О Т З Ы В

официального оппонента на диссертацию Простосердова Михаила Александровича по теме «Экономические преступления, совершаемые в киберпространстве, и меры противодействия им», представленную на соискание ученой степени кандидата юридических наук по специальности 12.00.08. – уголовное право и криминология; уголовно-исполнительное право

Актуальность темы исследования.

Тема, положенная диссертантом в основу своего диссертационного исследования, представляется весьма актуальной. Понятие киберпространства сегодня используется уже не только в компьютерных и философских отраслях знаний, но и в сегменте массового потребления. Широкое развитие мобильных устройств, с выходом в интернет, относительно невысокая стоимость подключения к сети, перевод экономических взаимоотношений в виртуальное пространство, а также возможности новых компьютерных технологий создали предпосылки для незаконного, бесконтактного изъятия денежных средств и распространения новых экономических преступлений в виртуальном пространстве. Современное киберпространство это не просто удобный способ представления и описания объектов, широко распространенных в компьютерной сети, но и место, где преступники реально причиняют существенный материальный ущерб потерпевшим, а кибербезопасность становится проблемой № 1, не только для граждан, но и для финансовой системы государства в целом. Для обоснования подобного посыла приведем данные исследователей изложенные на сайте компании РосБизнесКонсалтинг. Например, «объем ущерба, который киберпреступники нанесли России в 2015 году, составил около 70 млрд. руб. ($1 млрд.), заявил первый заместитель председателя Сбербанка Лев Хасис на пресс-конференции «Лаборатории Касперг-

ского». Государство не до конца понимает уровень угрозы от киберпреступлений, а ответственность за них недостаточно серьезная.

Ежегодные потери мировой экономики от кибератак Всемирный банк (World Bank) оценивает в $445 млрд. По расчетам экспертов исследовательской компании Allianz Global Corporate & Specialty, который был опубликован в сентябре 2015 года, наибольший ущерб от действий хакеров приходится на США — $108 млрд., второе и третье места занимают Китай ($60 млрд.) и Германия ($59 млрд.) соответственно. Россия занимает восьмое место в рейтинге крупнейших экономик по масштабу ущерба от действий хакеров. Ее ежегодный ущерб оценивается в $2 млрд., или 0,1% ВВП»[1].

Нельзя сказать, что правоохранительные органы не занимаются данной проблематикой. Например, в 2015 году МВД России выявило организованную преступную группу, поставившую под угрозу безопасность всей банковской системы страны. «Как заявил глава управления «К» по борьбе с преступлениями в сфере компьютерной безопасности МВД России Алексей Мошков, мошенники пытались совершить хищение 1,5 млрд. рублей практически из всех банков России. Ключевым направлением деятельности группы было осуществление атак на процессинговые центры российских и мировых банков, а также пункты обмена межбанковскими сообщениями. Им удалось скомпрометировать крупнейшие международные платежные системы. Более того, в целях облегчения вывода денежных средств они создали в соответствии с международными правилами собственную платежную систему и активно ей пользовались»[2].

Но, несмотря на отдельные успехи правоохранительных органов, считаем верным мнение соискателя о том, что новые преступные экономические

---

[1] Сбербанк оценил годовой ущерб России от киберпреступлений в $1 млрд. // URL: http://www.rbc.ru/technology_and_media/09/12/2015/566837819a7947e4cbc991b6 (дата обращения 22.03.2016).

[2] МВД рассказало о попытке хищения денег у большинства российских банков // URL: http://www.rbc.ru/politics/04/02/2016/56b30b459a7947a50a165a79 (дата обращения 22.03.2016).

деяния, совершаемые в этой сфере, нередко остаются вне действия уголовного закона, а в отношении уже совершенных преступлений возникают существенные проблемы правовой оценки деятельности виновных. С учетом экспертных опросов, а также по сведениям, полученным из открытых информационных источников, можно констатировать предположение о том, что показанные преступления обладают не только значительной латентностью, но и предъявляют высокие требования к профессионализму сотрудников оперативных и следственных подразделений. Приведенные в работе данные явно свидетельствуют о недостаточной эффективности своевременной реакции правоохранительных структур, на экономические преступления, совершаемые в киберпространстве. Можно предъявлять справедливые претензии по всем составляющим профилактической работы, начиная от качества и эффективности уголовного закона, заканчивая государственно-правовым и специальным обеспечением защиты экономического киберпространства от преступных посягательств. Работа М.А. Простосердова конкретизирует и развивает эти положения.

Актуальности работы соискателя не преуменьшает тот факт, что многие вопросы затронутой темы уже становились предметом рассмотрения на уровне кандидатских и даже докторских исследований и монографий. Проведенное им исследование является научно-квалификационной работой, в которой содержится решение задачи, имеющей существенное значение для соответствующей отрасли знаний уголовного законодательства, повышения эффективности правовых и криминологических мер противодействия экономическим преступлениям, совершаемым в киберпространстве России, что свидетельствует не только об актуальности работы, но и об ее новизне.

Цель работы, поставленная перед собой М.А. Простосердовым, - научная разработка теоретических и практических аспектов охраны экономических отношений в условиях посягательства на них в киберпространстве, обоснование теоретических положений о понятии, содержании киберпресту-

плений, их видах, об использовании понятия киберпространство в системе признаков состава преступления и о рекомендациях правового и криминологического характера по созданию системы мер противодействия всему комплексу экономических преступлений, совершаемых в киберпространстве. Данная цель вполне успешно достигнута диссертантом за счет последовательного решения задач им выделенных.

Можно говорить, о недостатках или противоречиях отдельных положений диссертационного исследования, в том числе о недостатках представленных аргументов или их наполнения. Но, во-первых, оценивая работу, следует исходить не только из собственного представления о чем-либо, а принимать во внимание те цели и задачи, которые ставил перед собой диссертант, а, во-вторых, данное исследование представляет собой новое направление в сравнительном анализе и изучении проблем квалификации экономических преступлений в виртуальном пространстве, в сфере использования компьютерных технологий.

Объект исследования (общественные отношения, складывающиеся в процессе реализации уголовного законодательства об ответственности за экономические преступления (преступления против собственности и преступления в сфере экономической деятельности), совершаемые в киберпространстве, а также меры противодействия указанным преступлениям) установлен, верно, и в полном соответствии с названием работы и той целью, достижению которой посвящена диссертация. Нет претензий и к **предмету** диссертационного исследования.

Не вызывают сомнений **методология и методика исследования, его нормативная, теоретическая и эмпирическая базы.**

Так, М.А. Простосердов, основываясь на диалектическом методе познания, активно использовал в работе общие и частные методы исследования: сравнительно-правовой и историко-правовой методы позволили автору изучить содержание норм зарубежного и российского уголовного

законодательства в сфере экономических отношений и защиты компьютерной информации; социологические методы использовались при опросе респондентов по проблемным вопросам предупреждения киберпреступлений; с помощью синтеза было получено новое знание по всему комплексу экономических преступлений, совершаемых в киберпространстве.

Нет нареканий к *нормативному аспекту* диссертационного исследования, который обширен. Причем автор обращался, как к законам, так и к подзаконным нормативно-правовым актам, широко применяемым в сфере связи, информации и защиты экономических отношений. Использовался и зарубежный опыт выявления содержания хищения чужого имущества путём использования средств компьютерной техники (например, опыт Белоруссии (с. 47 диссертации), США (с.с. 49, 52 диссертации), Италии, Китайской Народной Республики, Нидерландов, Германии, Японии и других стран).

Более, чем достаточна *теоретическая база* диссертационного исследования. М.А. Простосердов использовал не только уголовно-правовые и криминологические работы, но и работы по IT-технологиям, основам дистанционного банковского регулирования, гражданскому праву, экономической теории и др. (в относимом аспекте к теме диссертации). Количество источников исчисляется цифрой более 260.

Не вызывает возражений *эмпирическая база* диссертации, во многом позволяющая судить **об обоснованности и достоверности авторских выводов** (по свидетельству М.А. Простосердова, он изучил: данные 100 уголовных дел об экономических преступлениях, совершенных в киберпространстве, рассмотренных судами различных субъектов Российской Федерации; данные статистики Бюро специальных технических мероприятий МВД РФ, центров реагирования на компьютерные инциденты («CERT.RU», «GOV-CERT.RU», «CERT-GIB», «Лаборатория Касперского», «Яндекс», «Mail.Ru

Group» и др.) и зарубежных IT-компаний за 2011-2015 годы; результаты анкетирования 96 судей районных и областных судов Российской Федерации, в том числе председателей районных и областных (городских) судов Москвы, Санкт-Петербурга, Владивостока, Нижнего Новгорода, Тамбова, Уфы, и других регионов России.

Подтверждение использования результатов социологического опроса нами найдены на страницах работы (см.: с.с. 70, 153 диссертации). В свою очередь, результаты анкетирования имели бы более полноценное научное сопровождение при использовании сведений от иных респондентов, а именно сотрудников правоохранительных органов и лиц, осужденных за подобные преступления.

Научная новизна работы, выводов и рекомендаций, сформулированных в диссертации, обусловлена, прежде всего, формулированием темы кандидатской диссертации, о чем выше уже шла речь.

Автором сделана попытка (и в целом, довольно удачная) закрепить определенный порядок применения некоторых положений и понятий киберпространства, как в общей системе квалификации преступлений, так и в системе предупреждения экономической преступности. На основе изучения новых способов совершения экономических киберпреступлений предложена их авторская систематизация, что несет в себе несомненную положительную составляющую для правоприменителей. С учетом методики прогнозирования была разработана долгосрочная система мер противодействия комплексу экономических преступлений, совершаемых в киберпространстве.

Научная новизна диссертационного исследования заключается также в новизне положений, выносимых автором на защиту, большинство из которых должны быть поддержаны и одобрены (см. далее). В то же время, хотелось бы отметить, что диссертант вынес на защиту далеко не все из того нового и важного, что наработано им в обозначенном выше направлении.

Безусловны **теоретическая и практическая значимость** исследования, предпринятого М.А. Простосердовым. Теоретическая значимость, при этом, опирается на научную новизну исследования и заключается в том, что предложенные автором положения и выводы дополняют научные представления о противодействии преступлениям в сфере экономики при использовании киберпространства. Полученные результаты, безусловно, смогут найти применение в последующих научных исследованиях, давая им новое направление и развитие. Практическая значимость заключается в том, что представленные авторские выводы могут быть положены в основу нового Постановления Пленума Верховного Суда Российской Федерации «О судебной практике по делам о компьютерных преступлениях», а также в рекомендации сотрудникам правоохранительных органов по квалификации рассматриваемой категории преступлений.

Апробация результатов диссертационного исследования достаточна для кандидатской диссертации. Автор имеет девять опубликованных научных работ (3 – в ведущих рецензируемых научных журналах, рекомендованных Высшей аттестационной комиссией Министерства образования и науки РФ). Основные выводы диссертации внедрены в учебный процесс ФГБОУ ВО «Российского государственного университета правосудия» при преподавании дисциплин «Уголовное право» и «Криминология» и докладывались на ряде научно-практических конференций, в том числе, всероссийских и международных. Результаты научного исследования внедрены в деятельность федеральных районных судов и органов прокуратуры при повышении квалификации сотрудников, что подтверждается соответствующими актами о внедрении.

Структура работы включает введение, три главы, делящиеся на параграфы (всего их девять), заключение, список использованной литературы и приложение. Структура довольно логична, работа написана хорошим науч-

ным языком, легко читается. Кандидатская диссертация, без сомнения, состоялась.

Следует отметить, что автор не ограничивается теоретическими выкладками и умозрительными конструкциями, он доводит их до практических рекомендаций, что придает работе особую ценность. Нет необходимости подробно останавливаться на всех положениях представленного исследования. Ограничимся лишь наиболее существенными, аргументированными и заслуживающими поддержки, достоинствами диссертации М.А. Простосердова.

Например, заслуживает внимания предложенная М.А. Простосердовым классификация экономических киберпреступлений в зависимости от способа совершения:

– экономические киберпреступления, совершаемые путём психологического воздействия на человека с использованием компьютерной и иной аналогичной техники (обман, введение в заблуждение, угрозы);

– экономические киберпреступления, совершаемые путём воздействия на оборудование (компьютеры, смартфоны, маршрутизаторы и иное оборудование). Подобная систематизация позволяет не только распределить указанные преступления по главам уголовного законодательства, но и представляет практический интерес при раскрытии, расследовании и предупреждении подобных деяний.

Представляется актуальным достаточно содержательный анализ нормативных документов в сфере кибербезопасности, среди которых выделим Будапештскую Конвенцию Совета Европы «О киберпреступности» от 23 ноября 2001 года. Данная Конвенция не была подписана Российской Федерацией, так как многие её положения противоречат национальному законодательству России и нарушают её интересы. Однако учитывая то, что в Российской Федерации национальная стратегия кибербезопасности находится лишь в проекте, показанный документ представляет нам исходные положе-

ния для разработки подобной стратегии и совершенствования уголовного законодательства.

Следует признать логику и в том, что в виртуальном пространстве сложно установить место совершения экономических киберпреступлений. Ведь, киберпространство – это основное средство для совершения рассматриваемых деяний, и оно создаёт все необходимые условия для их совершения дистанционно. Местом их совершения следует считать территориальное пространство, где виновный совершил ввод компьютерных данных, то есть точку доступа в киберпространство (конкретную квартиру или Интернет-кафе).

Поддерживаем авторскую позицию в реализации международного сотрудничества по предупреждению экономических киберпреступлений. В диссертации (см.: с. 145 диссертации) правильно указано, что киберпространство само по себе экстерриториально – в нём нет границ, нет государств. Данная проблема серьезно усложняет работу правоохранительных органов. Некоторые экономические преступления, совершаемые в киберпространстве, в России либо вовсе не криминализированы, либо являются административными правонарушениями.

Возможна и обратная проблема: криминализированные в России общественно опасные деяния могут не являться таковыми в других странах. С учетом этих и других возникающих проблем, следует признать актуальным разработку под эгидой ООН новой универсальной конвенции по противодействию преступлениям в сфере кибербезопасности. Тем более данной работой уже занималась межправительственная группа экспертов Управления ООН по наркотикам и преступности. По итогам ее работы было подготовлено исследование по проблематике киберпреступности, где также указывалось на необходимость разработки подобной конвенции.

Таким образом, сформулированные в диссертационном исследовании выводы и рекомендации свидетельствуют о творческой зрелости соискателя,

его способности к самостоятельной аналитической работе. Приведенные фактические данные, будучи интересными сами по себе, составляют важнейшую часть системы аргументов диссертанта, свидетельствуя о его достаточно глубоком знании теоретического аспекта проблемы и запросов практики.

Высоко оценивая проделанную работу М.А. Простосердовым в целом, по праву официального оппонента, уместно обратить внимание и на некоторые, с нашей точки зрения, замечания:

1) Некоторые выводы в диссертации имеют под собой недостаточную степень обоснования и аргументации в их правоприменительном аспекте. Например, в положении на защиту под № 3 автор предлагает тезис о том, что криптовалюта, как цифровой информационный продукт, может выступать предметом хищения в преступлениях, предусмотренных статьями 159, 159.6 и 160 УК РФ. Однако законодатель, формулируя понятие хищения, прежде всего, указал на противоправные безвозмездное изъятие и (или) обращение чужого имущества. Тем самым выделяется то, что похищаемое имущество должно иметь характеристики предмета материального мира (в частности, физические признаки), а предмет хищения – это вещь, созданная трудом человека, имеющая форму, вес, объем, количество и другие параметры вещных свойств. В свою очередь, криптовалюта, в частности «Биткойн» (BTC) – это электронный механизм обмена, своеобразная платежная система, где используются криптографические методы обеспечения и функционирования транзакций между адресатами системы. Обмен на товары или другие денежные средства происходит через онлайн-сервисы без выделения в общественных отношениях материального носителя показанной информации. Носителями компьютерной информации, как правило, являются накопители флеш-памяти, оптические и жесткие диски и т.д. В этой связи, на защите хотелось бы услышать авторские пояснения того, на каком этапе экономиче-

ского преступления криптовалюта приобретет вещный характер объекта материального мира и необходимые признаки предмета хищения.

2) В предлагаемом диссертационном исследовании проводится анализ различных аспектов борьбы с экономическими преступлениями, совершаемыми в киберпространстве, и автор в целом корректно использует исследованный материал. Однако в некоторых выводах диссертанта имеются неточности технического характера, которые частично влияют на качество воспринимаемой информации. Например, на стр. 42 диссертации указано, что в 1998 году при Бюро специальных технических мероприятий МВД РФ было образовано Управление «К», целью которого является расследование исключительно компьютерных преступлений. Однако на сайте МВД РФ находим, что основными направлениями работы Управления «К» БСТМ МВД России считаются: борьба с преступлениями в сфере компьютерной информации; пресечение противоправных действий в информационно-телекоммуникационных сетях, включая сеть Интернет; выявление и пресечение фактов нарушения авторских и смежных прав в сфере информационных технологий; борьба с международными преступлениями в сфере информационных технологий; международное сотрудничество в области борьбы с преступлениями, совершаемыми с использованием информационных технологий. Расследование преступлений не является направлением работы данной службы.

На стр. 69 диссертации выделено, что при списании ВТС на сумму 1000 рублей без ведома собственника происходит не просто неправомерный доступ к компьютерной информации из корыстных побуждений, а хищение путём неправомерного безвозмездного обращения в пользу виновного 1000 рублей в форме ВТС. В данном случае обращаем внимание на то, что указанная сумма подпадает не под признаки уголовного законодательства, а под признаки ст. 7.27 КоАП РФ, где хищение чужого имущества признается мел-

ким, если стоимость похищенного имущества не превышает одну тысячу рублей.

3) На стр. 130 диссертации указывается, что анонимность в киберпространстве является основным детерминантом киберпреступлений и фактором высокого уровня латентности преступности в киберпространстве. Находим, что авторская позиция была бы более убедительной при подтверждении вывода соответствующими исследовательскими показателями или примерами из практики деятельности правоохранительных органов.

4) Одной из особенностей рассмотренного диссертационного исследования является то, что автор для обоснования полученных результатов использует следующие суждения: «киберпреступление», «компьютерное преступление», «преступление в сфере компьютерной информации», «преступления, совершаемые в киберпространстве» (с.с. 24-25 диссертации). Однако в уголовном законодательстве закреплено только понятие «преступлений в сфере компьютерной информации». Предлагая свою терминологию в этой проблематике автор, к сожалению, не указал соотношение указанных определений, критерии эффективности их применения, а также соответствующие нормативно-правовые акты или нормы уголовного закона, где соискатель предлагает раскрыть их содержательный аспект. В любом случае, хотелось бы услышать на защите пояснения по этому поводу.

Сделанные замечания, тем не менее, носят, в основном, так называемый, оппонентский характер и не влияют на общую положительную оценку диссертационного исследования, проделанного М.А. Простосердовым.

Автореферат отражает основные моменты диссертации.

ОБЩИЙ ВЫВОД: Диссертационная работа М.А. Простосердова соответствует требованиям раздела II Положения о присуждении ученых степеней, утвержденного Постановлением Правительства Российской Федерации от 24 сентября 2013 г. № 842, является научно-

квалификационной работой, в которой содержится решение задачи, имеющей значение для развития уголовно-правовых и криминологических отраслей знания об экономических преступлениях, совершаемых в киберпространстве, а ее автор – Михаил Александрович Простосердов – заслуживает присуждения искомой ученой степени кандидата юридических наук по специальности 12.00.08 – уголовное право и криминология; уголовно-исполнительное право.

Официальный оппонент:

Заведующий кафедрой организации правоохранительной деятельности
Тамбовского государственного университета
им. Г.Р. Державина
доктор юридических наук, доцент Михаил Александрович Желудков

392008, г. Тамбов, ул. Советская, 181 «Б»

Телефон: 8 (4752) 53-22-41

E-mail: institytprava@mail.ru

Подпись заведующего кафедрой М.А. Желудкова заверяю:

Директор Института права и национальной безопасности
ТГУ им. Г.Р. Державина
кандидат юридических наук, доцент Вера Анатольевна Шуняева

25 апреля 2016 г.

Желудков Михаил Александрович, доктор юридических наук, доцент (диссертация на соискание ученой степени доктора юридических наук защищена по специальности 12.00.08 – уголовное право и криминология; уголовно-исполнительное право).

ЗАВЕРЯЮ
Начальник управления кадровой политики
« 25 » 04 2016 г.