УДК 343.98

Гаспарян Гурген Зорикович, к.ю.н,
Академия управления МВД России
Gasparyan Gurgen Zorikovich, PhD in Law,
Academy of Management of the Ministry of Internal Affairs of Russia

МЕЖВЕДОМСТВЕННОЕ ВЗАИМОДЕЙСТВИЕ ПРИ РАССЛЕДОВАНИИ КИБЕРПРЕСТУПЛЕНИЙ: ОТ ДВУСТОРОННИХ СОГЛАШЕНИЙ К ЕДИНОЙ ГОСУДАРСТВЕННОЙ ИНФОРМАЦИОННОЙ СИСТЕМЕ (ПРАВОВОЙ И ОРГАНИЗАЦИОННЫЙ АСПЕКТЫ)

INTERAGENCY COOPERATION IN THE INVESTIGATION OF CYBERCRIMES: FROM BILATERAL AGREEMENTS TO A UNIFIED STATE INFORMATION SYSTEM (LEGAL AND ORGANIZATIONAL ASPECTS)

Аннотация. Статья посвящена исследованию организационно-правовых проблем межведомственного взаимодействия при расследовании преступлений, совершаемых с использованием информационно-телекоммуникационных технологий. Рассматривается комплексное нормативное решение, создающее единую государственную информационную систему противодействия правонарушениям.

Abstract. This article examines the organizational and legal challenges of interagency cooperation in the investigation of crimes committed using information and telecommunications technologies. It examines a comprehensive regulatory solution that creates a unified state information system for combating crime.

Ключевые слова: Киберпреступность, межведомственное взаимодействие, электронный документооборот, государственная информационная система.

Keywords: Cybercrime, interagency cooperation, electronic document management, state information system.

Цифровизация общественных отношений изменила не только повседневную жизнь граждан, но и характер преступной деятельности, что требует от правоохранительных органов адекватного реагирования. Киберпреступность как одна из наиболее динамично развивающихся форм преступной деятельности ставит перед следственными органами задачи, требующие немедленного и слаженного реагирования. В данных условиях межведомственное взаимодействие становится ключевым фактором, определяющим успех расследований в сфере информационно-телекоммуникационных технологий [1, с. 16].

Анализ правоприменительной практики свидетельствует о наличии позитивной динамики: по итогам пяти месяцев 2026 года в отдельных регионах регистрация IT-преступлений сократилась на 28%, а количество краж и мошенничеств в цифровом пространстве – на 23,9% [2]. Вместе с тем общий размер причиненного ущерба остается значительным, что указывает на необходимость дальнейшего совершенствования механизмов противодействия [3]. В этой связи особую значимость приобретает комплексное исследование новых нормативных актов, принятых в 2025-2026 годах и формирующих принципиально новую архитектуру межведомственного взаимодействия при расследовании преступлений в сфере информационно-телекоммуникационных технологий.

В современной практике противодействия преступлениям, совершаемым с использованием информационно-телекоммуникационных технологий, одним из ключевых элементов оперативно-розыскной и следственной деятельности выступает налаживание устойчивого информационного обмена между территориальными и федеральными

подразделениями Министерства внутренних дел Российской Федерации, с одной стороны, и представителями банковского сектора, операторов сотовой связи, а также провайдеров доступа к глобальной сети Интернет, с другой [4]. Теоретически предполагается, что такой обмен должен осуществляться в электронном виде, что обеспечивает оперативность получения значимых для доказывания и идентификации субъектов преступлений сведений.

На сегодняшний день организационная модель этого взаимодействия базируется на заключении двусторонних соглашений об электронном документообороте между МВД России (на федеральном либо региональном уровне) и соответствующими коммерческими структурами. За десятилетний период функционирования данной системы удалось заключить не более десяти-пятнадцати подобных соглашений, что само по себе свидетельствует о низкой институциональной эффективности избранного подхода [5, с. 210].

Первая и наиболее существенная проблема заключается в территориальной несостоятельности регионального уровня заключения таких соглашений. Киберпреступления, как убедительно демонстрирует статистика и эмпирические данные расследований, практически всегда носят межрегиональный, а в значительной части случаев – транснациональный характер. Субъект преступного посягательства, его технические средства и используемые серверные мощности могут находиться в различных субъектах Российской Федерации, а также за пределами национальной юрисдикции [6, с. 101]. В этом контексте заключение соглашения об электронном обмене данными между отдельным территориальным органом МВД России и местным отделением банка или региональным оператором связи лишено практического смысла: такая договоренность не распространяется на контрагентов из других регионов, а потому запросы, направляемые в адрес организаций, головные офисы или серверные мощности которых расположены за пределами конкретного субъекта, остаются без автоматизированного канала исполнения и вновь отправляются по традиционным почтовым либо курьерским маршрутам, что нивелирует саму идею электронного документооборота.

С другой стороны, попытка централизованного заключения генеральных соглашений на федеральном уровне сталкивается с не менее серьезными препятствиями. Во-первых, реализация подобного подхода неизбежно привела бы к колоссальной бюрократической нагрузке на центральный аппарат Министерства, фактически парализовав его оперативные и аналитические функции, поскольку согласование условий обмена с каждым из тысяч действующих банков, операторов и провайдеров превратилось бы в самоцельный и бесконечно длящийся процесс. Во-вторых, рассматриваемая сфера характеризуется высокой динамикой: кредитные организации реорганизуются, теряют лицензии, операторы связи и провайдеры меняют собственников, прекращают деятельность либо, напротив, возникают новые игроки. Заключение федеральных соглашений, рассчитанных на фиксированный перечень участников, оказывается заведомо нежизнеспособным в таких турбулентных условиях, поскольку оперативное включение в систему вновь зарегистрированных организаций либо исключение прекративших существование контрагентов требует повторного прохождения всех бюрократических процедур, что в силу своей протяженности во времени делает эту модель неприменимой для целей быстрого реагирования.

Дополнительным дестабилизирующим фактором, существенно снижающим практическую ценность даже уже заключенных соглашений, выступает гетерогенность технических и процедурных условий взаимодействия. Поскольку унифицированного стандарта электронного обмена между ведомством и внешними организациями не выработано, каждый отдельный контрагент предлагает собственный, зачастую уникальный канал передачи информации. В одном случае направление запроса осуществляется через защищенную ведомственную сеть передачи данных (в частности, ИСОД МВД России), в другом – требуется предварительная авторизация в корпоративном веб-интерфейсе с

использованием логина и пароля или усиленной квалифицированной электронной подписи, в третьем – запросы принимаются исключительно через формализованный почтовый ящик технической поддержки организации, в четвертом – заявителю предлагается заполнить типовую форму запроса по внутреннему регламенту компании, не всегда совместимому с процессуальными требованиями [7, с. 101]. Такое многообразие технических решений, при отсутствии единых стандартов и межплатформенной совместимости, превращает процесс взаимодействия в высокозатратный, малоэффективный и не поддающийся масштабированию комплекс рутинных операций.

Принципиально иной вектор решения обозначенной проблемы открывается в связи с принятием и предстоящей реализацией Федерального закона от 1 апреля 2025 года № 41-ФЗ «О создании государственной информационной системы противодействия правонарушениям, совершаемым с использованием информационных и коммуникационных технологий, и о внесении изменений в отдельные законодательные акты Российской Федерации» [8]. Указанный нормативный правовой акт, вступающий в силу с 1 марта 2026 года (в части создания государственной информационной системы), кардинальным образом трансформирует архитектуру взаимодействия правоохранительных органов с внешними организациями.

Законодателем предусмотрено создание единой государственной информационной системы (далее – ГИС) противодействия правонарушениям, совершаемым с использованием информационных и коммуникационных технологий, оператором которой определено Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации (Минцифры России). Пользователями данной системы, согласно части 6 статьи 1 закона, выступают МВД России, ФСБ России, Роскомнадзор, Росфинмониторинг, Генеральная прокуратура Российской Федерации, Следственный комитет Российской Федерации, Центральный банк России, кредитные организации, операторы связи, организаторы сервисов обмена мгновенными сообщениями, владельцы социальных сетей и сервисов размещения объявлений [8]. Таким образом, впервые на нормативном уровне закрепляется не эксклюзивный перечень контрагентов, связанных двусторонними соглашениями, а открытая система, к которой могут подключаться все субъекты, отнесенные законом к числу пользователей.

Ключевым механизмом информационного обмена в рамках нового правового регулирования выступает единая система межведомственного электронного взаимодействия (далее – СМЭВ). Федеральным законом № 41-ФЗ установлена обязанность кредитных организаций, операторов связи и владельцев агрегаторов информации о товарах (услугах) предоставлять уполномоченным государственным органам, осуществляющим оперативно-разыскную деятельность или обеспечение безопасности, запрошенные сведения с использованием СМЭВ [8]. При этом порядок, сроки, состав и формат предоставления таких сведений устанавливаются Правительством Российской Федерации по согласованию с Банком России (в части кредитных организаций). Для операторов связи и владельцев маркетплейсов соответствующие подзаконные акты уже вступили в силу с 1 сентября 2025 года, для кредитных организаций – с 1 марта 2026 года. В состав передаваемых по запросу уполномоченных органов сведений включен широкий круг данных: абонентские номера, сведения о счетах и операциях по ним, информация о местонахождении пользователя, уникальные идентификаторы устройств (IMEI), данные о транзакциях и иная криминалистически значимая информация.

Также увеличивается с 1 до 3 лет срок, в течение которого организатор распространения информации в Интернете обязан хранить на территории РФ информацию о фактах приема, передачи, доставки или обработки электронных сообщений пользователей Интернета и информацию об этих пользователях (изменения внесены Федеральным законом от 01.04.2025 № 41-ФЗ и Постановлением Правительства РФ от 30.10.2025 № 1698) [9].

Помимо этого, следует также упомянуть Постановление Правительства Российской Федерации от 30.08.2025 № 1344, которое входит в комплекс мер по реализации Концепции государственной системы противодействия преступлениям, совершаемым с использованием ИКТ, утвержденной в декабре 2024 года [10]. Постановлением предусматривается обязанность операторов связи, интернет-провайдеров, организаторов распространения информации уведомлять правоохранительные органы о случаях выявления признаков преступлений, совершаемых с помощью цифровых технологий, а также создание единого реестра адресов электронных ссылок на официальные сайты интернет-магазинов для борьбы с «электронными двойниками» [11].

Вышеуказанные правовые решения позволяют преодолеть все обозначенные выше системные барьеры. Во-первых, исключается необходимость заключения двусторонних соглашений, поскольку обязанность предоставлять информацию возникает непосредственно в силу федерального закона, а универсальность СМЭВ как единой технологической платформы обеспечивает доступ любого уполномоченного территориального органа к данным любой организации, подключенной к системе, вне зависимости от региональной принадлежности запрашивающего подразделения и местонахождения организации-держателя сведений. Во-вторых, единый стандарт электронного взаимодействия через СМЭВ нивелирует проблему гетерогенности технических решений, поскольку все участники системы работают по унифицированным протоколам и форматам обмена данными, что исключает необходимость адаптации к индивидуальным требованиям каждого контрагента. В-третьих, динамика рыночных изменений (появление новых операторов, реорганизация, прекращение деятельности) не нарушает функционирования системы, поскольку подключение к ГИС и СМЭВ осуществляется по единым правилам без пересмотра договорных отношений на индивидуальной основе.

Кроме того, законом вводятся дополнительные механизмы противодействия киберпреступности: обязательная маркировка звонков от организаций, запрет для сотрудников государственных органов, банков и операторов связи на общение с гражданами через иностранные мессенджеры, запрет на передачу SIM-карт третьим лицам (за исключением членов семьи), право абонента на отказ от массовых рассылок, а также возможность установления добровольного запрета на заключение договоров об оказании услуг связи без личного присутствия через Единый портал госуслуг или МФЦ [9]. Предусмотрены также мероприятия по противодействию несанкционированной выдаче наличных денежных средств через банкоматы: кредитные организации обязаны ограничивать выдачу при выявлении признаков отсутствия добровольного согласия клиента.

Таким образом, системное преодоление организационных, технических и правовых барьеров, длительное время препятствовавших эффективному информационному взаимодействию правоохранительных органов с банками, операторами связи и интернет-провайдерами и другими субъектами информационно-телекоммуникационной инфраструктуры, находящихся в юрисдикции Российской Федерации, имеет только комплексное нормативное решение. Успешная реализация положений вышеуказанных нормативно-правовых актов, в первую очередь – создание и полноценное функционирование ГИС и использование СМЭВ как единого канала межведомственного и межорганизационного обмена, способна кардинально повысить оперативность получения криминалистически значимой информации, сократить временные и ресурсные затраты следственных и оперативных подразделений, а также создать устойчивую правовую и технологическую основу для противодействия киберпреступности в условиях стремительно меняющейся цифровой среды.

В перспективе также требуется дальнейшее совершенствование международного сотрудничества в сфере противодействия киберпреступности, включая заключение

двусторонних и многосторонних соглашений о правовой помощи по делам, связанным с использованием информационно-телекоммуникационных технологий. Это позволит преодолеть существующие барьеры при получении доказательственной информации от иностранных провайдеров и операторов связи, что особенно актуально в условиях транснационального характера киберугроз.

Таким образом, комплексный и продуманный подход к совершенствованию межведомственного взаимодействия не только повысит эффективность борьбы с киберпреступностью, но и создаст более безопасную среду для пользователей информационных технологий и цифровых сервисов, что, в свою очередь, создаст благоприятные условия для развития цифровой экономики и повышения уровня доверия граждан к государственным институтам, занимающимся обеспечением правопорядка и защитой их интересов в цифровом пространстве.

Список литературы:

1. Афанасьев П.Б. Отдельные направления противодействия киберпреступности // Проблемы противодействия киберпреступности: материалы международной научно-практической конференции (Москва, 28 апреля 2023 г.). М.: Московская академия Следственного комитета Российской Федерации, 2023. С. 15-19
2. Официальный сайт МВД России. Статистика по итогам пяти месяцев 2026 года [Электронный ресурс] URL: https://мвд.рф/reports/ item/88925539/ (дата обращения: 25.06.2026).
3. В МВД посчитали ущерб от киберпреступлений в России // [Электронный ресурс] URL: https://www.gazeta.ru/tech/news/2026/03/14/28056109.shtml (дата обращения: 25.06.2026).
4. Харитонова С.А. Организационно-правовые проблемы использования системы электронного документооборота в системе МВД // Молодой ученый. 2023. – № 35 (482). – С. 121-125.
5. Шпетная А.В. Взаимодействие правоохранительных органов с банками и операторами сотовой связи в предупреждении дистанционных мошенничеств // Юридическая наука. 2023. №5. С. 209-211.
6. Гаврилин Ю.В., Салеева Ю.Е. Развитие учения о криминалистической регистрации в условиях цифровой трансформации преступности // Труды Академии управления МВД России. 2023. №2 С. 99-105.
7. Горошко И.В. Цифровизация - современный тренд развития правоохранительных органов // Обозреватель - Observer. 2022. №2 (385). С. 94-105.
8. Федеральный закон от 01.04.2025 № 41-ФЗ «О создании государственной информационной системы противодействия правонарушениям, совершаемым с использованием информационных и коммуникационных технологий, и о внесении изменений в отдельные законодательные акты Российской Федерации» // СПС «КонсультантПлюс».
9. Постановление Правительства РФ от 30.10.2025 № 1698 «О внесении изменений в Правила хранения организаторами распространения информации в информационно-телекоммуникационной сети "Интернет" информации о фактах приема, передачи, доставки и (или) обработки электронных сообщений пользователей и предоставления указанной информации уполномоченным государственным органам» // СПС «КонсультантПлюс».
10. Распоряжение Правительства Российской Федерации от 30 декабря 2024 г. № 4154-р «Об утверждении Концепции государственной системы противодействия противоправным деяниям, совершаемым с использованием информационно-коммуникационных технологий» // СПС «КонсультантПлюс».
11. Постановление Правительства РФ от 30.08.2025 № 1344 «О мерах по реализации Концепции государственной системы противодействия преступлениям, совершаемым с использованием информационно-коммуникационных технологий» // СПС «КонсультантПлюс».