельности полицейских и иных подразделений МВД России из всей системы выделяем два направления, которые, на наш взгляд, являются основными: 1) профессиональная подготовка, обеспечивающая достижение сотрудниками высокого уровня професси-

онализма на основе развития знаний, привития навыков и формирования умений; 2) морально-психологическое обеспечение, формирующее устойчивое морально-психологическое состояние личного состава, благоприятный социально-психологический климат в служебных коллективах. Со своей стороны полагаем, что в числе приоритетных задач в этом ракурсе в первую очередь должно стать развитие многоуровневой практико-ориентированной системы непрерывного профессионального образования. При этом важно обеспечить соответствие содержания и структуры профессиональной подготовки сотрудников ОВД с динамично изменяющимися потребностями указанных органов, а это предполагает разработку и реализацию профильных образовательных программ повышения квалификации полицейских. Оценку качества профессионального образования целесообразно проводить на основе комплексного мониторинга, предварительно разработав механизм его реализации.

Что же касается морально-психологического сопровождения работы с личным составом, то его организация, по мнению автора настоящей статьи, предполагает:

- использование современных информационных и педагогических технологий (дистанционное обучение, контрольные тестовые системы);

- внедрение автоматизированной информационной системы ведомственного мониторинга морально-психологического состояния служебного коллектива.

Такая работа должна быть нацелена на формирование системы защиты личного состава от негативного информационно-психологического воздействия. Это, в свою очередь, означает: а) выработку у сотрудников устойчивой системы взглядов, идей и подходов и формирование на этой основе способности к объективной оценке событий и фактов действительности с позиции интересов оперативно-служебной действительности; б) развитие форм и средств информационно-пропагандистского воздействия на личный состав в целях разъяснения истинного

содержания важных общественно-политических событий, социально-экономических процессов и явлений. Одним из условий успешного достижения указанной цели является формирование соответствующих потребностям времени нормативных правовых и организационных основ противоборства.

Заметим, что понятия «организация информационного противоборства» и «информационное противоборство» – не одно и то же (не идентичны), ибо в первом случае это вид деятельности в ее динамике, а во втором – нахождение его в статике.

Говоря о понятии «организация информационного противоборства», мы выделяем в нем следующие ключевые признаки, которые в целом его характеризуют. Это такие признаки, как вид согласованной и целенаправленной деятельности, ее упорядоченность, исходя из целей и задач, стоящих перед оперативными подразделениями полиции.

Руководители территориальных ОВД и их оперативных подразделений, оценивая современное состояние информационного противоборства, предварительно изучают среду функционирования через призму совокупности факторов. В частности, ими являются:

- условия глобализации и информатизации, которые помимо позитивных процессов несут в себе деструктивное воздействие на общество. Доказано, что обострение информационного противоборства является следствием глобализации;

- информационно-телекоммуникационное пространство для криминальных структур – это среда, в которой за относительно небольшие затраты можно охватить большую аудиторию под свое информационно-психологическое воздействие с целью манипулирования общественным сознанием (электронное мошенничество);

- скорость и качество получения необходимых сведений, заслуживающих оперативного внимания, и их переработки с учетом уже имеющейся в распоряжении оперативных подразделений информации. Немаловажным при этом является своевременное

доведение до адресата (исполнителя) окончательных данных. Информационное противодействие в обобщенном виде предполагает ряд действий, среди которых особо значимыми, на наш взгляд, являются: добытие оперативно значимой информации, ее переработка (проверка), защита информационных каналов от несанкционированного проникновения третьих лиц;

– совокупность противоречий экономического, политического, религиозного, национального характера. Преследуя геополитические цели, страны коллективного Запада (Европейского союза) стали широко применять не только решение конфликтов военным путем, экономическими санкциями, но и массовым использованием информационных средств и ресурсов. Зачастую именно информационное противоборство выходит на первый план при решении оперативно-тактических задач, для которых ранее использовали международное сотрудничество;

– сети связи и информационно-вычислительные сети, выступающие в качестве основных средств информационного противоборства;

– влияние психологических операций, служащих одним из элементов, на состояние противодействия информационных войн. Специалисты констатируют, что на сегодня уже существуют способы прогнозирования и эффект «срабатывания» от психологических операций.

– проблематика информационного противоборства, информационной безопасности, информационной войны, которая стала одной из наиболее популярных в современном научном и политическом дискурсе. В процессе глобализации общество переходит к информационному типу, где информация становится стратегическим ресурсом и ключевой ценностью, подверженной новым угрозам.

В зависимости от масштабов воздействия факторы, на наш взгляд, делятся: на глобальные (внешние) и внутренние.

Сущность информационного противоборства на современном этапе можно ха-

рактеризовать как деятельность ОВД и их оперативных подразделений по контролю и доминированию в финансово-экономическом (материально-техническом), научном и информационном пространстве посредством целенаправленного использования оперативно-розыскных и иных возможностей, которыми они располагают. На этом фоне в настоящее время существенным образом возрастает роль информационной составляющей в оперативно-розыскной политике.

Доказано, что сущность информационного противоборства и его составных компонентов находит внешнее проявление через совокупности признаков. В связи с этим укажем системообразующие признаки:

– открытые или скрытые целенаправленные информационные воздействия систем (правоохранительные органы – преступная среда) друг на друга с целью получения определенного выигрыша в материальной или идеологических сферах;

– достижение превосходства над криминальной структурой в своевременности, достоверности и полноте получения информации, представляющей оперативный интерес.

Что же касается содержания понятия «информационное противоборство», то мы под ним понимаем совокупность взаимосвязанных между собой действий, направленных на достижение преследуемой в ходе осуществления информационно-психологического противоборства цели. Речь идет о совокупности научно выверенных и апробированных на практике мер (действий) теоретического, правового, организационного, информационного, психологического, методического и иного характера, направленных на обеспечение интересов системы МВД России посредством создания благоприятных условий для успешного решения стоящих перед ней задач путем планомерного и системного осуществления возложенных на нее функций.

Говоря о содержании, сотрудники оперативных подразделений полиции должны придерживаться основных правил. Укажем их.

Первое правило: постоянно обеспечивать информационное доминирование в контексте оперативно значимой информации в отношении лиц и фактов, представляющих оперативный интерес (лиц, вынашивающих противоправные деяния (замысел) против структурных подразделений ОВД и их сотрудников [9, с. 80–83; 10, с. 915–200; 11, с. 195–200] либо распространяющих материалы экстремистского характера в сети Интернет).

Второе правило: добиваться полного задействования межведомственного взаимодействия оперативных подразделений органов, осуществляющих ОРД в интересах борьбы с международной, межгосударственной, трансграничной организованной преступностью.

Третье правило: использовать средства массовой информации (далее – СМИ) (медиа) для влияния через социальные сети, браузеры, взломы; прогнозировать риски и угрозы по результатам мониторинга ситуации, постараться заблаговременно иметь вариант реагирования (так называемая оперативная готовность на случай осложнения обстановки, внезапно возникших нестандартных ситуаций).

Четвертое правило: не следует занимать «оборонительную позицию», работать на упреждение, опережать жертв преступлений в трактовке фактов, а не только опровергать случившееся.

Пятое правило: активнее работать в социальных медиа, в том числе с молодежной аудиторией в соответствующем формате.

Упорядоченная система противоборства предполагает наряду с другими элементами совокупность принципов¹. Исследователи к их числу относят множество основополагающих идей.

К основным принципам информационного противоборства мы, в частности, относим: информационную асимметрию, при которой одна сторона – оперативные подразделения (противоборства) – имеет больший

объем информации, чем вторая (преступное сообщество); информационное доминирование; скрытость, латентность процессов информационно-психологической борьбы; внезапность реализации (легализации) в отношении лидеров и организаторов преступного сообщества имеющихся материалов оперативной проверки.

Заметим, что рост востребованности в деятельности оперативных подразделений полиции информационных ресурсов обозначил ряд проблем, стоящих перед ними, который включен в систему противодействия (содействие, комплекс оперативно-розыскных и иных мер, оперативно-розыскная работа, осуществляемая на системной основе в рамках дела оперативного учета).

Как справедливо отмечают многие исследователи, неотъемлемой составной частью информационного противоборства является информационно-психологическое противоборство, которое применительно к деятельности оперативных подразделений полиции на сегодня выступает одним из приоритетных направлений их деятельности. При ее осуществлении отчетливо проявляют себя такие принципы, как единство научно-методических и организационных подходов к выработке осуществляемой в рамках информационно-психологического противоборства политики; принцип инновационности, состоящий в разработке и внедрении прогрессивных научных технологий совершенствования его форм и методов; принцип профессионализации управления, основанный на необходимости повышения профессиональной компетенции задействованных на практическое осуществление специалистов. В системе названных принципов не менее востребованным считается принцип практической направленности, означающий подчиненность названной политики целям и задачам деятельности по информационно-психологическому противоборству. Как

¹ Автор настоящей статьи, помимо рассмотренных ниже, не исключает необходимость соблюдения законности, конспирации, разграничения компетенции в борьбе с преступностью, плановости, системности и коллегиальности при выработке решений, затрагивающих общие интересы всех служб и подразделений органов внутренних дел.

видим, названные начала выражают его специфику и целевую направленность.

Как нам представляется, благодаря соблюдению вышеперечисленных принципов, удастся добиться соразмерности и адекватности принимаемых сотрудниками указанных подразделений ответных мер.

Помимо принципов, правоприменительная практика при осуществлении информационного противоборства настоятельно рекомендует учесть складывающиеся условия, основными из которых являются:

- разработанность теоретических основ информационного противоборства в контексте деятельности правоохранительных органов;

- руководство информационным противоборством непосредственно руководителем ОВД;

- высокая техническая оснащенность информационного противоборства по сравнению криминальной средой;

- высокая степень секретности и скоординированности деятельности правоохранительных органов в ходе проведения мероприятий информационного противоборства;

- акцент на скрытные методы и способы информационного противоборства;

- обеспечение конфиденциальности применяемых сил, средств и приемов;

- привлечение к сотрудничеству в области информационного противоборства профессионалов в области СМИ.

В системе информационно-психологического противоборства мы выделяем его цели, задачи и функции. В частности, преследуются следующие цели:

- достижение превосходства в противодействии преступности;

- создание для этого благоприятных условий (правовых, организационных, методических, информационных, кадровых, материально-технических, финансовых, социальных, медицинских и т. п.);

- обеспечение устойчивости от информационно-психологического воздействия со

стороны криминальной среды в отношении сотрудников ОВД.

Чтобы достичь перечисленные цели, приходится решать ряд задач, основными из которых, на наш взгляд, являются:

- обеспечение информационной безопасности системы МВД России [12, с. 130–135];

- недопущение информационно-психологического воздействия на сотрудников ОВД;

- активное ведение информационного противоборства¹ [13, с. 85–89].

Органы внутренних дел и их оперативные подразделения в пределах своей компетенции осуществляют планомерную и системную работу по обеспечению информационной безопасности нашей страны от негативного воздействия СМИ на общественное сознание граждан Российской Федерации. К числу такого рода действий относятся следующие:

- осуществление работы по выявлению источников негативистского влияния из числа СМИ, социальных сетей, форумов, блогов, мессенджеров, распространению ложных новостей – «фейков»; причем в качестве таковых могут выступать блогеры, стримеры и иные пользователи систем на основе разного рода видеохостингов;

- инициирование прекращения деятельности СМИ, своевременное блокирование социальных сетей, форумов, блогов, мессенджеров, способствующих распространению ложных новостей – «фейков», в случае осуществления ими негативного воздействия на общественное сознание людей;

- осуществление работы в области создания официальных государственных СМИ, в которых на постоянной и системной основе проводилось бы разъяснение о негативном влиянии отдельных его недобросовестных участников, духовное воспитание граждан нашей страны;

- привлечение к ответственности лиц, распространяющих ложные новости – «фей-

¹ О некоторых особенностях использования информационно-телекоммуникационных технологий (достижений науки и техники) в преступных целях.

ки». В соответствии с нормами действующего законодательства Российской Федерации за негативистское влияние СМИ на общее сознание граждан предусмотрены следующие виды правовой ответственности:

– уголовная ответственность предусмотрена ст. 207.1, ст. 207.2, 207.3, 280.3, 284.2 УК РФ;

– административная ответственность предусмотрена ч. 9–11 ст. 13.15, 20.3.3 и 20.3.4 КоАП РФ.

Текущий этап развития системы оперативно-розыскного противодействия – информационный, характеризующийся не только широким использованием достижений науки и техники, но и той преступной средой, сформировавшейся преимущественно под влиянием информационных технологий, ее применением при совершении преступлений.

Оперативные подразделения полиции столкнулись с серьезным испытанием. К сожалению, сейчас ограничен, чего не было раньше, обширный перечень средств помощи, в том числе международной правовой. Действия оперативных подразделений полиции направлены главным образом на обеспечение защиты от деструктивного (разрушительного) воздействия информации. Заметим, что такое воздействие носит двойственный характер: с одной стороны, оно направлено на угрозоносителя, деструктивные силы, от которых можно ожидать с большой вероятностью нанесение ущерба (вреда), с другой – на систему обеспечения защиты информации в случае посягательства (общепрофилактическая направленность – превенция).

Благодаря оперативно-розыскному противодействию преступной среде представляется возможным своевременно распознать различные информационные конфликты, явное или скрытое предоставление субъектами информации ложных, деструктивных обстоятельств, влияющих на психологическое состояние общества с целью искусственного создания в нем социальной напряженности.

Изучение и критический анализ существующих научных источников и правоприменительной практики позволил прийти к

целому ряду предложений, направленных на повышение эффективности деятельности ОВД по информационному противодействию. В их числе основными являются:

1) формирование соответствующих потребностям времени нормативных правовых и организационных основ противодействия деятельности по информационному противодействию в органах внутренних дел;

2) формулирование многоуровневой практико-ориентированной системы оперативно-розыскной деятельности по информационному противодействию. Она должна соответствовать динамично изменяющимся условиям и потребностям оперативных подразделений полиции;

3) разработка научно обоснованных методик прогнозирования криминогенной ситуации и потребностей ОВД в специалистах различных профилей. Одновременно принять меры по реализации механизмов обеспечения комплексной автоматизированной информационной системы мониторинга их качества;

4) совершенствование системы профессиональной переподготовки и повышения квалификации кадров, что, в свою очередь, предполагает оперативную разработку и внедрение образовательных программ, обеспечивающих их обучение по новым специализациям и профилям подготовки в соответствии с запросами различных служб и подразделений ОВД;

5) выработка и внедрение в практику современных информационных и психологических технологий защиты личного состава от негативного воздействия преступной среды, надежного перекрытия каналов негативной информации, влияющей на сотрудников;

6) разработка и внедрение в работу единой автоматизированной информационной системы сбора сведений о принимаемых мерах территориальными органами МВД России на региональном уровне по локализации и нейтрализации со стороны преступной среды (криминальных элементов) негативного информационно-психологического воздействия на их сотрудников.

Заключение

Таким образом, главное звено в системе оперативно-розыскного противодействия направлено на лиц, вынашивающих противоправные действия против общественного порядка и общественной безопасности (протестная активность, массовые беспорядки и иные вызовы и угрозы, сопряженные с совершением тяжких и особо тяжких уголовно наказуемых деяний). Органы внутренних дел на сегодня подвержены масштабным информационно-психологическим воздействиям, прежде всего, со стороны органи-

зованных криминальных формирований. В этих условиях возникает неизбежная потребность заблаговременной подготовки сотрудников ОВД и их структурных подразделений к ведению противодействия информационному противоборству. Знание ими технологии его осуществления, когда информационно-телекоммуникационное пространство (социальные сети) активно используются, например, в экстремистских целях, является решающим фактором доминирования в противостоянии рассматриваемому феномену.

СПИСОК ИСТОЧНИКОВ

1. Ишин И. А. «Противодействие преступности» или «борьба с преступностью»: анализ понятий // Научный вестник Орловского юридического института МВД России имени В. В. Лукьянова. 2022. № 3 (92). С. 213–220.
2. Иванов П. И. Концептуальные основы формирования оперативно-розыскной политики: понятие, сущность и содержание // Вестник Владимирского юридического института. 2022. № 2 (63). С. 26–33.
3. Гавра Д. П. Информационное противоборство: современное понимание, характеристики, подходы к междисциплинарному познанию // Российская школа связей с общественностью. 2023. № 29. С. 10–26.
4. Расторгуев С. П. Философия информационной войны. М.: Вузовская книга. 2001. 468 с.
5. Манойло А. В. Государственная информационная политика в особых условиях. М.: Изд. МИФИ, 2003. 388 с.
6. Рощупкин В. Г. Информационно-психологическое противоборство и обеспечение информационной безопасности: учеб. пособие. Самара: Издательство Самарского университета. 2018. 92 с.
7. Шайкин В. И. Информационные войска России – настоящее веление времени: монография. Рязань: РВВДКУ, 2015. 272 с.
8. Мелешенко В. А. Информационная война и современные аспекты информационного противоборства // Научный резерв. 2021. № 1 (13). С. 74.
9. Иванов П. И. Противодействие органами внутренних дел дискредитации их сотрудников (организационно-тактический аспект) // Правоохранительная деятельность. 2023. № 2 (12). С. 80–83.
10. Иванов П. И. Защита чести, достоинства и деловой репутации сотрудников ОВД РФ (понятие, сущность и содержание) // Закон и право. 2023. № 12. С. 195–200.
11. Иванов П. И. Сущность дискредитации сотрудников ОВД РФ // Закон и право. 2024. № 1. С. 195–200.
12. Грищенко Л. Л., Синодов И. А. Роль и место МВД России в обеспечении информационной безопасности // Сетевое издание «Академическая мысль». 2022. № 4 (21). С. 130–135.
13. Иванов П. И. Оперативно-розыскное противодействие киберпреступлениям (проблемы и пути их решения) // Труды Академии управления МВД России. 2022. № 4 (64). С. 83–92.

REFERENCES

1. Ishin I. A. “Countering crime” or “fighting crime”: an analysis of concepts // Scientific Bulletin of Orel Law Institute of the Ministry of Internal Affairs of Russia named after V. V. Lukyanov. 2022. No. 3 (92). P. 213–220. (In Russ.)
2. Ivanov P. I. Conceptual foundations of the formation of operational investigative policy: concept, essence and content // Bulletin of Vladimir Law Institute. 2022. No. 2 (63). P. 26–33. (In Russ.)

3. Gavra D. P. Informational confrontation: modern understanding, characteristics, approaches to interdisciplinary cognition // The Russian School of Public Relations. 2023. No. 29. P. 10–26. (In Russ.)
4. Rastorguev S. P. The philosophy of information warfare. M.: University book. 2001. 468 p. (In Russ.)
5. Manoilo A. V. State information policy in special conditions. M.: MEFHI Publishing House, 2003. 388 p. (In Russ.)
6. Roshchupkin V. G. Information and psychological confrontation and ensuring information security: study guide. Samara: Samara University Press. 2018. 92 p. (In Russ.)
7. Shaikin V. I. Information troops of Russia – the imperative of the time: a monograph. Ryazan: RVVDKU, 2015. 272 p. (In Russ.)
8. Meleshenko V. A. Information warfare and modern aspects of information warfare // Scientific Reserve. 2021. No. 1 (13). P. 74. (In Russ.)
9. Ivanov P. I. Counteraction by internal affairs bodies to discredit their employees (organizational and tactical aspect) // Law enforcement. 2023. No. 2 (12). P. 80–83. (In Russ.)
10. Ivanov P. I. Protection of honor, dignity and business reputation of employees of the Ministry of Internal Affairs of the Russian Federation (concept, essence and content) // Law and Order. 2023. No. 12. P. 195–200. (In Russ.)
11. Ivanov P. I. The essence of discrediting employees of the Ministry of Internal Affairs of the Russian Federation // Law and Order. 2024. No. 1. P. 195–200. (In Russ.)
12. Grishchenko L. L., Synodov I. A. The role and place of the Ministry of Internal Affairs of Russia in ensuring information security // Online publication “Academic thought”. 2022. No. 4 (21). P. 130–135. (In Russ.)
13. Ivanov P. I. Operational investigative counteraction to cybercrimes (problems and ways to solve them) // Proceedings of the Academy of Management of the Ministry of Internal Affairs of Russia. 2022. No. 4 (64). P. 83–92. (In Russ.)

Информация об авторе:

П. И. Иванов, доктор юридических наук, профессор.

Information about the author:

P. I. Ivanov, Doctor of Law, Professor.

Статья поступила в редакцию 09.04.2024; одобрена после рецензирования 11.04.2024; принята к публикации 21.06.2024.

The article was submitted 09.04.2024; approved after reviewing 11.04.2024; accepted for publication 21.06.2024.