

Дата поступления рукописи в редакцию: 18.09.2026 г.

DOI: 10.24412/2076-1503-2026-10-853-861

Дата принятия рукописи в печать: 29.10.2026 г.

ДОЛЕВА Ольга Андреевна,
соискатель,
e-mail: olya.doleva@yandex.ru

ПРОТИВОДЕЙСТВИЕ ИСПОЛЬЗОВАНИЮ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ ПРИ ОРГАНИЗАЦИИ ПРЕСТУПЛЕНИЯ

Аннотация. В статье рассматриваются меры противодействия использованию информационно-телекоммуникационных технологий при организации преступлений. Отмечается, что цифровизация преступной деятельности существенно трансформирует институт соучастия: организатор получает возможность дистанционного руководства, что повышает латентность и распространенность преступлений. Объектом исследования выступают общественные отношения, охраняемые уголовным законом, в сфере противодействия использованию информационно-телекоммуникационных технологий при организации преступлений. Предметом исследования являются нормы уголовного законодательства Российской Федерации, предусматривающие ответственность за организацию преступлений, а также практика их применения. Методологическую основу исследования составили общенаучные (анализ, синтез, индукция, дедукция) и частнонаучные (формально-юридический, сравнительно-правовой) методы познания. Проведен анализ положений Общей и Особенной частей УК РФ, выявлены соответствующие недостатки. Сделан вывод о необходимости комплексного подхода, объединяющего законодательные, правоприменительные, профилактические и международные меры в целях эффективного противодействия исследуемому виду преступности.

Ключевые слова: информационно-телекоммуникационные технологии, организация преступления, организатор преступления, соучастие в преступлении, уголовно-правовые меры, противодействие преступности, профилактика, предупреждение.

Для цитирования: Долева О. А. Противодействие использованию информационно-телекоммуникационных технологий при организации преступления // Образование и право. 2026. № 10. С. 853–861.

DOLEVA Olga Andreevna,
applicant

COUNTERING THE USE OF INFORMATION AND TELECOMMUNICATION TECHNOLOGIES IN ORGANIZING A CRIME

Annotation. The article examines measures to counteract the use of information and telecommunications technologies in organizing crimes. It is noted that the digitalization of criminal activity significantly transforms the institution of complicity: the organizer gains the ability to provide remote guidance, which increases the latency and prevalence of crimes. The object of the study is the social relations protected by criminal law in the field of countering the use of information and telecommunications technologies in organizing crimes. The subject of the study is the norms of the criminal legislation of the Russian Federation that provide for liability for organizing crimes, as well as the practice of their application. The methodological basis of the study consisted of general scientific (analysis, synthesis, induction, deduction) and specific scientific (formal-legal, comparative-legal) methods of cognition. An analysis was carried out of the provisions of the General and Special Parts of the Criminal Code of the Russian Federation, and the relevant shortcomings were identified. It was concluded that a comprehensive approach is needed, combining legislative, law-enforcement, preventive, and international measures to effectively counter the type of crime under study.

Key words: *information and telecommunications technologies, crime organization, crime organizer, complicity in a crime, criminal law measures, crime counteraction, prevention, warning.*

For citation: *Doleva O. A. Countering the use of information and telecommunication technologies in organizing a crime. Education and law. 2026;(10):853–861. (In Russ.).*

Современный этап развития общества характеризуется масштабной цифровизацией всех сфер жизнедеятельности, что закономерно влечет за собой трансформацию как правомерного, так и противоправного поведения. На сегодняшний день информационно-телекоммуникационные технологии выступают не только распространенным средством коммуникации и обмена данными, но и высокоэффективным инструментом при совершении преступлений.

Согласно Статистическим данным Генеральной прокуратуры Российской Федерации, уголовно-правовая статистика демонстрирует устойчивый рост числа преступлений, совершаемых с использованием информационно-телекоммуникационных технологий. В частности, в 2025 г. зарегистрировано 675 372 преступления, тогда как в 2019 г. их количество составляло 294 409. Таким образом, за шестилетний период число указанных преступлений увеличилось на 129,4%, что свидетельствует о стремительной цифровизации преступной деятельности и повышении общественной опасности рассматриваемых посягательств.

В юридической литературе предложены различные классификации информационно-телекоммуникационных технологий применительно к преступной деятельности [1, с. 49–52; 2, с. 229–236]. Отдельного внимания заслуживает классификация способов совершения преступлений с использованием информационно-телекоммуникационных технологий, которая зависит от стадии преступной деятельности. В зависимости от этапа реализации преступного умысла выделяются:

способы подготовки к совершению преступления;

способы непосредственного совершения преступного деяния.

К первой группе относится, например удаленный доступ к устройствам потерпевшего, позволяющий провести анализ их уязвимости, установка специальных программ, предназначенных для анализа защищенности устройств жертвы от внешних угроз, установление контакта с потенциальной жертвой посредством социальных сетей, электронной переписки и иных средств коммуникации; получение и анализ персональных данных и иной личной информации о потенциальной жертве с использованием скомпрометированных баз данных (в том числе государственных сервисов).

При этом, как показывает анализ судебной и

следственной практики, информационно-телекоммуникационные технологии все чаще применяются как исполнителями преступлений, так и организаторами.

Наглядной иллюстрацией служит деятельность мошеннических центров, использующих генеративные нейросети и автоматизированных чат-ботов. В таких схемах исполнители вступают в контакт с потерпевшими через IP-телефонию или мессенджеры, применяя заранее сгенерированные алгоритмами сценарии обмана, тогда как организатор осуществляет дистанционное управление всей преступной инфраструктурой. Он внедряет алгоритмы, которые посредством Telegram-ботов или голосовых ИИ-ассистентов вербуют подставных лиц для обналаживания похищенных средств, автоматически распределяет задания между соучастниками, учитывая их загруженность и место нахождения, а также использует систему контроля, отслеживающую выполнение задач и направляющую напоминания, угрозы или поощрения.

В этой связи указанная выше классификация может быть дополнена такой классификационной группой как способ организации преступлений. Если для исполнителей преступлений информационно-телекоммуникационные технологии, как правило, выступают способом непосредственного воздействия на охраняемые уголовным законом общественные отношения, в частности при неправомерном доступе к компьютерной информации, хищении денежных средств с использованием электронных средств платежа, распространении запрещенных материалов, то для организаторов они приобретают значение универсального инструмента, обеспечивающего реализацию всех стадий организационной деятельности: от постановки цели и разработки плана преступных действий для ее достижения до иных активных действий по объединению усилий других соучастников и направлению их совместной преступной деятельности в стадии подготовки и (или) совершения преступления (покушения на исполнение).

Посредством телекоммуникационных сетей организатор преступления получает возможность дистанционно вовлекать новых участников, проводить их инструктаж, определять задачи и контролировать их исполнение, избегая непосредственного физического контакта с соучастниками. Применение средств шифрования, VPN-сервисов, анонимных сетей и иных технологий анонимиза-

ции позволяет существенно снизить риск идентификации личности организатора и, как следствие, повысить латентность его преступной деятельности.

Таким образом, использование информационно-телекоммуникационных технологий при организации преступлений трансформирует традиционную модель соучастия, придавая организационной преступной деятельности трансграничный, дистанционный и высоколатентный характер. Организатор приобретает возможность руководить соучастниками, находясь вне места совершения преступления, оперативно корректировать преступные планы с учетом изменения обстановки, а также привлекать специалистов узкого профиля, не устанавливая с ними личных контактов. Указанные обстоятельства существенно повышают общественную опасность деяния, поскольку усложняют выявление и раскрытие организованного дистанционно преступления, установление роли каждого участника и, в особенности, доказывание вины организатора. Это, в свою очередь, обуславливает необходимость разработки мер профилактического характера, направленных на нейтрализацию указанных рисков и обеспечение неотвратимости ответственности.

Говоря о тенденциях криминализации, мы неизбежно касаемся вопросов российской уголовно – правовой политики, сохранившей наследие советского периода, характеризующегося превашированием концепции самостоятельной теории ответственности соучастников. Э.Ф. Побегайло определял уголовную политику как направление специальной деятельности государства в области борьбы с преступностью [3, с. 464–465].

В научной литературе на сегодняшний день не утихают споры относительно сущности действующей в нашем государстве уголовной политики. Некоторые ученые придерживаются позиции усиления ее репрессивности [4, 144 с.; 5, с. 310–314], другие же настаивают на необходимости ее либерализации [6, с. 38–39; 7, с. 108; 8, с. 125]. В целом, в данном вопросе очевидно единство мнений относительно неудовлетворительного качества российской уголовной политики [9, с. 44–45; 10, 352 с.; 11, 208 с.; 12, 320 с.; 13, с. 185–197; 14, с. 9–13; 15, с. 38–41].

Еще Г. Гегель обращал внимание на то обстоятельство, что «если положение самого общества шатко, тогда закону приходится посредством наказания устанавливать пример» [16, с. 23], подразумевая, что криминализация тех или иных деяний, а также строгость наказания находятся во взаимосвязи с текущим состоянием общества.

Вопросы, касающиеся борьбы с организованной преступностью, в настоящее время не

менее актуальны, чем и 20 лет назад. Так, по итогам проведенного в мае 2006 года Координационного совещания руководителей федеральных правоохранительных органов сделан вывод о том, что «размеры организованной преступности в России приобретают характер национальной угрозы». Как сообщает «Российская газета» от 16 мая 2006 года, организованная преступность «поразила практически все сферы – политическую, экономическую, социальную».

Очевидная на сегодняшний день глобализация мировых процессов выводит преступность за рамки государственных границ на транснациональный уровень, при этом непосредственно организационная преступная деятельность являет собой реальную угрозу национальной безопасности нашего государства. «Усиливающаяся нестабильность в мире, рост радикальных и экстремистских настроений могут привести к попыткам разрешить нарастающие межгосударственные противоречия за счет поиска внутренних и внешних врагов, к разрушению экономики, традиционных ценностей и игнорированию основных прав и свобод человека» гласит п. 8 Стратегии национальной безопасности Российской Федерации, утвержденной Указом Президента Российской Федерации от 02.07.2021 № 400, буквально указывая на нарастающие угрозы, связанные, в том числе, с масштабированием транснациональной организованной преступной деятельности.

Спустя более 15 лет с момента проведения в мае 2006 года Координационного совещания (о котором указано выше), ситуация в корне не изменилась, и уже в июне 2022 года Генеральным прокурором Российской Федерации в рамках аналогичного совещания также отмечена необходимость борьбы с организованной преступностью, подчеркнуто, что «поскольку подавляющее большинство преступлений, совершаемых в организованных формах, составляют мошенничества и незаконный оборот наркотиков, необходимы системные и в то же время адресные меры, учитывающие широкое криминальное использование информационных технологий». Кроме того, Генеральным прокурором Российской Федерации отмечена актуальность борьбы с организацией незаконной миграции, перемещением оружия и боеприпасов.

Такое положение дел детерминировало потребность принятия законодателем комплекса мер, включающих, в том числе, криминализацию отдельных, самостоятельных составов преступлений в сферах, вызывающих особую озабоченность.

Современная уголовная политика Российской Федерации в качестве одного из приоритет-

ных направлений определяет противодействие преступности. Данный термин активно используется в законодательстве и в научной литературе, однако его содержание по-прежнему остается дискуссионным [17, с. 128–132].

Как отмечалось ранее, применительно к сфере использования информационно-телекоммуникационных технологий при организации преступлений система противодействия приобретает ряд особенностей, обусловленных трансграничным, дистанционным и высоколатентным характером организаторской деятельности.

Большинство научных работ ориентированы на исследование отдельных вопросов компьютерной преступности, мошенничества с использованием электронных средств платежа, однако организационные аспекты использования информационно-телекоммуникационных технологий в механизме преступного поведения остаются недостаточно изученными.

Применительно к сфере противодействия организационной функции при совершении преступлений с использованием информационных средств данная категория приобретает особое значение. Цифровая трансформация преступности существенно расширяет круг потенциальных потерпевших и затрудняет применение традиционных уголовно-правовых механизмов. Это требует переосмысления границ охранительного воздействия уголовного закона, уточнения объектов уголовно-правовой охраны и разработки новых нормативных конструкций, адекватных современным вызовам.

Указанное предопределяет необходимость углубленного исследования уголовно-правовых мер противодействия использованию информационно-телекоммуникационных технологий при организации преступлений.

Уголовное право, с одной стороны, охраняет наиболее значимые общественные отношения от преступных посягательств, с другой – регулирует поведение граждан посредством установления запретов и предписаний. Действующее уголовное законодательство Российской Федерации содержит ряд норм, которые в своей совокупности образуют правовую основу противодействия рассматриваемому виду преступности, которые могут быть дифференцированы на несколько групп в зависимости от их функционального назначения.

Первую группу составляют положения Общей части УК РФ, регламентирующие институт соучастия и определяющие правовой статус организатора преступления, прежде всего, это ч. 3 ст. 33 УК РФ. Уголовный закон выделяет организатора как самостоятельную фигуру соучастия, отличающуюся наибольшей степенью общественной опас-

ности, поскольку именно его действия определяют возникновение, развитие и направленность преступной деятельности. Организатор не просто участвует в преступлении, а зачастую инициирует его, объединяет усилия других соучастников, распределяет роли, обеспечивает координацию и контроль.

Данная норма не содержит прямого указания на возможность использования информационно-телекоммуникационных технологий при выполнении организаторских функций, однако ее толкование в правоприменительной практике позволяет распространять действие на случаи дистанционных организации и руководства. В этой связи закономерно возникает вопрос, насколько нормы действующего уголовного законодательства отвечают цифровой реальности и обеспечивают надлежащим образом охранительную функцию уголовного закона, сводя ее к применению мер уголовной ответственности за совершенное преступление, а также оказывая превентивное воздействие уголовно-правовых норм на сознание и поведение граждан [18, с. 26].

Наряду с этим важное значение имеют положения ст. 35 УК РФ, устанавливающие признаки организованной группы и преступного сообщества. Использование информационно-телекоммуникационных технологий при создании и функционировании таких объединений не меняет их юридической сущности, однако существенно влияет на способы установления устойчивости, сплоченности и иерархичности, что требует дополнительного доктринального осмысления.

К этой же группе следует отнести обстоятельства, отягчающие наказание, предусмотренные п. «т» и «ф» ч. 1 ст. 63 УК РФ. Пункт «т» признает отягчающим обстоятельством совершение умышленного преступления с публичной демонстрацией, в том числе в средствах массовой информации или информационно-телекоммуникационных сетях (включая сеть «Интернет»), а п. «ф» – совершение преступления с использованием программно-аппаратных средств доступа к информационным ресурсам, информационно-телекоммуникационным сетям, доступ к которым ограничен. Применительно к организаторской деятельности данные нормы позволяют учитывать цифровой характер совершаемых действий при назначении наказания, однако их формулировки ориентированы на конкретные способы использования информационно-телекоммуникационных технологий и не охватывают всех возможных форм дистанционного организаторства.

Вторую группу образуют нормы Особенной части УК РФ, устанавливающие ответственность за деяния, непосредственно связанные с органи-

зацией преступной деятельности, в том числе с использованием информационно-телекоммуникационных технологий. В частности, положения Особенной части УК РФ, устанавливающие ответственность за организацию преступлений отдельных видов (ч. 1, 3 ст. 279, ч. 4 ст. 2051, ч. 4 ст. 2811 УК РФ); положения Особенной части УК РФ, устанавливающие ответственность за организацию преступной деятельности (ст. 1102, ст. 1733, ч. 1 ст. 2055, ч. 1 ст. 2822, ч. 2 ст. 3303, ст. 353 УК РФ); положения Особенной части УК РФ, устанавливающие ответственность за организацию преступных групп, организаций, сообществ (ч. 1 ст. 2054, ст. 208, ст. 209, ст. 210, ч. 1 ст. 2813, ч. 1 ст. 2821 УК РФ); положения Особенной части УК РФ, устанавливающие ответственность за организацию действий, являющихся по своей природе непроступными до их организации, но признаваемых противоправными, аморальными или опасными (ст. 1712, ст. 1722, ч. 1, 2 ст. 239, ст. 212, ст. 232, ст. 241, ч. 3 ст. 2841, ст. 3221 УК РФ).

Следует отметить, что перечисленные составы Особенной части УК РФ устанавливают ответственность за сам факт их создания, руководства или участия в них независимо от совершения иных преступлений. При их применении ссылка на ч. 3 ст. 33 УК РФ не требуется, поскольку данные деяния признаются оконченными с момента выполнения организационных действий.

Третью группу составляют иные меры уголовно-правового характера, среди которых особое значение имеет конфискация имущества (ст. 1041 УК РФ). В условиях цифровизации преступной деятельности конфискации могут подлежать не только традиционные виды имущества, но и цифровые активы: криптовалюта, электронные денежные средства, доменные имена, а также технические средства, использованные для организации преступления. Вместе с тем правовое регулирование конфискации цифровых активов остается недостаточно разработанным, что снижает эффективность данной меры применительно к рассматриваемой категории деяний.

Помимо уголовно-правовых мер противодействия исследуемого вида преступности, на наш взгляд, особое внимание необходимо уделить общим и специальным профилактическим мерам.

Важнейшим документом стратегического планирования в рассматриваемой сфере является Концепция государственной системы противодействия противоправным деяниям, совершаемым с использованием информационно-коммуникационных технологий (далее – Концепция), утвержденная Распоряжением Правительства Российской Федерации от 30 декабря 2024 г. № 4154-р. Концепция определяет принципы, це-

ли, задачи и функции государственной системы противодействия, а в качестве основных задач называет: обеспечение защищенности российского общества от противоправных посягательств в информационном пространстве; развитие цифровой грамотности населения и правосознания граждан; повышение результативности расследования преступлений, совершаемых с использованием информационно-телекоммуникационных технологий.

Согласно Концепции, одной из важнейших частей государственной системы должна стать специализированная цифровая платформа, обеспечивающая оперативный обмен информацией между правоохранительными органами, Центральным банком, кредитными организациями и операторами связи. Создание системы эффективного противодействия преступлениям, совершаемым с помощью информационно-телекоммуникационных технологий, является одним из показателей достижения национальной цели развития «Цифровая трансформация государственного и муниципального управления, экономики и социальной сферы».

Институциональный уровень противодействия представлен деятельностью специализированных подразделений по борьбе с противоправным использованием информационно-коммуникационных технологий в структуре МВД России, а также взаимодействием правоохранительных органов с Банком России, кредитными организациями и операторами связи.

Профилактическое направление противодействия, в соответствии с Концепцией, предполагает развитие цифровой грамотности населения, формирование правосознания граждан и их ответственного отношения к использованию информационно-телекоммуникационных технологий, в том числе культуры поведения в цифровом пространстве. Профилактика должна быть ориентирована не только на потенциальных жертв, но и на лиц, склонных к вовлечению в преступную деятельность через сеть Интернет.

Наряду с этим, важнейшим элементом системы противодействия рассматриваемому виду преступности выступает международное сотрудничество и гармонизация уголовного законодательства. Необходимость данного направления обусловлена трансграничным характером организаторской деятельности, осуществляемой с использованием информационно-телекоммуникационных технологий. Территориальная разобщенность организатора, исполнителей и потерпевших, находящихся в разных юрисдикциях, существенно усложняет применение национальных уголовно-правовых мер. В таких условиях эффективное

уголовное преследование возможно только при условии тесного взаимодействия компетентных органов различных государств.

Одним из ключевых направлений такого взаимодействия является обмен оперативной информацией о готовящихся и совершаемых преступлениях, а также о лицах, причастных к их организации. Оперативность и полнота информационного обмена позволяют своевременно выявлять преступные схемы, устанавливать всех соучастников, включая организаторов, и принимать меры по предотвращению преступных посягательств. Для этих целей используются каналы Интерпола, органов внутренних дел, а также двусторонние соглашения о сотрудничестве в борьбе с преступностью.

Не менее значимым является взаимодействие, предполагающее согласованную деятельность правоохранительных органов нескольких государств по сбору доказательств, установлению обстоятельств преступления и привлечению виновных к ответственности. Применительно к использованию информационно-телекоммуникационных технологий при организации преступлений особое значение приобретает возможность получения электронных доказательств, находящихся за пределами национальной территории: данных о соединениях, переписке в мессенджерах, информации о транзакциях в криптовалюте, сведений о серверах и доменных именах. Отсутствие эффективных механизмов трансграничного доступа к таким доказательствам существенно затрудняет доказывание организаторской роли, особенно в условиях, когда преступники используют анонимные сети и средства шифрования.

Важную роль играет также экстрадиция лиц, обвиняемых в организации преступлений с использованием информационно-телекоммуникационных технологий. Однако практика показывает, что различия в национальных правовых системах, отсутствие единых определений киберпреступлений и разный подход к квалификации действий организаторов могут служить препятствием для выдачи. В этой связи особую актуальность приобретает гармонизация уголовного законодательства, направленная на выработку общих подходов.

Существенное значение имеет и правовая помощь по уголовным делам, включающая допросы свидетелей, производство обысков, наложение ареста на имущество и цифровые активы, а также передачу вещественных доказательств. Развитие институтов взаимного признания судебных решений позволило бы упростить процедуры наложения ареста на криптовалютные кошельки и иные цифровые активы, используемые организаторами преступлений. Однако на сегодняшний день меж-

дународно-правовая база в данной сфере остается фрагментарной, что требует дальнейшей работы по заключению универсальных и региональных соглашений.

Таким образом, международное сотрудничество и гармонизация законодательства представляют собой необходимое условие эффективного противодействия использованию информационно-телекоммуникационных технологий при организации преступлений. Без решения вопросов трансграничного взаимодействия и сближения уголовно-правовых норм национальные меры, как бы они ни были совершенны, не смогут в полной мере обеспечить неотвратимость ответственности организаторов, действующих в глобальном цифровом пространстве. Поэтому совершенствование международно-правовых механизмов должно рассматриваться как одно из приоритетных направлений уголовной политики в рассматриваемой сфере.

Важным элементом системы противодействия использованию информационно-телекоммуникационных технологий при организации преступлений является взаимодействие государства с субъектами частного сектора, прежде всего с разработчиками программного обеспечения, операторами связи, провайдерами хостинга и платежными системами. Такое партнерство объективно обусловлено тем, что значительная часть цифровой инфраструктуры находится в частной собственности, и без участия ее владельцев невозможно обеспечить эффективный мониторинг преступной активности. Взаимодействие может выражаться в обмене данными о новых угрозах и уязвимостях, совместной разработке инструментов для выявления аномальной сетевой активности, создании механизмов оперативного уведомления правоохранительных органов о фактах использования соответствующих сервисов для подготовки или совершения преступлений.

Кроме того, перспективным направлением является заключение соглашений, регламентирующих порядок предоставления технических данных, необходимых для установления организаторов и иных соучастников, при соблюдении требований законодательства о защите персональных данных. Эффективность такого сотрудничества напрямую зависит от нормативного закрепления обязанностей и стимулов для технологических компаний, а также от наличия доверительных каналов взаимодействия, исключающих злоупотребления и непропорциональное ограничение прав граждан.

Государство в лице правоохранительных органов должно активно применять современные технологические инструменты для мониторинга

и анализа информационного пространства, включая технологии искусственного интеллекта.

Изложенное подтверждает, что развитие информационно-телекоммуникационных технологий, выступая неотъемлемым условием цифровой трансформации общества, одновременно порождает новые виды преступности, в которых организационная функция приобретает особое значение. Использование информационно-телекоммуникационных технологий на этапе подготовки, планирования, координации и руководства преступной деятельностью существенно трансформирует традиционную модель соучастия, придавая ей дистанционный, трансграничный и высоклатентный характер. Организатор, действующий через зашифрованные каналы связи, анонимные сети и автоматизированные алгоритмы, получает возможность управлять преступной группой без личного контакта с исполнителями, что значительно затрудняет установление его роли и привлечение к ответственности. Указанные обстоятельства объективно требуют переосмысления сложившихся уголовно-правовых подходов и разработки адекватных мер реагирования, соответствующих современным технологическим реалиям.

Изучение действующего уголовного законодательства показывает, что система норм, направленных на противодействие использованию информационно-телекоммуникационных технологий при организации преступлений, меняется, реагируя на новые вызовы и угрозы. Положения Особенной части, предусматривающие ответственность за организационную деятельность, хотя и охватывают широкий круг деяний, не образуют единой системы, а их соотношение с общими нормами о соучастии остается коллизионным.

Учитывая трансграничный характер рассматриваемых преступлений, особое значение приобретает развитие международного сотрудничества. Взаимодействие компетентных органов различных государств должно охватывать обмен оперативной информацией, проведение совместных расследований, экстрадицию и оказание правовой помощи.

Важным компонентом системы противодействия должно стать публично-частное партнерство с технологическими компаниями. Взаимодействие государства с разработчиками программного обеспечения, операторами связи и платежными системами способно обеспечить обмен данными о новых угрозах, создание инструментов мониторинга сетевой активности и оперативное уведомление правоохранительных органов. Такое сотрудничество требует нормативного закрепления взаимных обязанностей и гарантий, исключающих непропорциональное ограничение прав граждан,

но его потенциал в выявлении организаторов преступлений значителен.

Таким образом, противодействие использованию информационно-телекоммуникационных технологий при организации преступлений представляет собой комплексную задачу, решение которой возможно лишь при условии согласованного развития уголовного и уголовно-процессуального законодательства, правоприменительной практики, международного сотрудничества, публично-частного партнерства и профилактической деятельности. Только системный подход, объединяющий указанные направления, позволит нейтрализовать риски, порождаемые цифровой трансформацией преступности, и обеспечить надлежащую уголовно-правовую охрану общественных отношений. Обозначенные научные исследования в данной области могут быть дополнены в сфере реализации уголовно-процессуальных механизмов по разработке конкретных законодательных предложений, методик доказывания организаторской роли в цифровой среде и оценке эффективности применяемых мер, что будет способствовать формированию действенной системы противодействия высокотехнологичной преступности.

Список литературы:

- [1] Полянская Е.П. Классификация способов использования информационно-телекоммуникационных технологий при совершении преступлений // Безопасность бизнеса. 2025. № 2. С. 49–52.
- [2] Сысенко А.В., Горденко А.С. Классификация способов совершения преступлений с использованием информационно-телекоммуникационных технологий // Криминалистика: вчера, сегодня, завтра. 2023. № 2. С. 229–236.
- [3] Побегайло Э.Ф. Уголовная политика современной России: концептуальный подход // Противодействие преступности: уголовно-правовые криминологические и уголовно-исполнительные аспекты: Материалы III Рос. Конгресса уголовного права (29–30 мая 2008 г.). М., 2008. С. 464–465.
- [4] Алексеев А.И., Овчинский В.С., Побегайло Э.Ф. Российская уголовная политика: преодоление кризиса. М., 2006. 144 с.
- [5] Смирнов А.М. К вопросу о чрезмерном гуманизме российской уголовной политики // Образование и наука в России и за рубежом. 2018. № 11 (46). С. 310–314.
- [6] Бабаев М.М., Пудовочкин Ю.Е. Российская уголовная политика XXI века: монография. М.: Юрлитинформ, 2020. С. 38–39.
- [7] Гилинский Я.И. Уголовная политика и человек // Уголовная политика и правопримени-

тельная практика: сб. статей по материалам VI Международной науч.-практ. конференции. СПб., 2019. С. 108.

[8] Мелихов А.А. Реализация уголовной политики в современной России // Наука сегодня: задачи и пути их решения: материалы Междунар. науч.-практ. конференции. В 2 ч. Ч. 2. Краснодар, 2018. С. 125.

[9] Лопашенко Н.А. Уголовная политика по принципу «чего изволите?», или уголовный закон как средство решения всех проблем // Вестник Московского ун-та. Серия «Право». 2015. № 1. С. 44–55.

[10] Лопашенко Н.А. Размышления об уголовном праве. Уголовная политика. Авторский курс: монография. М.: Юрлитинформ, 2025. 352 с.

[11] Бабаев М.М., Пудовочкин Ю.Е. Российская уголовная политика XXI века: монография. М.: Юрлит-информ, 2020. 208 с.

[12] Бабаев М.М., Пудовочкин Ю.Е. Уголовная политика и преступность: трансформация в эпоху социальных перемен. М.: Юрлитинформ, 2023. 320 с.

[13] Дегель П.С. Основания установления уголовной наказуемости деяний // Ученые записки ДВГУ. 1961. Вып. 3. С. 185–197.

[14] Наумов А.В. О состоянии и перспективах отечественного уголовного законодательства («Камо грядеши?») // Уголовное право: стратегия развития в XXI веке: материалы XVIII Междунар. науч.-практ. конференции 21–22 января 2021 г. М.: Проспект, 2021. С. 9–13.

[15] Гилинский Я.И. Уголовное законодательство в современной России: критические заметки // Уголовное право: стратегия развития в XXI веке: материалы XII Междунар. науч.-практ. конференции 29–30 января 2015 г. М.: РГ-Пресс, 2015. С. 38–41.

[16] Гегель Г. Философия права. М.: Мысль, 1990. § 1. С. 23.

[17] Майоров А.В. Противодействие преступности – приоритетное направление в уголовной политике государства // Вопросы современной юриспруденции. 2014. № 34. С. 128–132.

[18] Мартыненко Н.Э. Уголовно-правовая охрана потерпевшего // Автореф. дисс.... док. юрид. наук. М. – 2015. С. 26.

References:

[1] Polyanskaya E.P. Classification of Methods for Utilizing Information and Telecommunication Technologies in the Commission of Crimes // Business Security. 2025. No. 2. pp. 49–52.

[2] Sysenko A.V., Gordenko A.S. Classification of Methods for Committing Crimes Using Information and Telecommunication Technologies //

Criminalistics: Yesterday, Today, Tomorrow. 2023. No. 2. pp. 229–236.

[3] Pobegaylo E.F. Criminal Policy in Modern Russia: A Conceptual Approach // Combating Crime: Criminal Law, Criminological, and Penal Aspects: Proceedings of the III Russian Congress of Criminal Law (May 29–30, 2008). Moscow, 2008. pp. 464–465.

[4] Alekseev A.I., Ovchinsky V.S., Pobegaylo E.F. Russian Criminal Policy: Overcoming the Crisis. Moscow, 2006. 144 p.

[5] Smirnov A.M. On the Issue of Excessive Humanism in Russian Criminal Policy // Education and Science in Russia and Abroad. 2018. No. 11 (46). pp. 310–314.

[6] Babayev M.M., Pudovochkin Yu.E. Russian Criminal Policy of the 21st Century: A Monograph. Moscow: Yurлитinform, 2020. pp. 38–39.

[7] Gilinsky Ya.I. Criminal Policy and the Individual // Criminal Policy and Law Enforcement Practice: Collection of Articles Based on the Proceedings of the VI International Scientific and Practical Conference. St. Petersburg, 2019, p. 108.

[8] Melikhov A.A. Implementation of Criminal Policy in Modern Russia // Science Today: Challenges and Solutions: Proceedings of the International Scientific and Practical Conference. In 2 parts. Part 2. Krasnodar, 2018, p. 125.

[9] Lopashenko N.A. Criminal Policy Based on the Principle of "At Your Service?", or Criminal Law as a Means to Solve All Problems // Bulletin of Moscow University. Series "Law". 2015, No. 1, pp. 44–55.

[10] Lopashenko N.A. Reflections on Criminal Law. Criminal Policy. An Author's Course: A Monograph. Moscow: Yurлитinform, 2025, 352 p.

[11] Babayev M.M., Pudovochkin Yu.E. Russian Criminal Policy in the 21st Century: A Monograph. Moscow: Yurлитinform, 2020, 208 p.

[12] Babayev M.M., Pudovochkin Yu.E. Criminal Policy and Crime: Transformation in an Era of Social Change. Moscow: Yurлитinform, 2023, 320 p.

[13] Dage P.S. Grounds for Establishing Criminal Liability for Acts // Scholarly Notes of the Far Eastern State University (DVGU). 1961, Issue 3, pp. 185–197.

[14] Naumov A.V. On the State and Prospects of Domestic Criminal Legislation ("Quo Vadis?") // Criminal Law: Development Strategy in the 21st Century: Proceedings of the 18th International Scientific and Practical Conference. ...conference held on January 21–22, 2021. Moscow: Prospekt, 2021. pp. 9–13.

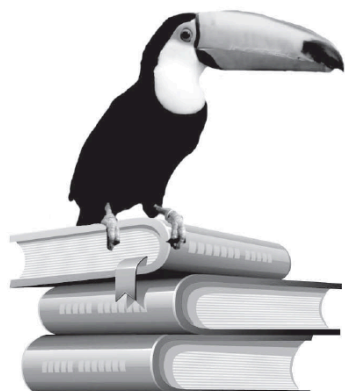
[15] Gilinsky Ya.I. Criminal Legislation in Modern Russia: Critical Notes // Criminal Law: Development Strategy in the 21st Century: Proceedings of the XII International Scientific and Practical Conference, January 29–30, 2015. Moscow: RG-Press, 2015. pp. 38–41.

[16] Hegel G. Philosophy of Right. Moscow: Mysl, 1990. § 1. p. 23.

[17] Mayorov A.V. Combating Crime as a Priority Area of State Criminal Policy // Issues of Modern

Jurisprudence. 2014. No. 34. pp. 128–132.

[18] Martynenko N.E. Criminal Law Protection of the Victim // Abstract of a Doctoral Dissertation in Law. Moscow, 2015. p. 26.



ЮРКОМПАНИ

www.law-books.ru

Юридическое издательство
«ЮРКОМПАНИ»

Издание учебников,
учебных и методических
пособий, монографий,
научных статей.

Профессионально.

В максимально
короткие сроки.

Размещаем
в РИНЦ, E-Library.