Академия управления МВД России

ОРГАНИЗАЦИЯ МЕЖВЕДОМСТВЕННОГО ВЗАИМОДЕЙСТВИЯ ПОДРАЗДЕЛЕНИЙ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ И ПРОТИВОДЕЙСТВИЯ КОРРУПЦИИ СИСТЕМЫ МВД РОССИИ В СФЕРЕ ПРОТИВОДЕЙСТВИЯ ПРЕСТУПЛЕНИЯМ, СОВЕРШАЕМЫМ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

Учебно-методическое пособие

Москва
2023

УДК 343.98
ББК 67.401.213
О64

Одобрено редакционно-издательским советом Академии управления МВД России

Рецензенты: *Агеенков А. А.,* кандидат юридических наук, доцент (Рязанский филиал Московского университета МВД России имени В. Я. Кикотя); *Австрийсков А. В.,* кандидат юридических наук (Волгоградская академия МВД России).

О64

Организация межведомственного взаимодействия подразделений экономической безопасности и противодействия коррупции системы МВД России в сфере противодействия преступлениям, совершаемым с использованием информационно-телекоммуникационных технологий : учебно-методическое пособие / Искалиев Р. Г., Катков Д. В., Телков А. В. [и др.]. – Москва : Академия управления МВД России, 2023. – 68 с.

ISNB 978-5-907530-83-6

В учебно-методическом пособии рассматриваются теоретико-правовые, организационные и методические аспекты межведомственного взаимодействия подразделений экономической безопасности и противодействия коррупции системы МВД России в сфере противодействия преступлениям, совершаемым с использованием информационно-телекоммуникационных технологий.

Учебно-методическое пособие предназначено для преподавателей, адъюнктов, слушателей (курсантов) образовательных организаций МВД России, а также для руководителей и сотрудников подразделений экономической безопасности и противодействия коррупции органов внутренних дел.

УДК 343.98
ББК 67.401.213

ISBN 978-5-907530-83-6

Авторский коллектив

Искалиев Р. Г., кандидат юридических наук;
Катков Д. В., кандидат юридических наук;
Телков А. В., кандидат юридических наук;
Кораблин А. М.;
Грибков С. С.

Содержание

Введение

В современной России функции обеспечения экономической безопасности и противодействия коррупции возложены на различные правоохранительные органы (прокуратура, МВД России, Федеральная служба безопасности Российской Федерации и т. п.). Анализ статистических данных свидетельствует, что ведущая роль в вопросах защиты экономических интересов государства, общества и личности принадлежит органам внутренних дел, подразделения экономической безопасности и противодействия коррупции которых выявляют более 70 % преступлений экономической направленности. Исходя из указанных факторов, возникает необходимость межведомственного взаимодействия с различными правоохранительными органами и ведомствами как одного из важнейших элементов организационно-управленческих мер организации оперативно-розыскной деятельности, в том числе и по вопросам противодействия преступлениям экономической направленности, совершаемым с использованием информационно-коммуникационных технологий.

Так, взаимодействие – это взаимная связь явлений, взаимная поддержка[1].

В широком смысле межведомственное взаимодействие определяется как слаженная работа и деловой контакт различных учреждений и ведомств в противодействии преступности:

– совместная целенаправленная деятельность при определении и реализации стратегии в этом противодействии;

– проведение совместных совещаний на различных уровнях, направленных на повышение оперативного взаимного информирования;

– включение всех сил и средств заинтересованных ведомств при проведении мероприятий в процессе разработки и оперативной проверки, проведении различных тактических операций;

– коллективная разработка тактических действий в отношении организованных групп с учетом существующей и видоизменяющейся системы и структуры этой среды, а также масштабов ее распространения;

– использование возможностей всех заинтересованных органов, учреждений и т. д. по противодействию преступности.

Развитие любой экономики государства будет продиктовано не только экономическими, но и эпидемиологическими, и други-

[1] Ожегов С. И., Шведова Н. Ю. Толковый словарь русского языка. М., 1994. С. 145.

ми факторами. Стремительное распространение коронавирусной инфекции COVID-19, проведение специальной военной операции на территориях Донецкой и Луганской республик, Запорожской и Херсонской областей стали глобальными испытаниями для мировой и российской экономик.

В связи с этим в настоящее время обеспечение экономической безопасности нашего государства является одной из главных задач правоохранительного блока. Достичь нужных результатов возможно лишь при условии правильной и грамотной организации межведомственного взаимодействия с иными правоохранительными органами и ведомствами, а также внедрения и использования современных информационно-коммуникационных технологий для противодействия преступлениям экономической направленности.

Глава 1. Теоретико-правовые аспекты межведомственного взаимодействия подразделений ЭБиПК системы МВД России в сфере противодействия преступлениям, совершаемым с использованием информационно-коммуникационных технологий

1.1. Понятие и классификация преступлений экономической направленности, совершаемых с использованием информационно-коммуникационных технологий

Важно понимать, что использование информационно-телекоммуникационных сетей (средств, инструментов) чаще всего выступает лишь способом совершения отдельных экономических и коррупционных преступлений. При этом в широких кругах до сих пор бытует ошибочное толкование по факту отношения преступления к той или иной сфере в связи с привязкой отдельных деяний к какой-либо из них (жилищно-коммунальное хозяйство, топливно-энергетической комплекс). Примером указанного суждения может быть то, что преступник в ходе причинения отдельному лицу повреждений с использованием орудия преступления в виде лопаты явно не совершает преступление с оттенком «сельское хозяйство или строительство», поскольку лопата относится к сельскохозяйственному или строительному инвентарю. Также и преступление по факту хищения, например, женской сумочки из помещения, принадлежащего какой-либо государственной структуре, не будет коррупционным, а будет иметь общеуголовный оттенок без привязки к месту совершения преступления. Таким образом, важно выработать правильное отношение со стороны правоохранителей к такому роду преступлений и четко понимать, что в одних случаях экономические и коррупционные преступления совершаются в информационно-телекоммуникационной сети, в других случаях они могут совершаться при помощи таких цифровых инструментов, а в иных – могут носить комбинированный оттенок.

Полагаем, что под компьютерной преступностью следует понимать социальное и уголовно-правовое явление, представляющее собой систему преступлений, совершенных с использованием информационных компьютерных технологий[1].

[1] Тутуков А. Ю. Основные детерминанты компьютерной преступности в Российской Федерации // Пробелы в российском законодательстве. 2018. № 3. С. 44.

Между тем обобщающим признаком преступлений в сфере информационно-коммуникационных технологий, по нашему мнению, выступают именно те самые «технологии», которые с определенной степенью однозначности требуют особого подхода к выявлению причин и условий их совершения, а также организации и методики предупредительного воздействия.

В свою очередь А. В. Аносов и Е. С. Кашапова в одной из своих работ приходят к закономерному выводу о том, что криминологическая дефиниция «преступления в сфере высоких технологий» представляет собой обобщающее понятие совокупности преступлений, совершенных с использованием современных сложных технологий, относящихся к наукоемким отраслям производства или обслуживания[1].

Данное мнение подтверждается тем, что такие преступления совершаются с использованием сложных технических устройств, понимание функционирования которых требует определенного базового «порога вхождения» для лиц, участвующих в указанной сфере общественных отношений.

Важными и необходимыми элементами научного обеспечения предупреждения преступности являются унификация и легитимизация терминов и определений, заметно сужающие возможность их расширительного толкования, включая и процесс правоприменения[2].

Таким образом, в настоящее время усматривается правовой пробел в данной отрасли, который отражает отсутствие законодательного закрепления отдельно взятых понятий и положений, таких как «киберпреступления», «преступления в сфере высоких технологий», «киберпреступность». Этот факт косвенно подтверждается тем, что в научных кругах указанные понятия рассматриваются с разных научных позиций.

Н. Р. Шевко считает, что понятие «преступление, совершаемое с использованием высоких технологий» носит собирательный характер, употребляется в случаях, когда для «совершения» традиционных в уголовном праве преступлений используются информационные технологии, ответственность за которые предусмотре-

---

[1] Аносов А. В., Кашапова Е. С. Понятие преступлений в сфере высоких технологий // Академическая мысль. 2018. № 4.

[2] Никеров Д. М., Хохлова О. М. Преступления в сфере высоких технологий в современной России // Вестник Восточно-Сибирского института МВД России. 2019. № 2.

на ст. 159.3, 159.6, 187 Уголовного кодекса Российской Федерации (далее – УК РФ)[1].

А. И. Фоменко считает, что термин «преступления в сфере высоких технологий» необходимо использовать как самостоятельную уголовно-правовую категорию в российском и международном уголовно-правовом законодательствах[2].

Преступления в сфере информационно-коммуникационных технологий ввиду отсутствия четких законодательных положений и дефиниций различными исследователями отождествляются по-разному, в соответствии прежде всего с личными, субъективными представлениями и степенью понимания информационно-коммуникационной среды, вовлеченности того или иного исследователя в современные тенденции развития и функционирования высоких технологий. Нормативно-правовое закрепление понятия «преступления в сфере высоких технологий» подразумевает его понимание в более широком смысле, не ограничивающемся конкретным средством, способом или относимостью к определенному типу технологий или информации. С криминологической стороны «преступления в сфере высоких технологий» относятся к категории противоправных уголовно наказуемых деликтов, которые совершаются с использованием наукоемких, современных технологий и инструментов в сфере информационно-телекоммуникационных технологий, руководство которыми осуществляется с помощью электронно-вычислительных систем и механизмов, в том числе и при использовании сети Интернет и других сетей общего и ограниченного доступа.

Под коррупционными и экономическими преступлениями, совершаемыми с использованием информационно-коммуникационных технологий в широком понимании, определяют категорию преступлений, которая по своей природе имеет отношение к получению и даче взяток, превышению и злоупотреблению должностными полномочиями, халатному отношению к своим профессиональным обязанностям. Между тем к экономическим преступлениям в рассматриваемой сфере относятся противоправные деяния, предусмотренные гл. 21, 22, 23 УК РФ, которые посягают на установленный порядок предпринимательской деятельности и осуществления

[1] Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ : принят Гос. Думой 24 мая 1996 г., одобр. Советом Федерации 5 июня 1996 г. // СПС КонсультантПлюс (дата обращения: 06.03.2022).

[2] Фоменко А. И. К вопросу об уголовно-правовой охране сферы высоких технологий как необходимого условия стабильного регионального развития // Интеллектуальные ресурсы – региональному развитию. 2015. № 1–5. С. 217–222.

службы как в коммерческих, так и в иных организациях вне зависимости от их формы учреждения.

При необходимости квалификации преступлений в сфере информационно-коммуникационных технологий (в том числе сети Интернет) в качестве коррупционных либо экономических следует обращаться к действующему указанию Генеральной прокуратуры Российской Федерации и МВД России № 11/11/1 от 17 января 2023 г., используемому для формирования статистической отчетности[1], в положениях которого содержатся квалифицирующие признаки и примечания, помогающие определить отношение того или иного противоправного деликта к экономическому или коррупционному, а также совершенному с использованием информационно-коммуникационных технологий (справочник № 25).

Обращаясь к постановлению Пленума Верховного Суда Российской Федерации от 9 июля 2013 г. № 24 «О судебной практике по делам о взяточничестве и об иных коррупционных преступлениях»[2], необходимо отметить, что при разрешении вопроса о том, совершено ли коррупционное преступление должностным лицом, судам следует руководствоваться прим. 1, 2 и 3 к ст. 285, прим. 2 к ст. 290, прим. 1 к ст. 201 УК РФ, учитывая при этом соответствующие разъяснения, содержащиеся в постановлении Пленума Верховного Суда Российской Федерации от 16 октября 2009 г. № 19 «О судебной практике по делам о злоупотреблении должностными полномочиями и о превышении должностных полномочий»[3].

Обратившись к постановлению Пленума Верховного Суда Российской Федерации от 16 октября 2009 г. № 19 «О судебной практике по делам о злоупотреблении должностными полномочиями и о превышении должностных полномочий», необходимо отметить правила установления того, является ли субъект преступлений должностным лицом. При этом следует исходить из того, что в соответствии с п. 1 прим. к ст. 285 УК РФ должностными признаются лица, постоянно, временно или по специальному полномочию

---

[1] О введении в действие перечней статей Уголовного кодекса Российской Федерации, используемых при формировании статистической отчетности : указание Генеральной прокуратуры Рос. Федерации, МВД России от 17 января 2023 г. № 11/11/1 // СПС КонсультантПлюс (дата обращения: 06.02.2003).

[2] О судебной практике по делам о взяточничестве и об иных коррупционных преступлениях : постановление Пленума Верховного Суда Рос. Федерации от 9 июля 2013 г. № 24 // СПС КонсультантПлюс (дата обращения: 06.02.2022).

[3] О судебной практике по делам о злоупотреблении должностными полномочиями и о превышении должностных полномочий : постановление Пленума Верховного Суда Рос. Федерации от 16 октября 2009 г. № 19 // СПС КонсультантПлюс (дата обращения: 06.02.2022).

выполняющие обязанности представителя власти, либо осуществляющие организационно-распорядительные, административно-хозяйственные функции.

Можно сделать вывод о том, что вне зависимости от способа (метода) совершения преступления, отнесения такого преступления к категории коррупционных либо экономических определяется на общих основаниях в рамках действующего законодательства.

Преступления экономической и коррупционной направленности, совершаемые в сфере информационно-коммуникационных технологий, обладают характерными признаками:

1) для реализации преступного замысла используются достижения технического прогресса, науки в области информационно-телекоммуникационных технологий;

2) совершаются должностными, материально ответственными и иными лицами, выполняющими на предприятиях, в учреждениях и организациях независимо от форм собственности и организационно-правовых форм организационно-распорядительные или административно-хозяйственные функции в процессе осуществления ими производственно-хозяйственной или финансовой деятельности (в том числе лицами, не наделенными указанными полномочиями, но имеющими доступ к предмету преступного посягательства для выполнения трудовых обязанностей по роду деятельности или службы);

3) наличие связи деяния со служебным положением, наличие корыстного мотива;

4) наличие субъекта уголовно наказуемого деяния, которым может быть должностное лицо, указанное в прим. к ст. 285 УК РФ (в том числе лицо, выполняющее управленческие функции в коммерческой или иной организации, действующее от имени юридического лица, а также в некоммерческой организации, не являющейся государственным органом, органом местного самоуправления, государственным или муниципальным учреждением, указанное в примечании к ст. 201 УК РФ);

5) противоправные деяния зачастую носят экстерриториальный размах.

Отдельное пояснение в рамках уголовно-правовой отрасли сделано Верховным Судом Российской Федерации. Так, в постановление Пленума от 9 июля 2013 г. № 24 «О судебной практике по делам о взяточничестве и об иных коррупционных

преступлениях»[1] внесены соответствующие изменения, в рамках которых определено, что предметом взятки могут стать и цифровые права.

В настоящее время мы имеем расширенное толкование предмета взятки, упомянув в качестве такового цифровые права, которые в соответствии со ст. 141.1 Гражданского кодекса Российской Федерации признаны имуществом, в связи с чем следует, что для дачи уголовно-правовой оценки тому или иному противоправному деянию такая категория имущества, как «цифровые права», должна иметь стоимостное денежное выражение. К примеру, категория цифровых прав «криптовалюта», определяемая как предмет взятки, должна быть оценена экспертом (специалистом), который может руководствоваться открытой и общедоступной информацией из криптовалютных бирж, официально зарегистрированных как на территории Российской Федерации, так и за ее пределами, в целях определения среднего значения искомой стоимости отдельно взятого цифрового права. И в случае, если эксперт, определяя денежное выражение для криптовалюты, сошлется на такой метод, то доказательство может быть признано допустимым. При этом необходимо отразить тот факт, что официально разработанных и описанных методик оценки критовалютных инструментов, а равно каких-либо иных цифровых прав в настоящее время не имеется. Однако постановление Девятого арбитражного апелляционного суда по делу № А40-124668/201747[2] указывает на существование возможности оценки криптовалюты как в рамках гражданского производства, так и в рамках производства, связанного с проверкой, основанной на наличии признаков коррупционного или экономического преступления, предметом которого может быть как криптовалюта, так и иной объект цифровых прав, признаваемый отечественным законодательством.

Приведем ряд примерных составов экономических и коррупционных преступлений, которые по своим признакам и характерным особенностям могут иметь отношение к тем, которые совершаются в сфере информационно-коммуникационных технологий (табл. 1).

---

[1] О судебной практике по делам о взяточничестве и об иных коррупционных преступлениях : постановление Пленума Верховного Суда Рос. Федерации от 9 июля 2013 г. № 24 // СПС КонсультантПлюс (дата обращения: 06.02.2022).

[2] Постановление Девятого арбитражного апелляционного суда по делу № А40-124668/2017 // Картотека арбитражных дел. URL: https://kad.arbitr.ru/Document/Pdf/3e155cd1-6bce-478a-bb76-1146d2e61a4a (дата обращения: 21.11.2022).

Таблица 1

Примерные составы экономических и коррупционных преступлений, которые по своим признакам и характерным особенностям могут иметь отношение к тем, которые совершаются в сфере информационно-коммуникационных технологий

№ статьи (состава) УК РФ	Краткое описание примерного состава преступления (объективной стороны противоправного деяния)	Дополнительные условия для квалификации преступления в качестве экономического или коррупционного
158	Кража цифровых активов, произведенная с использованием электронного средства платежа	Совершение преступления должностными либо материально ответственными лицами, выполняющими административно-хозяйственные функции в организациях и учреждениях различных форм собственности
159	Мошенничества, связанные с вовлечением лиц в финансирование криптовалютных пирамид	Совершение преступления лицами, не наделенными должностными полномочиями, но имеющими доступ к предмету преступного посягательства
159.1	Мошенничества, связанные с получением кредита (использование заведомо ложных обеспечительных сведений об имеющихся цифровых активах)	Совершение преступления должностными лицами, выполняющими организационно-распорядительные функции в организациях и учреждениях различных форм собственности
159.6	Хищение цифровых активов с криптовалютных кошельков (бирж данных, хранилищ цифровой валюты)	Совершение преступления должностными лицами, а равно лицами, не наделенными служебными полномочиями, но имеющими доступ к предмету преступного посягательства
171.2	Незаконная организация и проведение азартных игр (осуществляется с использованием информационно-телекоммуникационных сетей, в том числе сети Интернет)	Не требуется дополнительных условий для квалификации в качестве экономического преступления
193	Уклонение от исполнения обязанностей по репатриации денежных средств в иностранной валюте или валюте Российской Федерации	Не требуется дополнительных условий для квалификации в качестве экономического либо коррупционного преступления

193.1	Совершение валютных операций по переводу денежных средств в иностранной валюте или валюте Российской Федерации на счета нерезидентов с использованием подложных документов (цифровых финансовых активов)	Не требуется дополнительных условий для квалификации в качестве экономического либо коррупционного преступления
196, 197	Преднамеренное или фиктивное банкротство (при наличии скрытых цифровых финансовых активов, электронных средств платежа)	Не требуется дополнительных условий для квалификации в качестве экономического либо коррупционного преступления
198, 199	Уклонение от уплаты обязательных сборов, налогов, страховых взносов (в том числе при наличии скрытых цифровых финансовых активов, электронных средств платежа)	Не требуется дополнительных условий для квалификации в качестве экономического либо коррупционного преступления
204	Коммерческий подкуп, осуществляемый цифровыми финансовыми активами	Не требуется дополнительных условий для квалификации в качестве коррупционного преступления
290, 291, 291.1, 291.2	Получение взятки, дача взятки, посредничество во взяточничестве, мелкое взяточничество (предметом которого являются цифровые финансовые активы)	Не требуется дополнительных условий для квалификации в качестве коррупционного преступления

Можно сделать вывод, что для квалификации противоправного деликта, имеющего коррупционный либо экономический оттенок в сфере информационно-коммуникационных технологий (в том числе сети Интернет), достаточно наличия в виде предмета или способа совершения преступления отдельно взятых инструментов (электронные кошельки) либо имущества в виде цифровых финансовых активов.

Ключевая особенность совершения преступлений в сфере компьютерной информации связана с использованием технологически сложных систем и средств. Порог вхождения в разряд «уверенных» пользователей современных технических средств и систем достаточно высок, при этом зачастую граждане Российской Федерации ввиду различных социально-экономических причин не готовы или не хотят осваивать современные устройства и связанные с использованием таких устройств правила и особенности

их применения. Зачастую неправильное использование электронных механизмов приводит к невозможности возврата потерянных материальных ценностей, что является для преступных элементов благодатной почвой для осуществления противоправных действий по завладению чужим имуществом.

Между тем результаты проведенного эмпирического исследования в свою очередь говорят о высокой ликвидности и рентабельности деятельности по использованию цифровых (криптографических) валют. Использование указанных инструментов в условиях высокого уровня анонимизации последних может свидетельствовать о высокой степени латентности преступлений, совершаемых в сфере информационно-телекоммуникационных технологий, при этом данный тезис может быть усилен в том числе и тем, что в настоящее время уголовно-правовое и административное законодательство Российской Федерации не оптимизировано и в целом не готово отвечать на вопросы, связанные с квалификацией состава тех или иных событий, происходящих в сфере развития общественных отношений в области цифровых технологий.

1.2. Правовое регулирование межведомственного взаимодействия подразделений ЭБиПК по противодействию преступлениям экономической направленности, совершаемым с использованием информационно-коммуникационных технологий

В общей теории права под правовым регулированием понимается государственная деятельность органов и должностных лиц по упорядочению общественных отношений посредством установления правовых норм и принятия в необходимых случаях индивидуально регламентирующих решений в соответствии с этими нормами по юридически значимым вопросам, возникающим в рамках таких отношений[1].

На сегодняшний день правовую основу и систему нормативных правовых источников рассматриваемого нами вида деятельности принято делить на 5 уровней (групп). К первому уровню относят Конституцию и федеральные конституционные законы; ко второму – положения международных правовых актов; к третьему – федеральные законы; к четвертому – подзаконные норматив-

[1] См.: Фаткуллин Ф. Н. Проблемы теории государства и права : курс лекций. Казань: Казан. ун-т, 1987. С. 135; Годунов И. В. Энциклопедия противодействия этнической преступности. 2-е изд., перераб. и доп. М., 2005. С. 497.

ные правовые акты федеральных органов государственной власти (указы Президента Российской Федерации и постановления Правительства); к пятому – ведомственные и межведомственные нормативные акты государственных органов[1].

Анализируя нормы Конституции Российской Федерации (далее – Конституция)[2], следует отметить, что они имеют прямое действие и непосредственно затрагивают экономическую и правоохранительную сферы. На конституционном уровне гарантируются единство экономического пространства, свободное перемещение товаров, услуг и финансовых средств, поддержка конкуренции, свобода экономической деятельности (п. 1 ст. 8 Конституции), что обеспечивается положениями, прямо указывающими на цели оперативно-розыскной деятельности (ст. 1 Федерального закона «Об оперативно-розыскной деятельности» от 12 августа 1995 г. № 144-ФЗ (далее – ФЗ «Об ОРД»)). К таковым относятся защита прав и свобод граждан (п. 2 ст. 6 Конституции), различных форм собственности (п. 2 ст. 8), безопасность общества и государства от преступных посягательств. Конституция содержит в себе правовую основу межведомственного взаимодействия различных правоохранительных органов государства по обеспечению экономической безопасности. В соответствии с нормами последней на Президента Российской Федерации возлагаются обязанности по принятию мер, направленных на охрану суверенитета, независимости, государственной целостности, обеспечению согласованного функционирования и взаимодействия органов государственной власти Российской Федерации.

Нельзя не упомянуть и о том, что некоторые конституционные нормы являются основополагающими для регламентации ряда оперативно-розыскных действий, в частности, п. 2 ст. 23 Конституции определяет, что ограничение права граждан на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений допускается на основании судебного решения.

Важнейшая роль в правовом регулировании ОРД принадлежит специальному отраслевому законодательному акту – ФЗ «Об ОРД». С его принятием в нашей стране получила дальнейшее развитие правовая основа ОРД в части некоторых новых направлений, в том числе тех, которые затрагивают обеспечение экономической без-

---

[1] Теория оперативно-розыскной деятельности : учебник / под ред. К. К. Горяинова, В. С. Овчинского, Г. К. Синилова. М. : Норма, 2006. С. 51.

[2] Конституция Российской Федерации : принята всенар. голосованием 12 дек. 1993 г. : с изм., одобренными в ходе общерос. голосования 1 июля 2020 г. // СПС КонсультантПлюс (дата обращения: 14.11.2022).

опасности государства. Кроме того, в законе указано, что органы, осуществляющие ОРД для решения задач, возложенных на них законом, могут создавать и использовать информационные системы, а также заводить дела оперативного учета (далее – ДОУ).

Дополнение Федеральным законом от 6 июня 2016 г. № 374-ФЗ[1] ст. 6 ФЗ «Об ОРД» 15-м ОРМ (получение компьютерной информации) свидетельствует о заинтересованности законодателя в расширении арсенала инструментов оперативных подразделений, в том числе ЭБиПК, по противодействию преступлениям, совершаемым с использованием информационных технологий и телекоммуникаций (далее – ИТТ).

Актуальным является вопрос проявления у законодателя интереса к такому ОРМ, как «мониторинг информационно-телекоммуникационных сетей и систем»[2], на которое было обращено внимание на двадцать седьмом пленарном заседании Межпарламентской Ассамблеи государств – участников Содружества Независимых Государств.

На современном этапе развития цифровых способов взаимных расчетов между хозяйствующими субъектами и гражданами, на наш взгляд, имеется необходимость в создании и законодательном закреплении механизмов контроля субъектами ОРД в режиме реального времени электронных взаиморасчетов для предотвращения возможных преступных проявлений в экономической деятельности со стороны недобросовестных предпринимателей и граждан.

При рассмотрении возможных вариантов развития законодательства в области контроля электронных взаиморасчетов необходимы законодательное закрепление и детальная проработка механизма идентификации электронной единицы расчета. Анализируя правоприменительную практику, мы приходим к выводу, что подразделения ЭБиПК зачастую сталкиваются с проблемами документирования процесса вывода доходов, полученных преступным путем, в том числе на счета банковских учреждений, расположенных в офшорных юрисдикциях, и движения денежных средств в ходе совершения преступных транзакций.

---

[1] О внесении изменений в Федеральный закон «О противодействии терроризму» и отдельные законодательные акты Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности : Федеральный закон от 6 июля 2016 г. № 374-ФЗ : принят Гос. Думой 24 июня 2016 г. : одобр. Советом Федерации 29 июня 2016 г. // Собр. законодательства Рос. Федерации. 2016. № 28. Ст. 4558.

[2] Модельный закон «Об оперативно-розыскной деятельности» (принят постановлением на десятом пленарном заседании Межпарламентской Ассамблеи государств – участников СНГ от 6 декабря 1997 г. № 10-12). URL: https://base.garant.ru/2569039 (дата обращения 05.03.2022).

Для решения указанной проблемы необходима цифровая «метка» денежной единицы для ее идентификации в общем потоке транзакций. Реализация данной процедуры возможна при закреплении ее в ФЗ «Об ОРД» как самостоятельного ОРМ – «контроль данных в информационно-телекоммуникационных сетях и системах». Предлагаемое нами ОРМ позволит отслеживать представляющие оперативный интерес транзакции лиц, подозреваемых или обвиняемых в совершении преступления средней тяжести, тяжкого и особо тяжкого преступления, проведение которого будет допускаться на основании судебного решения.

В результате проведенного опроса большинство (79,7 %) сотрудников подразделений ЭБиПК высказались в пользу необходимости дополнительного инструмента документирования преступлений экономической направленности, совершаемых с использованием ИТТ, и включения в ФЗ «Об ОРД» ОРМ (например *«контроль данных в информационно-телекоммуникационных сетях и системах»),* которое позволит отслеживать представляющие оперативный интерес транзакции.

«Контроль данных в информационно-телекоммуникационных сетях и системах» в ст. 6 ФЗ «Об ОРД» предлагается рассматривать как «ОРМ, в рамках которого производится негласное установление уникального идентификационного цифрового кода (цифровой метки) на электронные данные и дальнейшая их фиксация путем наблюдения с применением специальных технических средств за характеристиками электромагнитных и других физических полей, возникающих при обработке информации в информационных системах и базах данных и ее передаче по сетям электрической связи, компьютерным сетям и иным телекоммуникационным системам».

На основании ст. 10 Федерального закона от 7 февраля 2011 г. № 3-ФЗ «О полиции»[1] полиция при осуществлении своей деятельности взаимодействует с другими правоохранительными органами, государственными и муниципальными органами, общественными объединениями, организациями и гражданами.

Правовую основу составляет также УК РФ, который определяет ответственность за преступления в сфере экономики в разделе VIII, состоящем из трех глав (гл. 21–23).

Уголовно-процессуальный закон определяет порядок взаимодействия следователя и оперативного сотрудника при расследова-

[1] О полиции : Федеральный закон от 7 февраля 2011 г. № 3-ФЗ : принят Гос. Думой 28 января 2011 г. : одобр. Советом Федерации 2 февраля 2011 г. // Официальный интернет-портал правовой информации. URL: http: // pravo.gov.ru (дата обращения: 06.03.2022).

нии преступлений (ч. 4 ст. 157, ч. 2 ст. 163, ч. 7 ст. 164); устанавливает перечень преступлений, по которым обязательно предварительное следствие (ст. 150), что согласно ст. 8 ФЗ «Об ОРД» является обязательным условием осуществления ОРМ, ограничивающих конституционные права граждан.

К законодательным актам, регулирующим отношения, возникающие при решении частных задач ОРД, можно отнести следующие законодательные акты.

Федеральным законом «О связи»[1] определяются вопросы взаимодействия предприятий связи с органами, осуществляющими ОРД. Предприятия связи, операторы связи независимо от ведомственной принадлежности и форм собственности, действующие на территории Российской Федерации, при разработке, создании и эксплуатации сетей связи обязаны в соответствии с законодательством Российской Федерации оказывать содействие и предоставлять органам, осуществляющим ОРД, возможность проведения ОРМ на сетях связи, принимать меры к недопущению раскрытия организационных и тактических приемов проведения указанных мероприятий.

Данным законом нормативно закреплены предписания, касающиеся соблюдения тайны связи, в частности, «Прослушивание телефонных переговоров, ознакомление с сообщениями электросвязи, задержка, осмотр и выемка почтовых отправлений и документальной корреспонденции, получение сведений о них, а также иные ограничения тайны связи допускаются только на основании судебного решения».

Помимо прочего законодатель определил обязанности операторов связи и ограничение прав пользователей услугами связи при проведении ОРМ.

Принятый 31 июля 2020 г. Федеральный закон «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации» № 259-ФЗ[2] установил правила выпуска цифровых финансовых активов, оборота цифровой валюты (криптовалюты), а также запретил принимать оплату товаров, работ и услуг цифровой валютой. Следу-

---

[1] О связи : Федеральный закон от 7 июля 2003 г. № 126-ФЗ : принят Гос. Думой 18 июня 2003 г. : одобр. Советом Федерации 25 июня 2003 г. // СПС КонсультантПлюс (дата обращения: 06.03.2022).

[2] О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации : Федеральный закон от 31 июля 2020 г. № 259-ФЗ : принят Гос. Думой 22 июля 2020 г. : одобр. Советом Федерации 24 июля 2020 г. // СПС КонсультантПлюс (дата обращения: 06.03.2022).

ет отметить, что до настоящего времени криптовалюта не признана имуществом в уголовном законодательстве, что существенно затрудняет квалификацию уголовно наказуемых деяний, в том числе экономической направленности с использованием ИТТ.

Ряд законов регламентируют процедуру получения сведений, составляющих тайну частной жизни граждан, а также иные защищаемые законом тайны.

Федеральный закон «О банках и банковской деятельности» от 2 декабря 1990 г. № 395-1[1] устанавливает, что справки по операциям и счетам юридических лиц и индивидуальных предпринимателей, по операциям, счетам и вкладам физических лиц выдаются на основании судебного решения кредитной организацией должностным лицам органов, уполномоченных осуществлять ОРД, при выполнении ими функций по выявлению, предупреждению и пресечению преступлений по их запросам, направляемым в суд в порядке, предусмотренном ст. 9 ФЗ «Об ОРД», при наличии сведений о признаках подготавливаемых, совершаемых или совершенных преступлений, а также о лицах, их подготавливающих, совершающих или совершивших, если нет достаточных данных для решения вопроса о возбуждении уголовного дела. Перечни указанных должностных лиц устанавливаются нормативными правовыми актами соответствующих федеральных органов исполнительной власти. Говоря о данном положении, следует отметить тот факт, что в порядке, предусмотренном ст. 9 ФЗ «Об ОРД», рассматриваются также ходатайства органов, осуществляющих ОРД, о предоставлении кредитными организациями справок по операциям и счетам юридических лиц и индивидуальных предпринимателей, по операциям, счетам и вкладам физических лиц. Указанные справки, согласно внесенным 1 апреля 2022 г. изменениям, предоставляются кредитными организациями на основании судебного решения в течение десяти рабочих дней со дня получения соответствующего постановления суда.

Федеральным законом «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма»[2] определены такие дефиниции, как «доходы, полученные преступным путем», «легализация», «уполномоченный орган», «обязательный контроль», «внутренний контроль» и дру-

[1] О банках и банковской деятельности : Федеральный закон от 2 декабря 1990 г. № 395-1 // СПС КонсультантПлюс (дата обращения: 06.03.2022).

[2] О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма : Федеральный закон от 7 августа 2001 г. № 115-ФЗ : принят Гос. Думой 13 июля 2001 г. : одобр. Советом Федерации 20 июля 2001 г. // СПС КонсультантПлюс (дата обращения: 30.03.2022).

гие. Данный акт регулирует вопросы предупреждения легализации доходов, определяет круг организаций, ответственных за исполнение закона: кредитные организации, страховые, лизинговые компании, почта, ломбарды и другие.

К нормативным правовым актам, регламентирующим отдельные вопросы межведомственного взаимодействия, можно отнести указы Президента Российской Федерации, определяющие основные направления деятельности подразделений ЭБиПК ОВД в области экономической безопасности[1].

Экономическая безопасность Российской Федерации, наряду с информационной безопасностью, крайне подробно охарактеризована в Стратегии национальной безопасности Российской Федерации[2], утвержденной указом Президента Российской Федерации от 2 июля 2021 г. № 400. В данном нормативном правовом акте охарактеризованы существующие в настоящее время угрозы в этих сферах, а также обозначены цели и задачи, решение которых позволит укрепить безопасность России.

Среди основных направлений и задач государственной политики в сфере обеспечения экономической безопасности Президент Российской Федерации отметил «создание экономических условий для разработки и внедрения современных технологий, стимулирования инновационного развития, а также совершенствование нормативно-правовой базы в этой сфере, обеспечение безопасности экономической деятельности, противодействие переводу безналичных денежных средств в теневой оборот наличных денежных средств и легализации доходов, полученных преступным путем от предикатных экономических преступлений».

Среди иных правовых источников необходимо отметить Указ Президента Российской Федерации «Об обеспечении взаимодействия государственных органов в борьбе с правонаруше-

---

[1] См.: указы Президента Российской Федерации: «О Стратегии национальной безопасности Российской Федерации» (2021 г.), «О Стратегии экономической безопасности Российской Федерации на период до 2030 года» (2017 г.), «Об уполномоченном органе по противодействию легализации (отмыванию) доходов, полученных преступным путем» (2001 г.), «О дополнительных мерах по обеспечению безопасного функционирования важнейших отраслей экономики» (2000 г.), «Об обеспечении взаимодействия государственных органов в борьбе с правонарушениями в сфере экономики» (1998 г.) и другие.

[2] О стратегии национальной безопасности Российской Федерации : Указ Президента Рос. Федерации от 2 июля 2021 г. № 400 // СПС КонсультантПлюс (дата обращения: 30.03.2022).

ниями в сфере экономики»[1] от 3 марта 1998 г. № 224 и постановление Правительства Российской Федерации от 19 января 2005 г. № 30 «О Типовом регламенте взаимодействия федеральных органов исполнительной власти»[2], посвященные рассматриваемому вопросу и устанавливающие общий порядок межведомственного взаимодействия федеральных органов исполнительной власти при реализации их полномочий, а также правила организации взаимодействия.

К нормативным правовым актам, регламентирующим рассматриваемую сферу деятельности, также относятся постановления Правительства Российской Федерации[3]. Утверждая Правила взаимодействия операторов связи с уполномоченными государственными органами, осуществляющими ОРД, Правительство Российской Федерации определило, что органы Федеральной службы безопасности Российской Федерации (далее – ФСБ) осуществляют взаимодействие с операторами связи при проведении в рамках ОРД ОРМ, связанных с использованием технических средств, в том числе в интересах других уполномоченных органов, а при отсутствии у органов ФСБ необходимых оперативно-технических возможностей для проведения ОРМ, связанных с использованием техниче-

[1] Об обеспечении взаимодействия государственных органов в борьбе с правонарушениями в сфере экономики : Указ Президента Рос. Федерации от 3 марта 1998 г. № 224 (ред. от 25.07.2000) // ИПП Гарант (дата обращения: 30.03.2022).

[2] О Типовом регламенте взаимодействия федеральных органов исполнительной власти : постановление Правительства Рос. Федерации от 19 января 2005 г. № 30 ред. от 06.06.2023 // ИПП Гарант (дата обращения: 30.03.2022).

[3] См.: Об утверждении Положения о лицензировании деятельности физических и юридических лиц, не уполномоченных на осуществление оперативно-розыскной деятельности, связанной с разработкой, производством, реализацией, приобретением в целях продажи, ввоза в Российскую Федерацию и вывоза за ее пределы специальных технических средств, предназначенных для негласного получения информации, и перечня видов специальных технических средств, предназначенных для негласного получения информации в процессе осуществления оперативно-розыскной деятельности : постановление Правительства Рос. Федерации от 1 июля 1996 г. № 770; Об утверждении Положения о ввозе в Российскую Федерацию и вывозе из Российской Федерации специальных технических средств, предназначенных для негласного получения информации, и списка видов специальных технических средств, предназначенных для негласного получения информации, ввоз и вывоз которых подлежат лицензированию : постановление Правительства Рос. Федерации от 10 марта 2000 г. № 214; Об утверждении Правил взаимодействия операторов связи с уполномоченными государственными органами, осуществляющими оперативно-розыскную деятельность : постановление Правительства Рос. Федерации от 27 августа 2005 г. № 538; Об утверждении Правил взаимодействия организаторов распространения информации в информационно-телекоммуникационной сети «Интернет» с уполномоченными государственными органами, осуществляющими оперативно-розыскную деятельность или обеспечение безопасности Российской Федерации : постановление Правительства Рос. Федерации от 31 июля 2014 г. № 743 и другие постановления.

ских средств, указанные мероприятия осуществляют ОВД, которые являются уполномоченными органами, в том числе в интересах других уполномоченных органов.

Важным направлением нормотворческой деятельности в рассматриваемой области является формирование ведомственной правовой базы МВД России, регламентирующей концептуальные положения, а также организацию и тактику деятельности ОВД и их специальных подразделений ЭБиПК. К таковым относятся приказ МВД России от 14 октября 2021 г. № 760 «Об утверждении Концепции реализации в системе МВД России государственной политики по обеспечению экономической безопасности Российской Федерации», который определяет среди прочих внедрение в научную деятельность МВД России современных информационных и телекоммуникационных технологий, разработку и наращивание справочно-правовых систем и обучающих информационных комплексов, организацию и проведение мониторинга контента сети Интернет. Концепцией предполагается создать оптимальный механизм научного обеспечения оперативно-служебной деятельности ОВД в постоянно меняющихся внутренних и внешних условиях их функционирования; приказ МВД России от 19 июня 2012 г. № 608 «О некоторых вопросах организации оперативно-розыскной деятельности в системе МВД России», который утверждает перечень оперативных подразделений системы МВД России, правомочных осуществлять ОРД, и другие приказы. Следует обратить внимание на ведомственный приказ МВД России от 1 августа 2013 г. № 588 «О некоторых вопросах организации оперативно-розыскной деятельности в системе МВД России», согласно которому оперативным подразделениям ЭБиПК запрещается напрямую обращаться с запросом к операторам сотовой связи при проведении ОРМ. Указанная процедура предусматривает дополнительное «звено» такого обращения в лице подразделений специальных технических мероприятий соответствующего региона, что существенно увеличивает сроки получения оперативно значимой информации, уменьшая, если не сводя к нулю обязательные условия наступательности и оперативности, которые являются принципиальными показателями результативности ОРД. По нашему мнению, это положение данного приказа следует отменить, тем самым дав возможность сотрудникам подразделений ЭБиПК действовать наступательно и оперативно в данном направлении. С нашим мнением согласилось абсолютное большинство (85,9 %) опрошенных сотрудников оперативных подразделений ЭБиПК.

Важность межведомственного взаимодействия находит свое подтверждение и в приказе МВД России от 2 сентября 2009 г. № 684 «Об утверждении Регламента взаимодействия Министерства внутренних дел Российской Федерации с федеральными органами исполнительной власти», где определяются конкретные полномочия руководителей подразделений МВД России, порядок образования координационных и совещательных органов, а также принятие согласованных или совместных актов федеральных органов исполнительной власти[1].

МВД России совместно с Федеральной службой безопасности России, Следственным комитетом и иными правоохранительными органами изданы межведомственные нормативные правовые акты, относящиеся к вопросам межведомственного взаимодействия по обеспечению экономической безопасности и противодействия преступности.

Формирование межведомственной правовой базы МВД России[2] является важным направлением нормотворческой деятельно-

[1] Об утверждении Регламента взаимодействия МВД России с федеральными органами исполнительной власти : приказ МВД России от 2 сентября 2009 г. № 684.

[2] Об утверждении Инструкции о порядке представления результатов оперативно-розыскной деятельности органу дознания, следователю или в суд : приказ МВД России № 776, Минобороны России № 703, ФСБ России № 509, ФСО России № 507, ФТС России № 1820, СВР России № 42, ФСИН России № 535, ФСКН России № 398, СК России № 68 от 27 сентября 2013 г.; Об утверждении Регламента информационного взаимодействия Банка России, Генеральной прокуратуры Российской Федерации, правоохранительных и иных федеральных государственных органов Российской Федерации при выявлении и пресечении незаконных финансовых операций кредитных организаций и их клиентов : приказ Генпрокуратуры, МВД, Росфинмониторинга, ФНС, ФСБ, ФСИН, ФТС, Следственного комитета, Банка России от 12 марта 2013 г. № 105/136/50/ ММ-7-2/117/131/98/447/12/ОД-121; Об утверждении Инструкции по организации информационного взаимодействия в сфере противодействия легализации (отмыванию) денежных средств и иного имущества, полученных преступным путем : приказ Генпрокуратуры, МВД, ФСБ, ФСКН, Следственного комитета, Росфинмониторинга России от 21 августа 2018 г. № 511/244/541/433/1313/80; Об утверждении Положения об организации межведомственного взаимодействия по противодействию преступлениям, совершаемым организованными группами и преступными сообществами (преступными организациями) : приказ Генеральной прокуратуры, МВД, ФСБ, Следственного комитета, ФСКН, ФТС, ФСИН России от 14 мая 2013 г. № 192/420/279/15/229/1071/293; Об утверждении Инструкции по организации информационного взаимодействия по линии Интерпола : приказ МВД, Минюста, ФСБ, ФСО, ФСКН, ФТС России от 6 октября 2006 г. № 786/310/470/454/333/971; О порядке представления результатов оперативно-розыскной деятельности налоговому органу : приказ МВД России и Федеральной налоговой службы от 29 мая 2017 г. № 317/ММВ-7-2/481; Порядок направления материалов налоговыми органами в ОВД РФ при выявлении обстоятельств, позволяющих предполагать совершение преступления, предусмотренного ст. 159 УК РФ (хищение бюджетных средств путем незаконного возмещения НДС) : утвержден Протоколом от 6 ноября 2018 г. № 3 к Соглашению о взаимодействии между МВД России и ФНС России от 13 октября 2010 г. № 1/8656/ММВ-27-4/11; Об утверждении Порядка взаимодействия Министерства внутренних дел Российской Федерации и Централь-

сти в рассматриваемой области, так как в нем формулируются понятия и основные виды документов, отражающих результаты ОРД; требования, предъявляемые к ним; закрепляется единая процедура представления результатов ОРД, а также механизм защиты сведений об органах, осуществляющих ОРД, и обеспечения безопасности ее участников.

В заключение следует отметить, что правовую основу ОРД составляет обширный перечень законодательных и иных нормативных правовых актов, знание и соблюдение которых является необходимым условием успешной ее организации и осуществления. В правоприменительной практике следует учитывать, что правовая основа ОРД находится в состоянии динамичного развития и постоянного совершенствования, но все же недостаточного в настоящее время для полного и своевременного реагирования на современные экономические цифровые угрозы.

1.3. Современное состояние организации межведомственного взаимодействия подразделений ЭБиПК в сфере противодействия преступлениям, совершаемым с использованием информационно-коммуникационных технологий

Согласно Стратегии национальной безопасности Российской Федерации, утвержденной Указом Президента Российской Федерации от 2 июля 2021 г. № 400[1] одной из задач государственной политики в сфере обеспечения государственной и общественной безопасности является предупреждение и пресечение правонарушений и преступлений, совершаемых с использованием информационно-коммуникационных технологий. Противодействие преступлениям, совершаемым с использованием ИТТ, также обозначено как одно из приоритетных направлений деятельности органов внутренних дел Российской Федерации.

Анализ статистических данных убедительно свидетельствует об устойчивой тенденции роста ИТТ преступлений. В период с 2014 по 2019 г. число зарегистрированных деяний данного вида увеличилось более чем в 25 раз (2014 г. – 11 тыс., 2019 г. – 294,4 тыс., 2020 г. – 503,5 тыс.), а с 2002 г. – почти в 50 раз (2002 г. – 6 тыс.). В 2021 г.

ного банка России в борьбе с фальшивомонетничеством : приказ МВД России и Банка России № 102/ОД-113 от 5 февраля 2009 г. и другие.

[1] О Стратегии национальной безопасности Российской Федерации : Указ Президента Рос. Федерации от 2 июля 2021 г. № 400 // Собр. законодательства Рос. Федерации. 2021. № 27 (ч. II). Ст. 5351.

органами внутренних дел Российской Федерации выявлено 517 тыс. преступлений, совершенных с использованием ИТТ.

На наш взгляд, это обусловлено особенностями криминальной деятельности в данной сфере, а именно активно развивающимся применением ИТТ, постоянным возникновением новых способов совершения противоправных действий, имеющимися возможностями для обеспечения анонимности преступников, а также виктимным поведением потерпевших.

Безусловно, сложившиеся в 2020–2021 гг. обстоятельства социально-экономического характера, вызванные пандемией коронавируса COVID-19, создали дополнительные условия для усиления криминальной активности с использованием ИТТ.

Анализ правоприменительной практики показывает, что подавляющее большинство криминальных деяний, совершенных с применением ИТТ, носит имущественный характер, в том числе мошенничества, предусмотренные ст. 159, 159.3, 159.6 УК РФ.

В 2019 г. проблемы, возникающие в области противодействия IT-преступности, рассмотрены на заседании коллегии МВД России, в результате чего в оперативных и следственных подразделениях центрального аппарата и территориальных органах МВД России созданы структурные подразделения, специализирующиеся на противодействии преступлениям данного вида[1].

Специализированные IT-подразделения созданы и в подразделениях экономической безопасности и противодействия коррупции, которые занимаются выявлением, предупреждением, пресечением и раскрытием преступлений экономической и коррупционной направленности, многие из которых совершаются с использованием ИТТ.

Говоря об имеющихся тенденциях, стоит отметить, что в целом на долю IT-подразделений службы ЭБиПК приходится не самое большое количество киберпреступлений, но, на наш взгляд, наиболее вредоносных как для государства, так и для граждан. Среди них: создание интернет-финансовых пирамид, фальшивомонетничество, организация незаконных азартных игр в сети, осуществление противоправных сделок с использованием криптовалют, попытки махинаций с электронными цифровыми подписями.

[1] Об объявлении решения коллегии Министерства внутренних дел Российской Федерации от 1 ноября 2019 г. № 3 «О мерах по совершенствованию организации работы по выявлению, раскрытию и расследованию преступлений, совершаемых с использованием информационно-телекоммуникационных технологий» : приказ МВД России от 25 ноября 2019 г. № 878.

По итогам 2020 г. IT-отделения и группы в структуре подразделений ЭБиПК выявили 1 243 киберпреступления, или 8 % от общего числа таких противоправных деяний, что в целом соотносится с долей экономических преступлений (15 742) от общего числа зарегистрированных IT-составов. Материальный ущерб в размере 581,1 млн рублей, задокументированный указанными подразделениями, возмещен на 60,2 % (349,7 млн рублей). В 2021 г. IT-подразделениями ЭБиПК выявлено уже более 3 тыс. преступлений, совершенных с использованием цифровых технологий.

ИТТ активно применяются злоумышленниками в сфере незаконной организации и проведения азартных игр. В 2020 г. выявлено 696 преступлений, предусмотренных ст. 171.2 УК РФ, из них 59 преступлений совершены в крупном и особо крупном размере. В суд направлены уголовные дела о 363 преступлениях. Выявлено 1,1 тыс. лиц, совершивших преступления, из них 694 – привлечены к уголовной ответственности[1].

Так, в результате комплекса оперативно-розыскных мероприятий, проведенных подразделениями ЭБиПК, пресечена деятельность преступного сообщества под руководством четырех граждан, которые создали сеть подпольных игорных заведений на территории г. Москвы, Челябинской области и других субъектов Российской Федерации и в период с мая 2018 г. по январь 2019 г. организовали проведение азартных игр вне игорных зон с использованием информационно-телекоммуникационной сети Интернет. В преступное сообщество входили самостоятельные структурные подразделения со строгой иерархией и четким распределением роли каждого участника, которым использовались различные способы конспирации, включая наличие системы допуска к проводимым незаконным азартным играм. По данному факту СУ СК России по Челябинской области 31 января 2020 г. возбуждено уголовное дело в отношении 4 организаторов преступного сообщества по ч. 1 ст. 210 УК РФ и в отношении 15 его активных участников по ч. 2 ст. 210 УК РФ.

В результате комплекса оперативно-розыскных мероприятий пресечена противоправная деятельность организованной группы на территории ряда регионов Российской Федерации. Участники группы из числа руководителей ООО «Букмекер Паб» в период 2017–2019 гг. на территории Брянской области, действуя умышленно, из личной заинтересованности, не исполнили обязанности налогового агента по перечислению в бюджетную систему Российской Федерации исчисленных и удержанных налогов на доходы физиче-

[1] Статистические данные ГИАЦ МВД России за 2020–2021 гг. Форма 5-БЭП.

ских лиц (НДФЛ), полученных от участия в азартных играх, проводимых в букмекерской конторе и на тотализаторе, в особо крупном размере на общую сумму 200,5 млн рублей. По данному факту СУ СК России по Брянской области 24 апреля 2020 г. возбуждено уголовное дело по ч. 2 ст. 199.1 УК РФ.

В 2020 г. ГУЭБиПК МВД России совместно с МВД по Республике Татарстан пресечена деятельность преступного сообщества, члены которого занимались изготовлением и реализацией на территории различных регионов Российской Федерации поддельных билетов Банка России номиналом 2 тыс. рублей посредством интернет-площадки «HYDRA».

В Мурманской области по материалам сотрудников IT-подразделения регионального УЭБиПК 31 марта 2020 г. возбуждено шесть уголовных дел по ч. 1 ст. 187 УК РФ в отношении группы лиц, направивших от имени руководителей ряда коммерческих организаций, использовав ключи электронных цифровых подписей последних, поддельные платежные поручения о переводе денежных средств на общую сумму более 26,4 млн рублей.

Несмотря на имеющиеся положительные результаты оперативно-служебной деятельности в данной сфере, существует целый комплекс проблем правового, методического, организационного характера, создающий трудности для противодействия преступлениям в сфере ИТТ.

Значительную сложность представляет установление личности преступника, совершившего преступление на территории иностранного государства, либо зарегистрировавшего «противоправный» интернет-домен в компании, представительство которой находится за рубежом, а также использующего для совершения противоправных действий мессенджеры Telegram, Instagram, Viber, WhatsApp, Skype, Jabber, Black-Jack. В своей работе они применяют технологии шифрования, а серверы расположены за пределами Российской Федерации. Помимо того что значимые сведения могут быть получены только при направлении запроса о правовой помощи в компетентные органы иностранного государства, разрешение которого требует значительного периода времени, законодательство иностранного государства может допускать анонимность пользователя сети Интернет в тех случаях, в которых российское законодательство ее исключает. Иным способом сохранения преступником конфиденциальности в сети Интернет является использование симкарт, приобретенных с нарушениями законодательства (например, у граждан, продающих ранее купленные для собственных нужд симкарты, или у организаций, закупивших идентификационные моду-

ли абонентов якобы для своих сотрудников и в дальнейшем перепродающих их без надлежащего оформления).

На фоне правовой неопределенности статуса криптовалют и стремительного развития криминального «крипторынка» растет количество фактов использования денежных суррогатов при совершении преступлений в сфере экономики, уклонения от уплаты налогов, финансирования экстремистской и террористической деятельности.

Определенные шаги на пути совершенствования мер по противодействию IT-преступлениям уже сделаны законодателем.

Так, Федеральным законом от 30 декабря 2020 г. № 533-ФЗ «О внесении изменений в Федеральный закон "О связи"»[1] изменен порядок заключения, прекращения договоров об оказании услуг связи и внесения в них изменений дистанционным способом. Теперь усилены требования к дистанционным продажам SIM-карт, для осуществления которых необходима усиленная квалифицированная электронная подпись или простая электронная подпись, полученная при личной явке за оказанием государственных и муниципальных услуг в электронной форме. Кроме того, при использовании простой электронной подписи гражданам необходимо пройти идентификацию через Единую биометрическую систему (далее – ЕБС), оператором которой является «Ростелеком».

Принят Федеральный закон от 31 июля 2020 г. № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении в отдельные законодательные акты Российской Федерации»[2], устанавливающий правила выпуска цифровых финансовых активов, оборота цифровой валюты (криптовалюты), а также запрещающий принимать оплату товаров, работ и услуг цифровой валютой. На сегодняшний день актуален вопрос признания криптовалюты имуществом в уголовном законодательстве. Развитие ведомственных информационно-аналитических ресурсов, обеспечивающих деятельность МВД России, в том числе в части обеспечения экономической безопасности, на наш взгляд, является одним из приори-

---

[1] О внесении изменений в Федеральный закон «О связи» : Федеральный закон от 30 декабря 2020 г. № 533-ФЗ : принят Гос. Думой 23 декабря 2020 г. : одобр. Советом Федерации 25 декабря 2020 г. // Официальный интернет-портал правовой информации. URL: http: // pravo.gov.ru (дата обращения: 06.03.2022).

[2] О цифровых финансовых активах, цифровой валюте и о внесении в отдельные законодательные акты Российской Федерации : Федеральный закон от 31 июля 2020 г. № 259-ФЗ : принят Гос. Думой 22 июля 2020 г. : одобр. Советом Федерации 24 июля 2020 г. // Официальный интернет-портал правовой информации. URL: http://pravo.gov.ru (дата обращения: 06.03.2022).

тетных направлений деятельности органов внутренних дел Российской Федерации.

Информационные ресурсы, обеспечивающие экономическую безопасность, используемые в МВД России:

– сервис обеспечения экономической безопасности органов внутренних дел Российской Федерации предназначен для обеспечения полного технологического цикла ввода, накопления, обработки и анализа оперативно-служебной, аналитической и оперативно-розыскной информации в ГУЭБиПК МВД России, а также в подразделениях ЭБиПК территориальных органов МВД России на региональном уровне. Использование сервиса повышает качество работ по выявлению, предупреждению, пресечению и раскрытию преступлений экономической и коррупционной направленности;

– информационно-поисковый сервис (далее – ИПС) «Следопыт-М» предназначен для поиска, сбора, обработки и представления информации, получаемой из разнородных информационных систем и баз данных, используемых в оперативных подразделениях на федеральном, межрегиональном, региональном и территориальном уровнях системы МВД России. ИПС «Следопыт-М» призван повысить эффективность информационного обеспечения деятельности подразделений оперативно-розыскной информации МВД России за счет сокращения времени и трудозатрат при получении информации, содержащейся в информационных системах и базах данных, путем формирования единого поискового запроса, сбора, обработки информации, досье в рамках унифицированного интерфейса и статистической отчетности.

Основными проблемными вопросами при организации противодействия преступлениям экономической и коррупционной направленности, совершенным с использованием ИТТ, по-прежнему являются:

– длительные сроки получения информации от кредитных организаций, операторов связи, социальных сетей и компаний, предоставляющих интернет-услуги;

– использование преступниками при совершении преступлений широкого спектра средств сокрытия личности (анонимные телефонные карты, VPN-сервисы, анонимные браузеры, IP-телефония);

– необходимость повышения уровня подготовки сотрудников специализированных подразделений.

Существенно ограничивает возможности расследования указанных видов преступлений недостаточное программно-техническое обеспечение производства компьютерных экспертиз. Так, при проведении экспертиз, объектами которых являются заблокированные мобильные телефоны и планшеты, имеющие графические

или неизвестные цифровые пароли, доступ к внутренней памяти устройств можно получить только в отдельных случаях (в зависимости от модели, операционной системы, серии чипсетов). Помимо этого, эксперты сталкиваются с проблемой шифрования самой внутренней памяти мобильных устройств.

Ограниченные возможности по производству компьютерно-технических экспертиз и длительное время их проведения приводят к тому, что органы предварительного следствия не назначают соответствующие экспертизы (и не предъявляют обвинения по дополнительным эпизодам преступной деятельности), в связи с чем часть преступлений в сфере ИТТ может оставаться без должного реагирования, а права потерпевших – без защиты.

Несмотря на осуществляемые мероприятия по совершенствованию информационного обмена в сфере противодействия IT-преступности, одной из основных проблем остается недостаточный уровень организации взаимодействия органов внутренних дел с кредитными организациями, интернет-провайдерами, операторами сотовой связи и интернет-сервисов.

Прогнозируя оперативно-служебную деятельность подразделений ЭБиПК в 2023 г., можно ожидать рост обращений граждан и организаций (экономической направленности), касающихся нарушения процедур закупок, завышения стоимости лекарственных препаратов и средств индивидуальной защиты, хищения бюджетных средств, выделенных на реализацию национальных проектов (программ), с преступлениями в сфере производства и потребительского рынка, мошенничеств в сети Интернет, а также мошенничеств, связанных с налоговой, банковской, коммерческой и иной деятельностью, которые отличаются гибкой адаптацией к новым формам и методам предпринимательской деятельности, имитацией заключения договоров и осуществления гражданско-правовых сделок.

Необходимо своевременно отреагировать на возрастающие угрозы в рассматриваемой сфере:

– законодательно закрепить возможность «исследования компьютерной информации», полученной в результате оперативно-розыскных мероприятий, в том числе с привлечением квалифицированных специалистов, обладающих специальными знаниями, т. е. фиксации юридически значимых следов киберпреступлений в интернете;

– провести разработку и распространение в подразделениях ЭБиПК территориальных ОВД обобщенных методик документирования таких преступлений в целях оказания методической помощи специализированным подразделениям на основе анализа наиболее значимых преступлений;

– проводить учебные занятия с руководителями и сотрудниками подразделений ИТТ ЭБиПК территориальных органов внутренних дел в целях совершенствования организации их деятельности и повышения уровня профессиональной подготовки;

– организовать и провести комплекс оперативно-профилактических мероприятий с целью информирования физических и юридических лиц о способах совершения преступлений с использованием ИТТ, применяемых для этого злоумышленниками методах и средствах, мерах по противодействию этим попыткам, с привлечением для этих целей СМИ, органов государственной власти и местного самоуправления, общественных организаций и других институтов гражданского общества.

Глава 2. Организационные аспекты межведомственного взаимодействия подразделений ЭБиПК по противодействию преступлениям экономической направленности, совершаемым с использованием информационно-коммуникационных технологий

2.1. Субъекты межведомственного взаимодействия подразделений ЭБиПК системы МВД России в сфере противодействия преступлениям экономической направленности, совершаемым с использованием информационно-коммуникационных технологий

Анализ статистических данных и отчетных документов подразделений ЭБиПК позволил установить основные направления и способы межведомственного взаимодействия, которые осуществляются между подразделениями ЭБиПК и подразделениями обеспечения экономической безопасности иных правоохранительных органов.

Сотрудники подразделений ГУЭБиПК МВД России для организации слаженной работы только в 2020 г. входили в состав 16 межведомственных рабочих групп и комиссий, провели более 500 рабочих встреч с представителями различных правоохранительных и контролирующих органов, министерств, ведомств и общественных организаций (следственных подразделений СК России; ФСБ России; ФТС России; Генеральной прокуратуры Российской Федерации, прокуратур субъектов Российской Федерации; Следственного департамента МВД России; следственных подразделений МВД России).

Сотрудники подразделений ЭБиПК проводили совместные мероприятия с сотрудниками ФСБ России, прокуратуры, Следственного комитета и ФТС России в целях организации борьбы с преступлениями экономической и коррупционной направленности.

Важность проведения межведомственного взаимодействия с указанными правоохранительными органами определяется сходностью и спецификой выполняемых ими функций[1]. К ним относятся:

– осуществление оперативно-поисковых мероприятий, направленных на получение информации о деятельности организованных

[1] Кураков Д. В., Приходько Н. Ю. Некоторые особенности выявления и раскрытия контрабанды оперативными подразделениями органов внутренних дел // Научный вестник Орловского юридического института МВД России имени В. В. Лукьянова. 2019. № 2 (79). С. 51.

преступных групп и сообществ, организованных преступных формирований в сфере экономики с целью оперативного проникновения в их структуру;

– выявление в органах власти и управления коррумпированных лиц;

– осуществление на постоянной основе сбора оперативной информации об активных криминальных лицах («ворах в законе», авторитетах уголовно-преступной среды в сфере теневой экономики, международных аферистах и финансовых махинаторах), которые способны «создавать» организованные группы и преступные сообщества в сфере экономики, а также подкупать должностных лиц в органах власти и управления;

– документирование связей и действий лиц, подготавливающих или совершающих преступления в экономической сфере и др.

Переходя к вопросам организации взаимодействия в рамках организационно-управленческих мер противодействия экономическим преступлениям, совершаемым с использованием ИТТ, следует отметить, что указанная деятельность может носить как внутренний характер, когда взаимодействие осуществляется между оперативными подразделениями одного оперативно-розыскного органа, так и внешний, который предполагает взаимодействие между двумя и более подразделениями различных правоохранительных органов.

Говоря о внешнем взаимодействии подразделений ЭБиПК в рамках противодействия преступлениям рассматриваемой категории, нужно упомянуть сотрудничество с налоговыми органами, банковскими учреждениями системы Банка России, подразделениями Росфинмониторинга, Федеральной антимонопольной службы, операторами связи, интернет-провайдерами, криптообменниками, операторами платежных систем: Яндекс.Деньги, Киви, WebMoney и т. д.

При выявлении и документировании преступной деятельности в сфере экономики следует обратить внимание на механизмы взаимодействия с ФНС России, располагающей огромными информационными ресурсами, которые могут быть использованы для решения задач ОРД в данной сфере.

Помимо участия ФНС России в выявлении признаков совершаемых или совершенных преступлений в сфере налогообложения (ст. 198–199.4 УК РФ), работники налоговых органов могут получать оперативно значимую информацию о фактах легализации (отмывания) денежных средств или иного имущества, приобретенных лицом в результате совершения им преступления, незаконного образования юридического лица, либо незаконного использования

документов для осуществления данных действий и ряда других деяний, предусмотренных УК РФ, в том числе совершенных с использованием ИТТ.

Стоит сказать о том, что вопросы взаимодействия рассматриваемых субъектов урегулированы довольно полно и всесторонне[1], начиная от общих принципов и порядка взаимодействия, заканчивая процедурой предоставления результатов ОРД в налоговый орган. Можно сказать, что взаимодействие подразделений ЭБиПК и налоговых органов существенным образом обогащают оперативно-розыскные возможности в аспекте получения сведений, касающихся экономических преступлений, в том числе совершаемых с использованием ИТТ. Вместе с этим для наиболее точного и эффективного выявления преступлений ФНС России необходима поддержка в виде осуществления взаимодействия со стороны соответствующих оперативных подразделений[2].

Анализируя практику взаимодействия МВД России и ФНС России в лице их территориальных органов, можно прийти к выводу, что налоговые органы не всегда предоставляют материалы о выявлении признаков незаконного возмещения налога на добавленную стоимость (далее – НДС). Учитывая, что подразделения ЭБиПК такого рода информацию могут получить исключительно в налоговых органах, возникает вопрос эффективности организации взаимодействия налоговых и правоохранительных органов как со стороны МВД России, так и ФНС России в данном направлении, который сегодня стоит достаточно остро.

Учитывая изложенные обстоятельства, в целях дальнейшей оптимизации и результативности практики взаимодействия между МВД России и ФНС России, на наш взгляд, представляется необходимым систематическое (при поступлении в налоговый орган) предоставление в подразделения ЭБиПК информации о «подставных» юридических лицах, требующих незамедлительной оператив-

---

[1] Об утверждении порядка взаимодействия органов внутренних дел и налоговых органов по предупреждению, выявлению и пресечению налоговых правонарушений и преступлений (с приложениями) : приказ МВД России № 495, ФНС России № ММ-7-2-347 от 30 июня 2009 г.; О порядке представления результатов оперативно-розыскной деятельности налоговому органу : приказ МВД России № 317, ФНС России № ММВ-7-2/481 от 29 мая 2017 г.; О порядке взаимодействия с МВД России : письмо ФНС России от 22 апреля 2015 г. № ПА-4-6/6929 и др.

[2] Кудакова К. С., Елфимов О. М. Актуальные вопросы взаимодействия подразделений экономической безопасности и противодействия коррупции Министерства внутренних дел Российской Федерации и Федеральной налоговой службы России по вопросам «фирм-однодневок» (на материалах Нижегородской области) // Вестник Волжского университета имени В. Н. Татищева. 2020. Т. 2. № 3 (46). С. 101.

ной проверки на предмет финансовых взаимоотношений с организациями, ведущими реальную финансово-хозяйственную деятельность, в случаях интенсивной финансовой активности по лицевым счетам, а также субъектах предпринимательской деятельности, которым было отказано в возмещении из бюджета крупных сумм НДС (прим. к ст. 159 УК РФ).

Операторы информационных систем, в которых осуществляется выпуск цифровых финансовых активов, операторы обмена цифровых финансовых активов являются субъектами Федерального закона «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма», в котором цифровая валюта признана имуществом.

Одной из основополагающих задач по дестабилизации экономических основ организованной преступности, связанной с совершением преступлений экономической направленности, является исключение доходов, полученных в результате совершения таких противоправных деяний, из экономической деятельности и недопущение их использования для восстановления и расширения инфраструктуры, необходимой для возобновления данной незаконной деятельности.

Тактика работы подразделений МВД России по данному направлению базируется на получении адекватной информации о финансовой активности объектов оперативного интереса. В этой связи взаимодействие с Росфинмониторингом – это важный ресурс борьбы с экономической преступностью через вскрытие ее финансовой составляющей, что является одним из приоритетных направлений правоохранительной деятельности.

Росфинмониторинг также рассматривает совместную с МВД России работу по борьбе с легализацией доходов, полученных преступным путем, как один из ключевых элементов национальной системы ПОД/ФТ, действующей в соответствии с принципами и рекомендациями ФАТФ.

В настоящее время взаимодействие органов внутренних дел с подразделениями Росфинмониторинга осуществляется в порядке, установленном недавно обновленной Инструкцией по организации информационного взаимодействия в сфере противодействия легализации (отмыванию) денежных средств и иного имущества, полученных преступным путем, утвержденной межведомственным приказом Генеральной прокуратуры Российской Федерации, Федеральной службы по финансовому мониторингу, МВД России, ФСБ России, ФТС России, Следственного комитета Россий-

ской Федерации от 21 августа 2018 г. № 511/244/541/433/1313/80 (далее – Инструкция) (приложение 3).

Ориентируясь на многолетний опыт сотрудничества с Росфинмониторингом в сфере противодействия легализации доходов, полученных преступным путем, справедливо констатировать, что на сегодняшний день отсутствуют какие-либо административные барьеры, препятствующие оперативному решению служебных задач на всех уровнях подчиненности: начиная от рядовых исполнителей и заканчивая руководящим составом. Такой алгоритм совместных действий непременно должен быть сохранен и в дальнейшем, но с условием придания ему все более совершенной формы с каждым успешно реализованным делом.

У Росфинмониторинга имеется опыт получения и обработки выписок, предоставленных криптобиржами и обменниками, в которых содержатся оперативно значимые сведения.

С учетом новых тенденций в финансовых схемах сетевого сбыта поддельных денежных средств МВД России и Росфинмониторинг осуществляют работу по обновлению (в том числе с учетом зарубежного опыта) методик отработки движения криптоактивов, используемых в качестве инструментов для совершения таких преступлений.

В данном случае большое значение имеют возможности международного взаимодействия Росфинмониторинга с подразделениями финансовой разведки (далее – ПФР) других государств (более 100). Что касается информации, полученной из ПФР иностранного государства, то в отношении ее использования действуют специальные правила, предусмотренные п. 17.3 Инструкции.

В частности, такие сведения допустимо применять только при оперативной проверке или в процессе оперативного сопровождения уголовного дела. Для приобщения таких данных к материалам уголовного дела в качестве доказательств требуется согласие зарубежного информатора, которым выступает ПФР. В отличие от длительной процедуры, осуществляемой в рамках оказания взаимной международной правовой помощи, Росфинмониторинг, являясь членом Группы Эгмонт[1], может оперативно получать интересующую информацию от ПФР иностранных государств по защищенным каналам указанной группы. При этом следует учитывать,

[1] The Egmont Group of Finance Intelligence Unit – неофициальная международная ассоциация (сеть) подразделений финансовой разведки. Целью работы группы является содействие в расширении и систематизации обмена оперативной финансовой информацией между национальными ПФР, повышение квалификации и возможностей их сотрудников, а также совершенствование средств связи между ними.

что Росфинмониторинг наделен правом участия в международных правовых отношениях по вопросам получения информации, касающейся существования, местонахождения, движения, характера, юридического статуса и стоимости имущества, подлежащего конфискации как полученного в результате преступной деятельности. Указанные функции осуществляются центральным аппаратом Росфинмониторинга в рамках ряда международных конвенций, сотрудничества с экспертами ФАТФ, ЕАГ[1], МАНИВЭЛ[2].

Иными словами, разведывательные функции Росфинмониторинга предоставляют возможность активнее использовать ресурсы информационного обмена с иностранными компетентными органами для получения необходимых сведений о счетах и характере трансграничных переводов, в том числе в криптовалюте, и, основываясь на этих данных, направлять мотивированные ходатайства в судебные органы тех государств, куда были выведены активы, полученные в России от экономических и коррупционных преступлений, с целью их блокировки и последующего возврата (как правило, если провайдер заявил о себе официально).

Эффективность и результативность взаимодействия с Росфинмониторингом зависят не только от правильного понимания пределов компетенции национального ПФР, постановки перед его специалистами верно сформулированных вопросов, но и от четкого соблюдения правила «обратной связи» в части использования полученной информации и материалов, а именно: в течение 10 рабочих дней с момента завершения либо передачи дела оперативного учета, принятия соответствующего процессуального решения по итогам проверки сообщения о преступлении, а также предварительного расследования уголовного дела (п. 24 и 25 Инструкции. Образец справки приведен в приложении № 3 к Инструкции); в течение 30 дней с момента получения информации и материалов Росфинмониторинга, направленных в соответствии со ст. 8 Федерального закона № 115-ФЗ (п. 29 Инструкции).

---

[1] Eurasian Group on Combating Money Laundering and Financing of Terrorism (EAG) – Евразийская группа по противодействию легализации преступных доходов и финансированию терроризма (ЕАГ) создана 6 октября 2004 г. по инициативе Российской Федерации, поддержанной ФАТФ, МВФ, Всемирным банком и рядом государств. ЕАГ является региональной группой по типу ФАТФ (участники: Китайская Народная Республика, Кыргызская Республика, Республика Беларусь, Республика Казахстан, Республика Таджикистан и Российская Федерация).

[2] Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism (MONEYVAL) – Комитет экспертов Совета Европы по оценке мер борьбы с отмыванием денег и финансированием терроризма.

В форме обратной связи конкретизируется характер использования данных ПФР, что, безусловно, важно для службы в целях определения «коэффициента полезного действия» и дальнейшего совершенствования деятельности.

Многоаспектный формат полномочий Росфинмониторинга в соотношении с тактическими возможностями оперативно-розыскной деятельности органов внутренних дел определяют перспективные пути дальнейшего взаимодействия по подрыву экономических основ организованной преступности экономической направленности. При этом важно понимать, что «подвижность» финансовой структуры экономической преступности нацеливает на своевременное обновление системы мер противодействия, в частности, имеющихся с Росфинмониторингом межведомственных алгоритмов выявления, документирования и доказывания преступлений, связанных с бесконтактным способом сбыта поддельных денежных средств и легализацией преступных доходов, совершенных с использованием виртуальных активов.

2.2. Информационные ресурсы субъектов межведомственного взаимодействия, используемые подразделениями ЭБиПК для противодействия преступлениям экономической направленности, совершаемым с использованием информационно-коммуникационных технологий

Всякое взаимодействие оперативных и иных подразделений органов внутренних дел в сфере оперативно-розыскной деятельности по решению задач борьбы с преступностью в раскрытии преступлений может быть успешным лишь при наличии соответствующего информационного обеспечения, идет ли речь об информации, касающейся самого процесса взаимодействия, или об информации о преступлении и его раскрытии.

В соответствии с ч. 4 ст. 13 Федерального закона от 7 февраля 2011 г. № 3-ФЗ «О полиции» для выполнения возложенных обязанностей сотрудникам предоставлено право запрашивать и получать на безвозмездной основе по мотивированному запросу уполномоченных должностных лиц полиции от государственных и муниципальных органов, общественных объединений, организаций, должностных лиц и граждан сведения, справки, документы (их копии), иную необходимую информацию, при этом требования (запросы, представления, предписания) уполномоченных должностных лиц полиции являются обязательными для исполнения.

Органы, осуществляющие оперативно-розыскную деятельность, наделены правом направлять запросы для получения необходимой информации в соответствии со ст. 6, 7, 15 ФЗ «Об ОРД».

Применительно к рассматриваемой теме практически обоснованным представляется конкретизация направлений в контексте ОРМ «наведение справок»: это непосредственно запрос в целях решения тактических задач ОРД о предоставлении оперативной информации в адрес юридических и (или) физических лиц, запрос данных в какой-либо информационной поисковой системе и получение оперативной информации посредством ознакомления с носителями данных.

Как отмечено выше (ст. 6 Федерального закона № 259), порядок запроса информации от цифровых операторов в рамках ОРД установили по аналогии с предусмотренным ст. 26 Федерального закона от 2 декабря 1990 г. № 395-1 «О банках и банковской деятельности».

Это право предоставлено органам, осуществляющим ОРД, в 2013 г.[1] в качестве значимого средства для достижения оперативных целей получение сведений, составляющих банковскую тайну. Главным условием его реализации является наличие проверенных данных о признаках подготавливаемых, совершаемых или совершенных преступлений, а также о лицах, их подготавливающих, совершающих или совершивших, если нет достаточных оснований для решения вопроса о возбуждении уголовного дела.

В качестве отступления от основной темы отметим, что перечень информации, разрешенной к получению в порядке названной выше статьи, должен быть гораздо шире, поскольку в настоящее время кредитные учреждения, в том числе операторы платежных систем, обладают эксклюзивными программными комплексами, позволяющими получать и детализировать финансовую информацию, которая является оперативно значимой для выявления и раскрытия тяжких и особо тяжких составов преступлений экономической направленности.

В этой связи на межведомственном уровне продолжается разработка предложений о расширении спектра получаемых сведений для внесения изменений в ст. 26 Федерального закона «О банках и банковской деятельности».

---

[1] О внесении изменений в отдельные законодательные акты Российской Федерации в части противодействия незаконным финансовым операциям : Федеральный закон от 28 июня 2013 г. № 134-ФЗ : принят Гос. Думой 11 июня 2013 г. : одобрен Советом Федерации 26 июня 2013 г. // Официальный интернет-портал правовой информации. URL: http://www.pravo.gov.ru (дата обращения: 17.05.2022).

Обмен информацией в рамках межведомственного взаимодействия с ПАО Сбербанк и ПАО Банк ВТБ осуществляется в электронном виде в рамках соглашений от 29 октября 2017 г. и от 25 декабря 2017 г. соответственно. В настоящее время прорабатывается технический вопрос об обмене информацией через личные кабинеты, доступ к которым обеспечен через ИСОД МВД России.

Актуальный стандарт данных, необходимых для начального анализа финансовой составляющей преступной деятельности, который требуется запросить:

– движение денежных средств (входящие/исходящие транзакции) по счету (счетам) в банковских учреждениях либо по учетным записям в электронных платежных системах и сервисах (например, QIWI Кошелек);

– подключение услуг интернет-банкинга, привязанные к электронным платежным инструментам номера телефонов, адреса электронной почты, IP-адреса, IMEI используемого мобильного оборудования;

– биометрия, фото и видеоизображения с устройств фиксации на банкоматах и платежных терминалах, геолокация субъектов финансовых операций;

– обменные операции, связанные с виртуальными активами.

Возвращаясь к рассматриваемому вопросу, необходимо уточнить, что существует специальный порядок получения информации в отношении сведений конфиденциального характера (сведения, составляющие служебную, врачебную, нотариальную, адвокатскую, банковскую, коммерческую тайны, тайны страхования, переписки, телефонных переговоров, почтовых отправлений, телеграфных или иных сообщений и так далее).

Вместе с тем категория тайны применительно к цифровым финансовым активам и цифровой валюте для целей Федерального закона № 259 не конкретизирована, как и официальный статус криптоплатформ, работающих на российского потребителя. Кроме того, цифровая валюта до настоящего времени не поименована в качестве «имущественного актива» в целях уголовно-процессуального законодательства.

В таких условиях правового обеспечения деятельности органов внутренних дел предмет наведения справок для рассматриваемого направления деятельности – это сведения, аккумулированные в информационных системах операторов услуг, связанных с цифровыми активами и цифровой валютой, созданные по правилам публичного блокчейна.

Блокчейн является открытой сетью, что позволяет любому участнику изучить историю транзакций, а также установить размер пересылаемых между адресами сумм. При этом (фактически) сеть является анонимной, что дает возможность злоумышленникам использовать криптовалюту для незаконных операций.

Вместе с тем существует ряд методов, позволяющих установить владельца кошелька, зная номер незаконной или подозрительной транзакции (далее – целевая транзакция), которая по своей сущности отображает перемещение криптовалютных средств (далее – целевые средства).

Например, преступник получил на адрес кошелька некоторую сумму целевых средств из нелегальных источников. Его задача – переместить эти средства на другие кошельки путем дробления целевой транзакции на минимальные части для конвертации полученных целевых средств посредством их обмена на рубли или валюту по выбору. Для этого он будет использовать обменную площадку или переведет сумму целевых средств на централизованные биржи.

Установить всю цепочку транзакций в системе блокчейн можно самостоятельно или посредством использования аналитических инструментов по типу Прозрачный блокчейн[1], Crystal, Chainanalysis, CipherTrace, Eliptic, Merkle Science, Scorechain, TRM Labs и других, которые в кратчайшие сроки отследят и установят список всех адресов, через которые проводились операции. В наглядной форме будут получены операции с кошельком, составлен алгоритм кластеризации, объединяющий адреса с общим владельцем, и обозначен «выводной» адрес «обменника» или биржи, в адрес которого (как правило, посредством электронной формы обратной связи) следует обратиться с запросом информации.

В случае самостоятельного отслеживания и установления всей цепочки транзакций для определения адреса «обменника» или биржи через систему блокчейн необходимо принять во внимание следующее.

Адрес централизованной биржи помечен отличительным знаком в системе блокчейн. Адрес обменного пункта в большинстве

[1] МВД России использует «Прозрачный блокчейн» в тестовом режиме в качестве аналитического программного продукта. Это совместный проект Росфинмониторинга и РАН в целях создания собственной информационно-ресурсной базы профиля блокчейн. Инструмент с онлайн-доступом, который автоматически группирует и маркирует bitcoin-адреса, а также позволяет выявлять, анализировать и визуализировать операции с криптовалютой bitcoin. Сервис сканирует Интернет и Даркнет для выявления bitcoin-адресов и кошельков.

случаев не отличается от обычного адреса, принадлежащего любому пользователю, но есть ряд свойственных ему признаков:

Частота использования. Адрес используется для транзакций чаще, чем адрес обычного пользователя.

Узнаваемость. Номер адреса присутствует в поисковой системе браузера.

На основе этих данных можно установить адрес обменного пункта посредством поиска в поисковой системе адреса кошелька, который был обнаружен и установлен как использующийся для операций по вводу/выводу целевых средств. Результат поискового запроса позволит перейти по ссылкам на обозначенные системой сайты. В большинстве случаев поиск приведет на сайт bestchange.ru, где указаны различные сведения (номер телефона, адрес электронной почты, номер банковской карты и так далее), позволяющие связаться с представителями обменных пунктов. Некоторые из них придерживаются политики «знай своего клиента» и проводят идентификацию пользователей перед совершением сделки купли-продажи криптовалюты путем документального фиксирования предоставленной информации. Это также позволит получить информацию о клиенте, совершившем целевую транзакцию, через мотивированный запрос.

Содержание запроса должно включать допустимые обстоятельства дела, номер транзакции или кошелька, просьбу предоставить информацию о клиенте, которой обладают представители обменного пункта, справки и иные сведения (прил. 1).

Представляется целесообразным заранее обсудить с представителями обменного пункта предпочтительный вид связи (e-mail, почта, мессенджер или иное).

Большое количество криптовалютных сервисов расположены вне юрисдикции Российской Федерации, поэтому запрос необходимо составить на английском языке (образцы таких запросов даны в приложении к данному пособию).

Если сайт не имеет переключения на русский язык, то нужно использовать сервисы автоматического перевода (прил. 2).

Поиск контактных данных. Как показывает практика, криптовалютные сервисы оставляют каналы для связи: например, сведения о компании в «подвале» страницы сайта; в разделе юридических документов (Terms of use, User agreement); в поле «почта» или «чат» от службы поддержки.

Более предпочтительна электронная почта, на которую необходимо отправить скан официального запроса.

Запрос следует отправлять с адреса ведомственной электронной почты, иначе он может быть проигнорирован.

Что не стоит запрашивать: выгрузку данных всех пользователей сервиса (или их большого количества); выгрузку транзакций по всему сервису или за продолжительный период времени; публично доступные данные (например сведения о транзакциях по конкретному кошельку или выгрузку по всей сети Bitcoin).

Практика показывает, чем более конкретизирован запрос (есть привязка к пользователю или транзакциям), тем больше вероятность получения ответа.

Рекомендации по документальному закреплению мероприятия.

В предложенном формате ОРМ «наведение справок» будет длящимся мероприятием, место проведения которого ничем не регламентировано, сроки для наведения справок не являются ограниченными, поскольку зависят от продолжительности периода времени от направления запроса до получения ответа.

В соответствии с правилами оформления результатов ОРМ «наведение справок» полученная от провайдера услуг обмена виртуальными активами информация должна быть задокументирована. Сведения оформляют в виде рапорта, справки (справки-меморандума), акта оперативного сотрудника, который проводил ОРМ по добыванию информации, и прочих допустимых в оперативно-служебной деятельности документов с обязательным указанием оснований для наведения справок и аргументирующих мероприятие обстоятельств[1].

В настоящее время запрашиваемые операторы, действующие в сфере цифровых финансовых услуг, как правило, не предоставляют ответа в письменной или электронной формах с реквизитами подтверждения (бланк, подпись, печать). В таком случае распечатанная информация легализуется приобщением к акту оперативного сотрудника, к которому в качестве дополнительного обоснования могут быть приложены скрины экрана и другие технические носители информации и предметы (например видеофиксация осмотра сайта и наличия в электронном почтовом ящике ответа на запрос).

Бесспорно, что процессуально самостоятельными (процессуально обоснованными) документами являются только сведения, поступившие в качестве ответов по направленным запросам из официальных организаций, в том числе с приложением материалов

[1] Все данные, полученные в результате наведения справок, направляемые в уголовный процесс, подлежат оформлению по установленным применительно к результатам ОРД правилам.

на различных носителях. Эти данные впоследствии приобщаются к уголовному делу в качестве доказательств.

Иная полученная оперативным путем информация, закрепленная документом оперативного сотрудника, может использоваться в целях ОРД и подлежит подтверждению следственными действиями (например запрос в рамках предварительного расследования, протокол допроса представителя оператора информационной системы, протокол осмотра сайта провайдера и ящика электронной почты сотрудника для фиксации получения ответа на запрос).

Кроме того, в рамках ОРД на основании международного соглашения или договора имеется возможность обращаться в компетентные органы зарубежных государств по месту лицензирования деятельности провайдера услуг в сфере виртуальных активов с запросом об оказании помощи по наведению справок.

Большую практическую значимость имеют и информационные ресурсы других организаций и учреждений.

Так, с помощью получения выписок из Единого государственного реестра юридических лиц (далее – ЕГРЮЛ) или Единого государственного реестра недвижимости (далее – ЕГРН) можно понять, имеет ли правонарушитель право заниматься предпринимательской деятельностью, код ОКВЭД позволяет определить, какая именно отрасль экономической деятельности разрешена государством. Для этого достаточно знать ИНН организации или физического лица. Сотрудничество с Федеральной налоговой службой, располагающей обширными сведениями об организациях и индивидуальных предпринимателях, полученными посредством проведения камеральных и выездных проверок, анализа бухгалтерской и финансовой отчетности, является эффективным источником информации.

Еще один информативный источник – база Федеральной службы судебных приставов, которая предоставляет обширные сведения об имеющейся задолженности возможного преступника и которая может стать причиной совершения им противоправных действий.

Государственная информационная система ГИС «ЖКХ» позволяет сотрудникам ЭБиПК получать сведения об объектах государственного учета жилищного фонда, стоимости и перечне работ и услуг по содержанию того или иного жилищного объекта, о задолженности по оплате жилищно-коммунальных услуг.

Немаловажным источником информации являются, как было отмечено выше, средства массовой информации и сеть Интернет, различные популярные сайты: ВКонтакте, Одноклассники и др. Действия интересующих объектов можно отследить и вычис-

лить онлайн, поскольку все действия пользователей фиксируются и сохраняются на серверах владельцев сайтов. Даже при удалении личных страниц пользователей цифровой след от них сохраняется долгое время.

Достаточно эффективно зарекомендовал себя веб-сервис быстрой проверки контрагентов, зарегистрированных на территории Российской Федерации, на основании данных из официальных и неофициальных источников «Контур.Фокус» или СКБ «Контур». Данный портал позволяет быстро проверить интересующего субъекта на предмет его регистрационных данных, осуществления финансово-хозяйственной деятельности, ведения судебных тяжб, их количества; определить, кто выступает ответчиком и истцом, сроки давности судебных разбирательств, их предмет. Данный сервис предоставляет возможность проверки связанных организаций, их руководящий состав, а также доходы, полученные организацией, участие в госзакупках, наличие различных лицензий, товарных знаков и прочее.

Похожей платформой по проверке контрагентов является «Спарк». Данная программа предоставляет доступ к данным кредитного бюро, нотариата, Росреестра, позволяет просмотреть результаты годовой и квартальной отчетности юридических лиц, оценить рисковые факторы (сведения о банкротстве, смене владельцев, судах и отслеживание движения дел, возможной аффилированности юридических и физических лиц). Также можно проследить деятельность интересующего субъекта, в частности, его участие в различных тендерах и грантах, наличие лицензий, патентов и пр. Интересным и значительным представляется наличие информации о проверках Генеральной прокуратуры Российской Федерации и сведения о привлечении лиц к ответственности за незаконное вознаграждение.

Портал также предоставляет доступ к реестру недобросовестных поставщиков, что может также характеризовать деятельность организаций и индивидуальных предпринимателей и представлять интерес для подразделений ЭБиПК.

Участие субъектов финансово-хозяйственной деятельности в арбитражных делах также является источником оперативно значимой информации для сотрудников оперативных подразделений ЭБиПК. С данной информацией можно ознакомиться на официальном сайте http://www.arbitr.ru.

Раскрытие информации о недвижимости по ее адресу может позволить оперативным сотрудникам получить ряд сведений, которые владелец не желает афишировать.

Юридическую информацию о недвижимости можно получить из официальных источников. Например, для России: из кадастровой карты Российской Федерации: http://kadastrmap.ru; единого государственного реестра прав на недвижимое имущество: http://rosreestr.ru/wps/portal/cc_egrp_form_new; справочной системы по объектам недвижимости: https://rosreestr.ru/wps/portal/cc_information_online.

Визуальный осмотр территории объекта с помощью GoogleStreetView, панорам Яндекс.Карт или фотографий, размещенных на ресурсе Wikimapia.org, может дать информацию о специфике деятельности располагающейся на территории организации, благосостоянии владельца частного дома и т. п.

Полезной может быть информация о недвижимости в связке со сведениями о ее владельце. Подобные данные могут быть найдены на сайте https://phonenumber.to и других ресурсах.

В задачи поисковой работы нередко входит сбор сведений о собственниках или маршрутах транспортных средств (будь то автомобили, корабли, самолеты или иная техника).

В частности, получение регистрационной информации возможно для автотранспорта на национальных ресурсах:

www.gov.uk/get-vehicle-information-from-dvla (Великобритания);

http://avtocod.ru (Россия) и т. д.

Для морского и авиатранспорта на интернациональных: сайт www.vesselfinder.com и база www.airframes.org соответственно.

Для автотранспорта также доступны неофициальные сведения о владельцах: их адресная и контактная информация (например, с помощью ресурса http://nomer.today/mosgibdd или телеграм-ботов @AvinfoBot или @AntiParkonBot).

Информация о маршрутах транспортных средств представлена: для судов на сайте www.marinetraffic.com; для самолетов – https://planefinder.net.

Есть и другие аналогичные ресурсы, содержащие сведения, которые могут оказаться полезными сотрудникам оперативных подразделений ЭБиПК.

В целях противодействия преступлениям экономической и коррупционной направленности важное место занимает межведомственное взаимодействие с Федеральной антимонопольной службой России, на вооружении которой имеется автоматизированная программа по выявлению и доказыванию картелей (ст. 178 УК РФ «Ограничение конкуренции»), так называемый веб-сервис «Большой цифровой кот» (официальное название – «Антикартель»). С его помощью осуществляется контроль за проведением аукцио-

нов и выявляются антиконкурентные соглашения. Программа работает также на базе информационной системы закупок и других источников данных: СМИ, электронных торговых площадок, открытых источников информации и прочих. В ФАС создано специализированное подразделение для расследования дел о картелях и иных антиконкурентных соглашениях в цифровой сфере. В рамках Управления по борьбе с картелями создан специальный отдел, который занимается именно цифровыми расследованиями.

Перспективным информационным ресурсом является ГИС в области противодействия коррупции «Посейдон»[1]. Она работает сразу с несколькими базами, объединенными в единое целое: база ФНС, база Росфинмониторинга, база Росимущества, а также информация из соцсетей. «Посейдон» позволяет создать цифровой портрет проверяемого человека и узнать, нет ли у него пересечения интересов, неформального общения с людьми, в котором могут быть скрыты коррупционные отношения. Силовики могут отправлять так называемый запрос на проверку лица. Например, у сотрудника МВД есть необходимость проверить чиновника высокого ранга, тогда направляется запрос в управление по вопросам противодействия коррупции Администрации Президента Российской Федерации или в ФСО. Уровень лиц, которые могут подвергнуться проверке, может быть очень высокий, поэтому система является закрытой.

2.3. Организация межведомственного взаимодействия подразделений ЭБиПК по противодействию отельным видам преступлений экономической направленности, совершаемых с использованием информационно-коммуникационных технологий

Взаимодействие с налоговыми органами в ходе выявления признаков преднамеренного банкротства

Одной из особенностей выявления и расследования дел о преднамеренном банкротстве является то, что работа по выявлению признаков таких преступлений с каждым годом становится все более трудоемкой и сложной. Это обусловлено не только постоянными изменениями в законодательстве и трансформацией форм отчет-

[1] О государственной информационной системе в области противодействия коррупции «Посейдон» и внесении изменений в некоторые акты Президента Российской Федерации (вместе с «Положением о государственной информационной системе в области противодействия коррупции «Посейдон») : Указ Президента Рос. Федерации от 25 апреля 2022 г. № 232 // Собр. законодательства Рос. Федерации. 2022. № 18. Ст. 3053.

ности юридических лиц, предоставляемой в налоговые органы, но и тем, что сами представители преступного сообщества постоянно модернизируют способы, формы и методы совершения преступлений, связанных с преднамеренным или фиктивным банкротством.

Процедура выявления любого преступления в обязательном порядке связана с необходимостью сбора и последующего анализа такой информации, которая представляет собой ценность для расследования уголовного дела. Кроме этого, процесс выявления преступления предполагает обязательную проверку достоверности полученной информации, ее оценку и последующую реализацию в ходе возбуждения уголовного дела и осуществления предварительного расследования[1].

С теоретической точки зрения основанием для возбуждения уголовного дела в отношении лиц, подозреваемых в совершении действий, приведших к преднамеренному или фиктивному банкротству, может стать любой повод, предусмотренный ст. 140 УПК РФ. Однако на практике, к примеру, явка с повинной практически никогда не встречается в уголовных делах о банкротстве, поскольку этот вид преступлений предполагает высокую степень скрытности и согласованность действий участников. Как правило, выявление преступлений, связанных с фиктивным или преднамеренным банкротством, происходит в процессе расследования других преступлений, например мошенничества.

Наиболее часто на практике основанием для возбуждения уголовных дел по факту совершения действий, приводящих к фиктивному или преднамеренному банкротству, становятся материалы выездных и реже камеральных проверок, осуществляемых налоговыми органами. Кроме этого, достаточно часто таким основанием выступают результаты расследования налоговых преступлений, которые также осуществляются в тесном взаимодействии с подразделениями Федеральной налоговой службы. Причинами такого пересечения интересов двух ведомств является то, что, как правило, преступления, связанные с фиктивным или преднамеренным банкротством, имеют истинной целью уклонение от уплаты налогов или списание части задолженности по налогам перед бюджетами различных уровней.

Вторым наиболее распространенным поводом для возбуждения уголовного дела о преднамеренном или фиктивном банкротстве

[1] См.: Кручинина Н. В. Проблемы теории и практики проверки достоверности уголовно-релевантной информации в досудебном уголовном процессе. М., 2019. 166 с.

выступают заявления кредиторов, которые при нормальных условиях совершенно не заинтересованы в утрате своих собственных материальных и нематериальных активов, а следовательно, всеми силами стараются предотвратить искусственное создание ситуации, в которой должник оказывается неспособным отвечать по своим долговым обязательствам. Однако специфической особенностью таких заявлений кредиторов выступает то, что они поступают в правоохранительные органы на поздних стадиях, когда уже фактически известно о начале процедуры банкротства или о несостоятельности должника. Кроме того, далеко не всегда информация, которая предоставляется кредиторами, является достаточной для возбуждения уголовных дел, поскольку качество и количество такой информации, собираемой физическими и юридическими лицами в своих интересах, может существенным образом различаться. Так, в крупных организациях, в которых штатным расписанием предусмотрена служба экономической безопасности, могут собрать действительно ценную для расследования информацию, в то время как представители индивидуальных предпринимателей чаще оперируют слухами и домыслами.

Несмотря на то, что именно арбитражные управляющие в первую очередь сталкиваются с признаками фиктивного или преднамеренного банкротства, по их инициативе, а также по решениям арбитражных судов уголовные дела рассматриваемой категории практически не возбуждаются. Похожая ситуация складывается и в подразделениях полиции, в которых ни по рапортам сотрудников оперативных служб, ни по материалам оперативно-розыскной деятельности уголовных дел о криминальном банкротстве не возбуждается. Это объясняется тем, что для сбора доказательств по таким уголовным делам недостаточно выявить признаки преднамеренного или фиктивного банкротства и необходимо назначение ревизии, проверки бухгалтерской и финансовой отчетности, проведение финансово-экономического анализа, анализа хозяйственной деятельности. И только по результатам такого анализа и документальной проверки возможно возбуждение уголовного дела. Именно этим фактом объясняется то, что наиболее значимая информация для возбуждения и расследования рассматриваемых нами уголовных дел поступает от подразделений Федеральной налоговой службы.

Данное обстоятельство объясняется в первую очередь тем, что именно в подразделениях налоговых служб работают специалисты, обладающие всеми необходимыми знаниями, опытом и квалификацией, позволяющими выявлять и собирать доказательную базу по фактам преднамеренного и фиктивного банкрот-

ства. Однако при этом следует понимать, что специалисты налоговой службы не обладают всеми полномочиями, которые позволили бы им эффективно осуществлять борьбу с такими криминальными банкротствами, в связи с чем возникает вопрос о взаимодействии органов Федеральной налоговой службы и различных правоохранительных органов, в первую очередь МВД России и следственного комитета.

Законодатель предусмотрел механизм регулирования такого межведомственного взаимодействия. В частности, Налоговым кодексом Российской Федерации предусмотрено две статьи, которые раскрывают особенности и порядок обмена информации между налоговыми органами и правоохранительными органами.

Статья 32 Налогового кодекса Российской Федерации предусматривает, что сотрудники налоговых инспекций обязаны направлять материалы своих проверок по факту выявления налоговых правонарушений в том случае, если лицо, допустившее нарушение, не исполняет решение налогового органа об уплате соответствующих платежей в бюджет в течение двух месяцев. В случаях с фиктивным банкротством ситуация намного сложнее, поскольку, как правило, выявляются только признаки криминальных действий, которые необходимо расследовать для того, чтобы собрать доказательную базу.

На этот случай в Налоговом кодексе Российской Федерации предусмотрена ст. 82, в которой в ч. 3 говорится о том, что налоговые и правоохранительные органы осуществляют обмен информацией о проводимых ими проверках, аналитических материалах, выявленных фактах правонарушений в области уплаты налоговых платежей, с целью повышения эффективности противодействия уклонению от уплаты налогов, при этом положения данной статьи предполагают, что для такого обмена информацией между ведомствами нет необходимости дожидаться вынесения решения по налоговой проверке или ждать два месяца, чтобы понять, что правонарушитель не собирается исполнять решения налогового органа. Данное умозаключение подтверждается и решением Арбитражного суда от 8 декабря 2021 г. № Ф10-4908/2021 по делу № А08-10204/2020, которым разъяснено, что налоговые органы вправе направлять в следственные органы и подразделения полиции любые материалы, включая и материалы налоговых проверок, по которым еще не вынесены решения.

Принимая во внимание тот факт, что криминальное банкротство наиболее часто применяется именно для уклонения от уплаты налогов, такое взаимодействие, предусмотренное Налоговым кодек-

сом Российской Федерации, является чрезвычайно действенной мерой, позволяющей дополнять усилия различных органов исполнительной власти в борьбе с подобными проявлениями. Однако необходимо отметить, что на этом регламентация взаимодействия ФНС России и правоохранительных органов не заканчивается.

Налоговым кодексом предусмотрена отдельная глава 6, которой регламентируется участие органов внутренних дел и следственных органов в расследовании и раскрытии налоговых преступлений совместно с налоговыми органами. Так, ст. 36 Налогового кодекса Российской Федерации регламентирована возможность сотрудников налоговых органов привлекать при необходимости сотрудников органов внутренних дел для проведения необходимых следственных и иных действий в случаях, когда возникает такая необходимость. Также ст. 37 Налогового кодекса Российской Федерации предусмотрена обязанность сотрудников органов внутренних дел передавать сотрудникам налоговых органов информацию, которая стала известна в результате расследования и имеет значение для предотвращения уклонений от уплаты налогов.

В 2016 г. было проведено совместное заседание коллегий ФНС России и Следственного комитета Российской Федерации от 7 июня 2016 г. № 2/4 по вопросу «Повышение эффективности взаимодействия налоговых и следственных органов по выявлению и расследованию преступлений в сфере налогообложения», по результатам которого были разработаны межведомственные методические рекомендации по установлению в ходе налоговых и процессуальных проверок обстоятельств, свидетельствующих об умысле в действиях должностных лиц налогоплательщика, направленном на неуплату налогов (сборов). Данные методические рекомендации подробно раскрывают отличия случайно совершенных правонарушений в области налогового законодательства от умышленных. Подробно раскрываются признаки таких умышленных противоправных действий, направленных на уклонение от уплаты налоговых платежей. К числу таких признаков относится организация фиктивной деятельности посредством создания фирм-однодневок, имитации хозяйственной деятельности и т. д. Все эти действия, приводящие к совершению налоговых преступлений, являются сопутствующими и при организации криминальных банкротств, поскольку имеют общие и схожие цели.

Однако выявление признаков фиктивного банкротства на практике значительно сложнее, чем выявление признаков налогового преступления. Основным источником информации для выявления и расследования преступлений, связанных с криминальными бан-

кротствами, выступает анализ финансово-хозяйственной деятельности организации или предприятия, в отношении которого инициирована процедура банкротства. Основная сложность заключается в том, что по результатам такого анализа не всегда можно однозначно утверждать, является ли данный случай фиктивным и преднамеренным, или же у организации действительно сложилась безвыходная ситуация.

Именно этим объясняется тот факт, что уголовных дел, возбужденных по ст. 197 УК РФ, очень мало. По данным МВД России, в 2020–2021 гг. таких дел было возбуждено более 250, а к ответственности привлечено около 80 человек. На практике представители правоохранительных органов чаще применяют ст. 159 УК РФ, под которую попадает большинство экономических преступлений, в том числе и фиктивное банкротство. Дело в том, что собрать доказательные материалы по мошенничеству менее трудоемко, чем детально анализировать финансово-хозяйственную деятельность для выявления признаков фиктивного банкротства.

При этом следует отметить, что и представители налоговых органов также не ставят для себя первоочередной задачей выявление признаков фиктивного банкротства и передачу материалов для возбуждения уголовных дел. Это объясняется тем, что ключевой задачей налоговых органов является возвращение неуплаченных денежных средств в бюджет, а такой возврат, пусть даже и частичный, осуществляется в рамках работы арбитражного управляющего и дальнейших судебных разбирательств. С точки зрения налоговых органов, если в рамках судебной процедуры банкротства удалось частично возместить неуплаченные средства в бюджет, то задача считается выполненной.

Следует понимать, что актуальность ст. 197 УК РФ была высока тогда, когда существовала процедура внесудебного объявления банкротства. Именно в этот период времени любое юридическое лицо могло просто объявить себя неплатежеспособным по своему усмотрению, что конечно же вызывало многочисленные злоупотребления. После введения института арбитражных управляющих и судебного порядка признания банкротом таких случаев фиктивного банкротства практически не осталось. Одновременно с этим возросла сложность схем, применяемых недобросовестными предпринимателями для уклонения от своих обязательств, в том числе и по налоговым платежам в бюджет.

Именно поэтому в 2021 г. в СМИ появилось сообщение о совместном обращении МВД России и ФНС России с предложением упразднить ст. 197 УК РФ как малоиспользуемую на прак-

тике. Однако следует помнить, что это не единственная статья Уголовного кодекса, которая устанавливает ответственность за рассматриваемые нами преступления. По-прежнему остаются актуальными ст. 195 и 196 УК РФ, но их упразднение даже не обсуждается ни научным сообществом, ни представителями правоохранительных органов.

Взаимодействие при выявлении и раскрытии преступлений экономической и коррупционной направленности в бюджетной сфере

Анализ правоприменительной практики свидетельствует о том, что при реализации национальных проектов и государственных программ наиболее криминализованной является сфера закупок, причем противоправные действия совершаются как представителями организаций, участвующих в закупках в качестве потенциальных исполнителей контрактов, так и должностными лицами органов государственной власти и местного самоуправления, а также подведомственных им организаций и учреждений.

Одним из способов совершения противоправных деяний является заключение картельных соглашений, не позволяющих другим участникам торгов снижать цену контракта и одерживать победу на аукционах на право заключения государственного контракта.

Так, например, в результате совместной с СЭБ ФСБ России, УФСБ России по Воронежской области и УЭБиПК ГУ МВД России по Воронежской области реализации оперативных материалов СЧ по РОПД ГСУ ГУ МВД России по Воронежской области 22 января 2020 г. возбуждено уголовное дело по ч. 3 ст. 30 УК РФ и ч. 2 ст. 178 УК РФ в отношении учредителя ООО «Комстрой», представителя ООО «Икстелеком», соучредителя ООО «СКС Пром», представителя ООО «АКС ГРУПП», представителя АО ФИРМА «СМУР» и по ч. 5 ст. 33 УК РФ, ч. 3 ст. 30 УК РФ, ч. 2 ст. 178 УК РФ в отношении заместителя директора Департамента организации строительства централизованных проектов Макрорегионального филиала «Центр» ПАО «Ростелеком», которые в результате заключения между хозяйствующими субъектами – конкурентами соглашений, запрещенных в соответствии с антимонопольным законодательством, обеспечивающих видимость конкурентной борьбы, и поддержания максимально высокой цены контракта заключили договоры, в том числе на строительство линий связи при реализации федерального проекта «Информационная инфраструктура» национальной программы «Цифровая экономика Российской Федерации» на общую сумму более 965 млн рублей, где незаконная прибыль составила бы 778 млн рублей.

На наш взгляд, в целях выявления картельных сговоров необходимо проводить оперативно-розыскные мероприятия, направленные на установление фактического местонахождения IP-адресов, с которых подавались заявки на электронные площадки. Отправление заявок и предложений с IP-адресов, находящихся по одному почтовому адресу, может свидетельствовать об аффилированности участвующих в торгах лиц и наличии ограничивающих конкуренцию соглашений.

По мнению авторов, расследование несвоевременно выявленных коррупционных преступлений в бюджетной сфере, когда проведение оперативно-розыскных мероприятий уже не актуально, а доказательственная база, которая могла бы содержаться на электронных или материальных носителях, уничтожена, сопряжено со значительными сложностями в доказывании. Проблемы выявления и расследования данной категории преступлений, как правило, обусловлены способами подготовки к совершению преступления и действиями по сокрытию его следов. Так, полномочия по подписанию документов делегируются неаффилированным подставным лицам, принятие решения или выражение согласия на подписание документов осуществляется коллегиально, взятки маскируются под законные платежи, вместо передачи денежных средств оплачиваются услуги, взятки передаются третьими лицами, не имеющими очевидных связей с взяткодателем или взяткополучателем, наличными или выплачиваются из специальных «фондов» (slush funds), не вовлеченных непосредственно в преступную схему. Кроме того, доказывание преступного умысла на совершение коррупционного преступления осложняют способы коммуникации преступников. Зачастую удаленное общение организуется через защищенные мессенджеры с шифрованием, во время встреч используются сообщения, написанные от руки или напечатанные на электронном устройстве, а сами встречи проводятся в местах, оговоренных злоумышленниками ранее (до попадания в орбиту внимания правоохранительных органов), а также на территориях ограниченного доступа или за границей.

При таких приемах противодействия со стороны лиц, совершающих противоправные действия, правоохранителям необходимо активнее использовать современные приемы и средства получения компьютерной информации, мониторинг сети Интернет, проводить сложные оперативно-розыскные мероприятия, ограничивающие конституционные права и свободы человека и гражданина, такие как снятие информации с технических каналов связи, получение компьютерной информации.

Одним из распространенных способов хищения бюджетных средств является их вывод через цепочку аффилированных организаций за рубеж. В последнее время для легализации (отмывания) доходов, полученных преступным путем, все чаще используются различные виртуальные активы, в том числе криптовалюты. В связи с этим особое значение для защиты средств бюджета, выделяемых на реализацию национальных проектов (программ), приобретает применение информационно-коммуникационных технологий. Вывод денежных средств за рубеж осуществляется, как правило, путем заключения мнимых внешнеэкономических сделок, в том числе с использованием фирм-однодневок, выявление которых возможно посредством программного сервиса АСК НДС-3, находящегося на «вооружении» налоговых органов. Данный программный комплекс позволяет полностью автоматизировать процесс контроля за движением средств между счетами юридических и физических лиц и повысить его продуктивность с 10 до 100 %. Алгоритм интеллектуального поиска дает возможность автоматически выстраивать цепочки движения денежных средств между юридическими и физическими лицами и видеть в числе прочего, уплачен ли налог на добавленную стоимость в этих цепочках. Принцип работы сервиса заключается в том, что программа сверяет все имеющиеся у нее данные между декларациями, книгами покупок и книгами продаж разных категорий налогоплательщиков, выявляя при этом цепочки контрагентов. Если имеются расхождения, программа автоматически формирует требование налогоплательщику о представлении пояснений по выявленным расхождениям. Такой сервис позволяет бороться с «фирмами-однодневками». С 2018 г. в базу АСК НДС-3 добавлена база кредитных учреждений, что еще более совершенствует новый сервис ФНС России для поиска незаконных вычетов НДС. При этом сервис АСК НДС-3 анализирует движение денежных средств не только между компаниями и индивидуальными предпринимателями, но и между компаниями и физическими лицами. Сервис АСК НДС-3 также обрабатывает данные кассовых аппаратов и сверяет их с книгами продаж. После запуска сервиса АСК НДС-3 государство вышло на новый уровень борьбы с «фирмами-однодневками», а также противодействия иным способам обналичивания денежных средств. При организации эффективного внешнего взаимодействия правоохранительные органы России могут использовать данный сервис в оперативных интересах, в том чисел и для противодействия хищениям бюджетных средств.

С мая 2019 г. ГУЭБиПК МВД России и подразделениями ЭБиПК территориальных органов МВД России на региональном

уровне используются возможности подсистемы управления национальными проектами ГИИС «Электронный бюджет» (ведется Минфином России), которая позволяет осуществлять контроль эффективности расходования бюджетных средств в режиме реального времени. Подключение ответственных сотрудников подразделений ЭБиПК к данному сервису позволяет проводить поисковые мероприятия, направленные на получение оперативно значимой информации, не выходя из кабинета.

В рамках указанных совещаний обращено внимание на ряд моментов, препятствующих надлежащему выполнению поставленных задач:

– необходимость заключения органами исполнительной власти субъектов Российской Федерации соглашений с Росфинмониторингом об организациях, участвующих в реализации национальных проектов, имеющих риски неисполнения обязательств по госконтрактам (риск-ориентированный подход), что позволит превентивно реагировать на негативные проявления со стороны недобросовестных подрядчиков и минимизировать факты хищения бюджетных средств;

– своевременное получение информации от органов исполнительной власти субъектов Российской Федерации о рисках нецелевого расходования и несвоевременного доведения средств, выделенных на реализацию национальных и федеральных проектов, а также иных нарушениях, возникающих в ходе реализации проектов.

Таким образом, в целях повышения эффективности противодействия преступлениям, связанным с неправомерным использованием денежных средств, выделенных из бюджетов всех уровней на реализацию национальных проектов, федеральных целевых программ, государственных программ субъектов Российской Федерации и муниципальных программ, руководителям территориальных подразделений ЭБиПК целесообразно:

– организовать систему оперативного отслеживания бюджетных средств – от главного распорядителя до конечного получателя с учетом региональной специфики и объемов бюджетного финансирования, в том числе обеспечить оперативным сотрудникам доступ к подсистеме управления национальными проектами ГИИС «Электронный бюджет», которая позволяет осуществлять контроль эффективности расходования бюджетных средств в режиме реального времени; проводить оценку коррупционных рисков в сфере закупок для государственных (муниципальных) нужд и закупок отдельными видами юридических лиц, устанавливать угрозы и уязвимости, требующие повышенного внимания правоохранительных

органов (внедрение риск-ориентированного подхода при выявлении и расследовании коррупционных преступлений, совершаемых в ходе закупочной деятельности), что позволит своевременно реагировать на складывающуюся оперативную обстановку в данной сфере. Суть данного подхода заключается в выявлении возможно проблемных организаций, для которых характерен ряд признаков: совершение подозрительных финансовых операций, в том числе до заключения госконтракта; отсутствие собственного капитала; малочисленность персонала и др.;

– завершить внедрение сервиса Росфинмониторинга «Личный кабинет правоохранительного органа», который позволит всем территориальным подразделениям МВД оперативно получать в электронном виде информацию о финансовых рисках экономики по всей стране;

– учитывать при планировании оперативно-розыскных мероприятий характеристики организаций, осваивающих бюджетные средства, выделенные на реализацию национальных проектов, используя информационные ресурсы, имеющиеся в Росфинмониторинге, Федеральной антимонопольной службе и налоговых органах; устанавливать их аффилированность должностным лицам, курирующим те или иные региональные программы (проекты), а также причастность к хищениям бюджетных средств и их последующей легализации.

Заключение

Подводя итоги, отметим, что в Российской Федерации с использованием информационно-коммуникационных технологий совершается целый спектр преступлений экономической направленности. Выявление и раскрытие этих противоправных деяний относится к компетенции подразделений ЭБиПК органов внутренних дел, которые наделены полномочиями на проведение оперативно-розыскной деятельности. Одной из ключевых организационно-управленческих мер при организации оперативно-розыскной деятельности по противодействию рассматриваемым видам преступлений является осуществление межведомственного взаимодействия.

Правовую основу межведомственного взаимодействия составляет обширный перечень законодательных и иных нормативных правовых актов, знание и соблюдение которых является необходимым условием его успешного осуществления. В правоприменительной практике следует учитывать, что правовая основа ОРД и межведомственного взаимодействия находится в состоянии динамичного развития и постоянного совершенствования, но все же, на наш взгляд, недостаточного в настоящее время для полного и своевременного реагирования на современные экономические цифровые угрозы.

Всякое взаимодействие оперативных и иных подразделений органов внутренних дел в сфере оперативно-розыскной деятельности по решению задач борьбы с преступностью в раскрытии преступлений может быть успешным лишь при наличии соответствующего информационного обеспечения, идет ли речь об информации, касающейся самого процесса взаимодействия, или об информации о преступлении и его раскрытии.

Несмотря на осуществляемые мероприятия по совершенствованию информационного обмена в сфере противодействия IT-преступности, одной из основных проблем остается недостаточный уровень организации взаимодействия органов внутренних дел с кредитными организациями, интернет-провайдерами, операторами сотовой связи и интернет-сервисов.

В целях устранения возможных недружественных действий между субъектами системы правоохранительных органов при обеспечении экономической безопасности осуществляется межведомственное взаимодействие, которое должно выстраиваться в фор-

ме совещаний и рабочих встреч[1]. При осуществлении межведомственного взаимодействия определяются принципы и направления согласованной деятельности и используются преимущества (положительный опыт) определенного органа для наиболее полного достижения целей при обеспечении экономической безопасности.

Перспективным направлением по противодействию преступлениям экономической направленности, совершаемым с использованием информационно-коммуникационных технологий, является межведомственное взаимодействие подразделений ЭБиПК с Росфинмониторингом, Росреестром, налоговыми органами, Федеральной антимонопольной службой Российской Федерации, банковскими организациями, которые располагают автоматизированными информационными ресурсами, позволяющими оперативно получать сведения, необходимые для решения задач оперативно-розыскной деятельности.

[1] Лаптев С. К. Некоторые аспекты выявления и расследования коррупционных преступлений // Актуальные проблемы юриспруденции: сб. статей по материалам XXXV Международной научно-практической конференции. Новосибирск, 2020. С. 66.

Список литературы

1. Ожегов, С. И., Шведова, Н. Ю. Толковый словарь русского языка. – М. : Азъ, 1994. – 960 с. – Текст : непосредственный.

2. Теория оперативно-розыскной деятельности : учебник / под ред. К. К. Горяинова, В. С. Овчинского, Г. К. Синилова. – М. : Норма, 2006. – 832 с. – Текст : непосредственный.

3. Кручинина, Н. В. Проблемы теории и практики проверки достоверности уголовно-релевантной информации в досудебном уголовном процессе. – М., 2019. – 166 с. – Текст : непосредственный.

4. Лаптев, С. К. Некоторые аспекты выявления и расследования коррупционных преступлений. – Текст : непосредственный // Актуальные проблемы юриспруденции : сб. статей по материалам XXXV Международной научно-практической конференции. – Новосибирск, 2020.

5. Тутуков, А. Ю. Основные детерминанты компьютерной преступности в российской Федерации. – Текст : непосредственный. // Пробелы в Российском законодательстве. – 2018. – № 3.

6. Аносов, А. В., Кашапова, Е. С. Понятие преступлений в сфере высоких технологий. – Текст электронный // Академическая мысль. – 2018. – № 4. URL: https://а.мвд.рф/nauka/-академическая-мысль-/архив-номеров (дата обращения: 17.07.2021).

7. Никеров, Д. М., Хохлова, О. М. Преступления в сфере высоких технологий в современной России. – Текст : непосредственный // Вестник Восточно-Сибирского института МВД России. – 2019. – № 2.

8. Фоменко, А. И. К вопросу об уголовно-правовой охране сферы высоких технологий как необходимого условия стабильного регионального развития. – Текст : непосредственный // Интеллектуальные ресурсы – региональному развитию. 2015. № 1–5.

9. Фаткуллин, Ф. Н. Проблемы теории государства и права : курс лекций. Казань : Казан. ун-т, 1987. – 336 с. – Текст : непосредственный.

10. Годунов, И. В. Энциклопедия противодействия этнической преступности. – 2-е изд., перераб. и доп. – М., 2005. – Текст : непосредственный.

11. Кураков, Д. В., Приходько, Н. Ю. Некоторые особенности выявления и раскрытия контрабанды оперативными подразделениями органов внутренних дел. – Текст : непосредственный. // Научный вестник Орловского юридического института МВД России имени В. В. Лукьянова. 2019. – № 2 (79).

12. Кудакова, К. С., Елфимов, О. М. Актуальные вопросы взаимодействия подразделений экономической безопасности и противодействия коррупции Министерства внутренних дел Российской Федерации и Федеральной налоговой службы России по вопросам «фирм-однодневок» (на материалах Нижегородской области). – Текст : непосредственный // Вестник Волжского университета имени В. Н. Татищева. – 2020. – Т. 2. – № 3 (46).

Приложение 1

МИНИСТЕРСТВО ВНУТРЕННИХ ДЕЛ РОССИЙСКОЙ ФЕДЕРАЦИИ (МВД России)

Главное управление экономической безопасности и противодействия коррупции (ГУЭБиПК МВД России)

Рязанский переулок, д. 1, Москва, 107078

Администрации криптовалютной биржи (название компании)

support@companyname.com

_____ № _____

на № _____ от _____

О предоставлении сведений

В связи с возникшей служебной необходимостью, руководствуясь ст. 13 Федерального закона от 07.02.2011 № 3-ФЗ «О полиции», ст. 6, 7, 15 Федерального закона от 12.08.1995 № 144-ФЗ «Об оперативно-розыскной деятельности», прошу предоставить имеющиеся сведения о лицах, которые использовали прилагаемые транзакции при совершении торговых операций на валютном рынке, включая статистические данные для IP-адресов, с которых была произведена регистрация, а также последующее администрирование счетов.

Дополнительно прошу предоставить реквизиты адресов криптовалюты в сети «Bitcoin», «Litecoin», «Ethereum», «TRON», связанных с этими лицами; сведения о совершаемых ими транзакциях; копии документов, предоставленных для идентификации, а также информацию о платежных средствах, используемых для пополнения фиатных счетов.

Ответ на запрашиваемую информацию прошу направить на адрес имяпользователя@mvd.ru (контактный телефон 8-916-000-00-00).

Приложение: сведения о совершенных операциях на 1 л.

Начальник
Ф.И.О.

Приложение 2

MINISTRY OF INTERNAL AFFAIRS OF THE RUSSIAN FEDERATION

Main Directorate of Economic Security and Combating the Corruption

1 Ryazansky alleyway, 107078, Moscow, Russia

_____ № _____

on № _____ from _____

「 Namecompany 」

support@namecompany.com

「 About providing information 」

Pursuant to article 13, part 1, paragraphs 3 and 4 of the Federal Law of February 7, 2011 No. 3-FZ «On the Police», articles 2, 6, 7, 8 and 13 of the Federal Law of August 12, 1995 No. 144-FZ «On Operational and Search Activity» please provide us available information concerning the persons who have used the attached transactions while trading and working on the currency market including statistic data for the IP-addresses from which the registration has been made as well as subsequent administrating of the accounts.

We request also information on the cryptocurrency addresses in the «Bitcoin», «Litecoin», «Ethereum», «TRON» network related to the aforesaid persons, on the transactions performed by them and copies of the documents presented for verification as well as information about the means of payment used for replenishment of the fiat accounts.

Taking into account tight schedule of the inspection please provide the requested information by e-mail to the address 0000000@mvd.ru (contact telephone number 8-000-000-00-00).

Annex: 1 pp., 1 copy, no copies retained, w/n.

Head of the department
S.N.P.

Запрос в Росфинмониторинг о предоставлении информации

Направляется в

_____

(структурное подразделение, территориальный орган Росфинмониторинга)

Объекты проверки

_____

(краткое наименование организации, фамилия и инициалы лица)

Всего _____ юридических лиц (ЮЛ) _____, физических лиц (ФЛ)

1. Цель проверки: получение сведений об осуществлении объектами проверки финансовых операций (сделок), связанных с легализацией (отмыванием) доходов, полученных прцеступным путем

2. Инициатор запроса

_____

(структурное подразделение, территориальный орган)

3. Основания для направления запроса:

3.1. Расследование уголовного дела

Номер уголовного дела								
Дата возбуждения уголовного дела								
(рег. № _____ от __ _____ 20__ г.)	(дд)		(мм)		(гггг)			

Статьи УК РФ, по которым возбуждено уголовное дело_____

_____

_____

Наименование органа, осуществляющего предварительное расследование _____

_____

3.2. Проверочные мероприятия_____

(х - в случае проведения проверочных мероприятий)

3.3. Необходимость уточнения или дополнения ранее направленного запроса

Исходящий номер запроса

Дата запроса								
	(дд)		(мм)		(гггг)			

4. Описание характера противоправной деятельности проверяемых

_____

_____

_____

Сведения о возможной легализации (отмывании) преступных доходов

_____

_____

5. Период времени, в течение которого предположительно совершались противоправные действия: с _____ по _____

Приложение: _____

Всего на _____ л.

Начальник _____ _____ _____

(должность) (подпись) (Ф.И.О.)

Рег. № _____ от __ _____ 20__ г.

Учебное издание

Искалиев Равиль Гарифуллаевич,
Катков Дмитрий Владимирович,
Телков Александр Валериевич и др.

ОРГАНИЗАЦИЯ МЕЖВЕДОМСТВЕННОГО ВЗАИМОДЕЙСТВИЯ ПОДРАЗДЕЛЕНИЙ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ И ПРОТИВОДЕЙСТВИЯ КОРРУПЦИИ СИСТЕМЫ МВД РОССИИ В СФЕРЕ ПРОТИВОДЕЙСТВИЯ ПРЕСТУПЛЕНИЯМ, СОВЕРШАЕМЫМ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

Редактор А. А. Уварова
Верстка С. Н. Портновой

Подписано в печать 02.08.2023. Формат 60 × 84 $^{1}/_{16}$.
Усл. печ. л. 3,49. Уч.-изд. л. 3,1. Тираж 42 экз. Заказ 41у

Отделение полиграфической и оперативной печати РИО
Академии управления МВД России
125171, Москва, ул. Зои и Александра Космодемьянских, д. 8

ISBN 978-5-907530-83-6