На правах рукописи

Простосердов Михаил Александрович

ЭКОНОМИЧЕСКИЕ ПРЕСТУПЛЕНИЯ, СОВЕРШАЕМЫЕ В КИБЕРПРОСТРАНСТВЕ, И МЕРЫ ПРОТИВОДЕЙСТВИЯ ИМ

12.00.08 - уголовное право и криминология;
уголовно-исполнительное право

АВТОРЕФЕРАТ
диссертации на соискание ученой степени
кандидата юридических наук

Москва – 2016

Работа выполнена на кафедре уголовного права в Федеральном государственном бюджетном образовательном учреждении высшего образования «Российский государственный университет правосудия»

Научный руководитель	Заслуженный юрист Российской Федерации доктор юридических наук, профессор **Бриллиантов Александр Владимирович**
Официальные оппоненты	**Желудков Михаил Александрович** доктор юридических наук, доцент заведующий кафедрой организации правоохранительной деятельности Института права и национальной безопасности, ФГБОУ ВПО «Тамбовский государственный университет имени Г.Р. Державина»
	Гузеева Ольга Сергеевна кандидат юридических наук прокурор отдела государственной статистики управления правовой статистики Главного организационно-аналитического управления Генеральной прокуратуры Российской Федерации
Ведущая организация	ФГБОУВО «Московский государственный университет им. М.В. Ломоносова»

Защита состоится «14» июня 2016 года в 12:00 часов на заседании диссертационного совета Д 170.003.01, созданного на базе Федерального государственного бюджетного образовательного учреждения высшего образования «Российский государственный университет правосудия», по адресу: 117418, г. Москва, ул. Новочеремушкинская, д. 69, ауд. 910.

С диссертацией можно ознакомиться в библиотеке и на сайте Федерального государственного бюджетного образовательного учреждения высшего образования «Российский государственный университет правосудия».

Диссертация и автореферат размещены на официальном сайте Федерального государственного бюджетного образовательного учреждения высшего образования «Российский государственный университет правосудия» по адресу http://www.rgup.ru/

Автореферат разослан «_____»_____ 2016г.

Ученый секретарь
диссертационного совета С. П. Ломтев

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность исследования. С развитием современных технологий сформировались условия к появлению нового вида преступлений, совершаемых в киберпространстве (киберпреступлений). Большинство из этих преступлений являются экономическими и способны причинить реальный вред отношениям собственности и нормальному порядку осуществления предпринимательской или иной экономической деятельности. В науке уголовного права и криминологии активно ведутся дискуссии о понятии, природе, видах киберпреступлений и мерах противодействиях им.

Этому новому виду преступности необходимо противопоставить действенные меры, в число которых входят и меры уголовно-правового воздействия. Однако действующее отечественное уголовное законодательство не всегда успевает реагировать на вызовы современной преступности. Поэтому новые реально опасные деяния, совершаемые в киберпространстве, нередко остаются вне сферы действия уголовного закона, а в отношении уже криминализированных деяний возникают существенные проблемы их правовой оценки и привлечения виновных к ответственности. Данное обстоятельство и обуславливает актуальность темы исследования.

Актуальность исследованию придаёт и тот факт, что размер причиняемого экономическими киберпреступлениями ущерба за последние годы многократно вырос. По мнению многих ученых, доходы теневого бизнеса в сети «Интернет» могут сравниться с прибылью от незаконной торговли наркотиками. Ежегодные потери мировой экономики от экономических преступлений, совершаемых в киберпространстве, составляют 500 миллиардов долларов. Тенденция роста киберпреступлений имеется и в России, где уже ежедневно совершается 44 хищения из систем дистанционно-банковского обслуживания. Более того, согласно статистическим данным Европола за 2013-2014 годы, большинство хакеров и киберпреступников в Европе – это граждане России и стран СНГ. Одновременно на эффективность противодействия

киберпреступлениям негативно влияет очень высокий уровень латентности, как экономических преступлений, совершаемых в киберпространстве, так и преступлений в сфере компьютерной информации.

Степень разработанности темы. В России существует несколько фундаментальных исследований, посвященных проблеме киберпреступности. Однако все они основаны на законодательстве своего времени (1996 – 2008 гг.), и многие их положения уже не являются достаточно актуальными. Более того, существующие исследования посвящены в целом всем киберпреступлениям, в то время как специальные исследования именно экономических киберпреступлений не проводились.

Отдельные уголовно-правовые и криминологические вопросы экономических преступлений, совершаемых в киберпространстве либо сети «Интернет», в отечественной науке рассматриваются в работах А.И.Бойцова, А.Г. Волеводза, Б.В. Волженкина, В.Г. Голубева, О.С. Гузеевой, М.С. Дашяна, Д.В. Добровольского, И.А. Клепицкого, Н.Н. Ковалевой, А.Н. Копырюлина, Т.М. Лопатиной, В.Г. Степанова-Егиянца, П.С. Яни и многих других.

По теме противодействия киберпреступности и ответственности за совершение компьютерных преступлений выполнено несколько диссертационных работ: В.Б. Вехова, Р.И. Дремлюги, Н.В. Зигуры, Т.П. Кесареевой, Н.Н. Лыткина, И.М. Рассолова, М.В. Старичкова, Т.Л. Тропиной. Указанные диссертации внесли определенный вклад в исследование киберпреступлений и киберпространства, однако проблема экономических преступлений, совершаемых в киберпространстве, была затронута лишь частично. Поэтому в настоящей работе с учетом уже имеющихся исследований и действующего законодательства, в большей, чем ранее, мере раскрываются вопросы о понятии, объекте и предмете киберпреступлений в сфере экономики, способах совершения экономических киберпреступлений и уголовно-правовых мер противодействия им.

Целью диссертационного исследования является научная разработка теоретических и практических аспектов охраны экономических отношений в условиях посягательства на них в киберпространстве, обоснование теоретических положений о понятии, содержании киберпреступлений, 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.

Достижению указанной цели служат постановка и разрешение комплекса следующих **задач**:

- теоретически обосновать понятие киберпреступления и определить место киберпреступлений, как в общей системе преступлений, так и в системе экономических преступлений;
- исследовать составы экономических преступлений, совершаемых в киберпространстве, с целью выявления их специфических признаков, дать классификацию экономических киберпреступлений;
- исследовать социально-правовую специфику экономических отношений, которые подвержены посягательствам в киберпространстве, а также теоретически обосновать значение киберпространства как признака рассматриваемых составов;
- на основе сравнительно-правовой методологии определить современное состояние и тенденции развития российского и зарубежного уголовного законодательства, направленного на защиту экономических отношений от киберпреступлений, с целью выявления положительных моментов, которые могут быть использованы в российском законодательстве;
- обобщить практику применения норм об уголовной ответственности за киберпреступления в сфере экономики, выявить ее основные тенденции, на основании чего предложить научный прогноз дальнейшего развития практики и выработать конкретные рекомендации уголовно-правовой оценки таких деяний;

- с использованием криминологической методологии определить конкретные детерминанты экономической киберпреступности и выявить уровень ее латентности;

- на основе эмпирического материала сформировать криминологический портрет киберпреступника и потерпевшего, дать типологизацию киберпреступников, определить наиболее виктимные группы населения и сферы экономической деятельности;

- выработать научно обоснованные рекомендации по совершенствованию правовых и организационных мер противодействия экономическим преступлениям, совершаемым в киберпространстве, действующего уголовного законодательства в части охраны прав и интересов пользователя киберпространства, а также практики его применения.

Объектом исследования являются 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.

Предмет исследования составляют:

1. действующее уголовное законодательство Российской Федерации в части уголовно-правовых норм, охраняющих экономические отношения от посягательств в киберпространстве, а также отношения, обеспечивающие правомерный доступ, создание, обработку, приобретение, использование компьютерной информации;

2. практика реализации уголовно-правовых норм, направленных на охрану прав и интересов лиц в сфере экономических отношений (собственности и экономической деятельности) от посягательств в киберпространстве, а также в сфере компьютерной информации и информационно-телекоммуникационных сетей;

3. статистические и аналитические материалы органов предварительного расследования и суда по рассматриваемой проблеме;

4. зарубежное уголовное законодательство, а также международные акты, такие как Конвенции Совета Европы, Резолюции Генеральной Ассамблеи ООН и другие;

5. материалы СМИ и других источников по проблемам посягательств на экономические отношения в киберпространстве, а также посягательств в сфере компьютерной информации и информационно-телекоммуникационных сетей.

Методологическую основу работы составляют диалектический метод познания, общенаучные и формально-логические методы (сравнение, гипотеза, системно-структурный анализ), а также специально-научные и криминологические методы, такие как: метод анализа документов; историко-правовой и сравнительно-правовой метод; метод экспертного опроса.

Теоретическую базу составили работы следующих отечественных ученых: Р.А. Барышева, А.И.Бойцова, А.Г. Волеводза, Б.В. Волженкина, Р.И. Выкова, В.Г. Голубева, О.С. Гузеевой, М.С. Дашяна, М.Ю. Дворецкого, Р.И. Дремлюги, М.А. Желудкова, Д.А. Зыкова, И.А. Клепицкого, А.Н. Копырюлина, Т.М. Лопатиной, С.С. Медведева, И.М. Рассолова, В.Г. Степанова-Егиянца, Т.Л. Тропиной, С.Н. Хуторной, А.В. Шульги, П.С.Яни и многих других.

Нормативной основой стало отечественное и зарубежное уголовное законодательство, международные правовые акты об ответственности за преступления в сфере экономики (преступления против собственности, преступления в сфере экономической деятельности), в сфере компьютерной информации, а также иные нормативные правовые акты, регулирующие отношения в сфере связи, информации и ее защиты.

Эмпирическую основу исследования составляют результаты опроса 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; результаты изучения 100 уголовных дел об экономических преступлениях, совершенных в киберпространстве, рассмотренных районными, городскими и областными судами субъектов Российской Федерации: г. Москва, г. Санкт-Петербург, Приморский край, Самарская область, Тамбовская область, а также районными судами других субъектов Российской Федерации; результаты изучения статистических данных о состоянии и структуре киберпреступности, о личности киберпреступника и личности его жертв Бюро специальных технических мероприятий МВД РФ, центров реагирования на компьютерные инциденты («CERT.RU», «GOV-CERT.RU», «CERT-GIB»), а также отечественных (ЗАО «Лаборатория Касперского», ООО «Яндекс», «Mail.Ru Group» и др.) и зарубежных IT-компаний («Norton») за 2011-2015 годы. Использованы материалы судебной практики Верховного Суда Российской Федерации и судов общей юрисдикции за 2009-2014 годы.

Научная новизна. В исследовании дано авторское теоретическое обоснование и приведено понятие киберпреступления, определено место киберпреступлений, как в общей системе преступлений, так и в системе экономических преступлений, разработан вопрос об использовании киберпространства в системе признаков состава преступления. В исследовании дано теоретическое обоснование расширения предмета хищения. Впервые на уровне диссертационного исследования были изучены способы совершения экономических киберпреступлений (включая преступления против собственности и преступления в сфере экономической деятельности), дана авторская классификация экономических киберпреступлений. Определены тенденции развития отечественного и зарубежного уголовного законодательства, направленного на защиту экономических отношений от киберпреступлений. Предложен научный прогноз дальнейшего развития практики норм об уголовной ответственности за киберпреступления в сфере экономики и выработаны конкретные рекомендации уголовно-правовой оценки таких деяний. Определены общие и специальные детерминанты экономической

киберпреступности, сформирован криминологический портрет экономического киберпреступника и потерпевшего, а также определены наиболее виктимные группы населения и сферы экономической деятельности. На основе полученных данных была разработана и предложена система мер противодействия всему комплексу экономических преступлений, совершаемых в киберпространстве. Необходимой степенью новизны обладают и положения, выносимые на защиту.

Теоретическая значимость полученных результатов.

Полученные новые результаты исследования развивают научные представления о противодействии преступлениям в сфере экономики, совершаемым с использованием киберпространства. В работе дано теоретически обоснованное понятие «киберпреступления» с учетом специфики средства и способа его совершения, а также приведено теоретическое обоснование киберпространства как основного средства совершения киберпреступления.

Положения диссертационного исследования содержат научно обоснованные авторские предложения по решению проблем квалификации преступлений, совершаемых в киберпространстве; криминологический портрет личности экономического киберпреступника и личность потерпевшего; разработанные автором эффективные правовые и организационно-технические меры противодействия экономической киберпреступности.

Практическая значимость полученных результатов.

Практическая значимость диссертационного исследования заключается в том, что полученные результаты внедрены в работу федеральных районных судов и органов прокуратуры города Тамбова при проведении занятий и семинаров по повышению квалификации сотрудников, о чём составлены соответствующие акты о внедрении.

Результаты исследования также реализованы в учебном процессе ФГБОУ ВО «Российский государственный университет правосудия» при преподавании дисциплин «Уголовное право» и «Криминология», в учебно-

методической работе, связанной с подготовкой учебников, учебных и практических пособий, методических рекомендаций и т.п. Основные выводы и предложения отражены в монографии и восьми научных статьях, три из которых опубликованы в рецензируемых изданиях.

Основные положения, выносимые на защиту.

1. Диссертантом определено понятие киберпреступления как преступления, причиняющего вред разнородным общественным отношениям, совершаемого дистанционно, путём использования средств компьютерной техники, информационно-телекоммуникационных сетей и образованного ими киберпространства.

2. Автором дана классификация экономических киберпреступлений в зависимости от способа их 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).

3. Автором предлагается положение о том, что криптовалюта, как цифровой информационный продукт, то есть совокупность уникальных компьютерных данных, объединённых в виртуальный носитель, обладающих всеми признаками товара, собственной стоимостью и принадлежащих на праве собственности другому лицу, может выступать предметом хищения в преступлениях, предусмотренных статьями 159, 159.6 и 160 УК РФ.

4. Диссертантом определены основные детерминанты экономической киберпреступности:

- возможность извлечения в киберпространстве крупного дохода при минимальных затратах и невысоком риске, будь то незаконное Интернет-предпринимательство, легализация (отмывание) денежных средств, полученных преступным путём, либо мошенничество;

- низкий уровень осведомлённости в области информационной безопасности у пользователей систем Интернет-банкинга (дистанционного банковского обслуживания) и пользователей Онлайн-кошельков, в частности, у мобильных пользователей данных систем.

- анонимность пользователей глобальной информационной сети «Интернет», существование иных анонимных информационно-телекоммуникационных сетей, таких как «TOP», анонимность финансовых операций, проходящих в информационно-телекоммуникационных сетях;

- наличие программных уязвимостей разного уровня во всех экономически значимых информационных системах глобальной сети «Интернет», позволяющих нейтрализовать систему защиты, используя вирусы и иные вредоносные программы.

5. Автором составлен криминологический портрет лица, совершающего экономические преступления в киберпространстве: это мужчина, средний возраст 24 года, ранее не судимый, не состоящий в браке, не имеющий постоянного места работы, житель крупного города с развитой информационно-телекоммуникационной инфраструктурой, образованный, выпускник или учащийся высшего учебного заведения, имеющий высокий навык работы с компьютерной техникой, информационно-телекоммуникационными сетями и (или) вредоносным программным обеспечением, осознающий противоправность своих действий и движимый корыстными побуждениями.

6. Диссертантом дана типологизация экономических киберпреступников:

- первый тип (традиционные киберпреступники), т.е. лица, совершающие традиционные преступления (мошенничество, присвоение, растрату, вымогательство, незаконное использование товарного знака и другие) с использованием общедоступных ресурсов и возможностей киберпространства (т.е. электронная почта или социальные сети);

- второй тип (хакеры), т.е. лица, совершающие экономические киберпреступления (мошенничество в сфере компьютерной информации, незаконное собирание сведений, составляющих коммерческую, налоговую либо банковскую тайну, и другие) посредством неправомерного доступа к компьютерной информации либо с использованием вредоносного программного обеспечения в киберпространстве (вирусов, троянских программ, DDoS-программ и т.д.).

7. Автором составлен криминологический портрет жертвы киберпреступников: это лицо, как мужского, так и женского пола, в возрасте от 18 до 34 лет, доверчивое, являющееся активным пользователем социальных сетей, электронной почты, электронных кошельков и (или) систем дистанционного банковского обслуживания, с низкой культурой информационной безопасности, как правило, пользователь мобильных устройств, пренебрегающий средствами компьютерной защиты либо использующий контрафактные средства защиты.

8. На основе результатов исследования диссертантом разработан комплекс мер противодействия экономическим преступлениям, совершаемым в киберпространстве, включающий в себя меры уголовно-правового характера (положения о внесении изменений и дополнений в уголовное законодательство) и криминологического характера (организационные и технические меры).

Апробация результатов диссертационной работы. Результаты диссертационного исследования были внедрены в работу районных и областных судов Российской Федерации и работу органов Прокуратуры Российской Федерации. Результаты исследования используются в учебном процесс в Российском государственном университете правосудия при чтении дисциплин «Уголовное право» и «Криминология», а также в учебно-методической работе при подготовке методических материалов по указанным дисциплинам. Результаты диссертационного исследования реализуются при проведении занятий на факультетах повышения квалификации судей.

Положения диссертационного исследования прошли апробацию на VI и V Научно-практической конференции аспирантов и соискателей РАП «Общетеоретические и отраслевые проблемы российского правосудия» (Москва, 19 марта 2013 г. и 13 марта 2014 г. соответственно); на Международной научно-практической конференции "Преступления в информационной сфере: проблемы расследования, квалификации, реализации ответственности и предупреждения" (Тамбов, 14-15 февраля 2013 г.); на «круглом столе» факультета повышения квалификации и переподготовки судей, государственных гражданских служащих судов общей юрисдикции и Судебного департамента (Москва, 14 февраля и 18 февраля 2014 г., 30 сентября 2015 г.); на национальных форумах информационной безопасности «Инфофорум-2013» (Москва, 5-6 февраля 2013 г.), «Инфофорум-2014» (Москва, 30-31 января 2014 г.) и «Инфофорум-2015» (Москва, 5-6 февраля 2015 г.); на I и II Всероссийской научно-практической конференции «Актуальные проблемы теории и практики применения уголовного закона» (Москва, РАП, 26 апреля 2013г., и Москва, РГУП, 22 октября 2014 г. соответственно); на семинаре мировых судей и судей районных (городских) судов Тамбовской области (Тамбов, 26 сентября 2014 г.), а также в девяти публикациях по теме исследования, в том числе в форме монографии.

Структура работы состоит из введения, трёх глав (девяти параграфов), заключения, списка использованной литературы и приложений.

ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

Во **введении** обосновывается актуальность темы исследования, формулируются его цели и задачи, определяется объект и предмет, характеризуются нормативные, теоретические и эмпирические источники исследования, конструируются положения, выносимые на защиту, приводятся сведения об апробации исследования, теоретической и практической значимости.

Глава 1 «Понятие и признаки киберпространства и экономических киберпреступлений» состоит из трёх параграфов.

В первом параграфе «Понятие и общая характеристика киберпространства» проведён историко-правовой анализ и исследовано современное состояние такого явления, как киберпреступность, теоретически обосновано понятие киберпространства.

Выделено два исторических этапа развития киберпространства и киберпреступности: первый этап с 1960 по 1991 гг. и второй этап с 1991 г. по настоящее время. Этапы соотносятся с началом массового внедрения персональных компьютеров в жизнь общества и с появлением глобальных информационно-телекоммуникационных сетей.

Дано определение киберпространства, под которым понимается сфера деятельности в информационном пространстве, образованная совокупностью коммуникационных каналов сети «Интернет» и других телекоммуникационных сетей, технологической инфраструктуры, обеспечивающей их функционирование, и любых форм осуществляемой посредством их использования человеческой активности (личности, организации, государства).

Автором проведено разграничение понятий «киберпространство» и «Интернет». Отмечено, что киберпространство – это искусственно созданная среда, существование которой ограничено информационно-телекоммуникационной сетью. Сеть «Интернет» – это материальное отражение

киберпространства в реальном мире: это не само «киберпространство», а лишь техническое условие, в котором оно может существовать.

В конце параграфа автор делает вывод, что с появлением новых технологий (киберпространства) наблюдается появление нового, более сложного вида преступности (киберпреступности). Это свидетельствует о том, что преступники достаточно оперативно используют результаты научно-технического прогресса в своих целях. Данная тенденция представляет серьёзную угрозу всем общественным отношениям, складывающимся в киберпространстве, поскольку на данном этапе развития киберпространство и общество уже неотделимы.

Во втором параграфе «Понятие и общественная опасность киберпреступления» теоретически обосновывается понятие киберпреступления, дана классификация экономических киберпреступлений и определяется место киберпреступлений, как в общей системе преступлений, так и в системе экономических преступлений, даются рекомендации по совершенствованию отечественного уголовного законодательства.

Дано разграничение понятий «киберпреступление», «компьютерное преступление» и «преступление в сфере компьютерной информации». Автор приходит к выводу, что под киберпреступлением следует понимать преступление, причиняющее вред разнородным общественным отношениям, совершаемое дистанционно, путём использования средств компьютерной техники и информационно-телекоммуникационных сетей и образованного ими киберпространства. Также выделено два самостоятельных вида экономических киберпреступлений:

- экономические киберпреступления, совершаемые путём психологического воздействия на человека (обман, введение в заблуждение, угрозы), такие как мошенничество, вымогательство, причинение имущественного ущерба путём обмана или злоупотребления доверием, принуждение к совершению сделки либо отказу от её совершения и другие;

- экономические киберпреступления, совершаемые путём воздействия на оборудование (компьютеры, смартфоны, маршрутизаторы и иное оборудование), такие как мошенничество в сфере компьютерной информации, собирание сведений, составляющих коммерческую, банковскую либо налоговую тайну.

Анализируя характер и степень общественной опасности киберпреступления, автор замечает, что экономические киберпреступления обладают двухобъектной природой, а ущерб от киберпреступлений невероятно высок.

В конце параграфа автор приходит к выводу, что преступления, совершаемые в киберпространстве, обладают большей степенью общественной опасности, нежели преступления, совершаемые без использования последнего. Автор научно обосновал предложение по дополнению уголовно-правовых норм об обстоятельствах, отягчающих наказание, в частности, предложил дополнить часть 1 статьи 63 УК РФ новым пунктом:

«с) совершение преступления дистанционно с использованием средств компьютерной техники, информационно-телекоммуникационных сетей и киберпространства».

Одновременно дополнить статью 63 УК РФ новой частью:

«1.2. Судья (суд), назначающий наказание, в зависимости от характера и степени общественной опасности преступления, обстоятельств его совершения и личности виновного, может не признать отягчающим обстоятельством совершение преступления с использованием средств компьютерной техники, информационно-телекоммуникационных сетей и киберпространства».

В третьем параграфе «Международный опыт в сфере противодействия экономическим преступлениям, совершаемым в киберпространстве» проведено сравнительно-правовое исследование уголовного законодательства разных стран в области противодействия экономическим киберпреступлениям, исследование национальных стратегий кибербезопасности разных стран, а

также проведено историко-правовое исследование основных международных актов в области противодействия киберпреступности.

С целью выявления положительных моментов, которые могут быть использованы в российском законодательстве, проведён анализ национальных стратегий Германии, Великобритании, Канады, Литвы, Люксембурга, Нидерландов, Словакии, США, Чешской Республики, Эстонии и Японии. Выявлены основные направления государственной политики по борьбе с киберпреступлениями.

Сравнив уголовное законодательство о противодействии экономическим киберпреступлениям Австрии, Белоруссии, Дании, Испании, Италии, КНР, Нидерландов, Польши, США, Украины, Финляндии, ФРГ, Швейцарии, Эстонии, Южной Кореи и Японии с отечественным, автор отмечает, что уголовное законодательство разных стран об экономических киберпреступлениях имеет множество особенностей и отличий, однако существуют нормы, встречающиеся в уголовных кодексах почти всех стран. К ним автор отнёс: 1) компьютерное мошенничество или компьютерное хищение; 2) получение сведений, составляющих коммерческую тайну, путём неправомерного доступа к компьютерной информации (коммерческий шпионаж); 3) вымогательство с использованием средств компьютерной техники.

В целом содержание данного параграфа позволяет сделать вывод, что эффективным решением для уголовного законодательства Российской Федерации станет его совершенствование, расширяющее понятия «хищение», «вымогательство», а также учитывающее использование средств компьютерной техники в качестве обстоятельства, отягчающего наказание.

Глава 2 «Уголовно-правовая характеристика экономических преступлений, совершаемых в киберпространстве» состоит из трёх параграфов.

В первом параграфе «Общая характеристика экономических преступлений, совершаемых в киберпространстве» исследована социально-

правовая специфика экономических отношений, которые подвержены посягательствам в киберпространстве, исследованы специфические признаки предмета экономических киберпреступлений, также теоретически обосновано значение киберпространства как признака составов киберпреступлений. Исследован вопрос места совершения киберпреступления.

В параграфе обобщена практика применения норм об уголовной ответственности за киберпреступления в сфере экономики, выявлены её основные тенденции, на основании чего предложен научный прогноз дальнейшего развития практики.

Самостоятельно исследован вопрос о признании криптовалюты предметом хищения. Проведено разграничение криптовалюты от безналичных и электронных денежных средств, от бездокументарных ценных бумаг и простой компьютерной информации (объекта авторских прав). Особо указано, что, приобретая криптовалюту за реальные деньги, покупатель приобретает уникальную индивидуально определённую вещь, имеющую коммерческую ценность, то есть товар.

Обоснован вывод, что криптовалюта, как цифровой информационный продукт, то есть совокупность уникальных компьютерных данных, объединённых в виртуальный носитель, обладающих всеми признаками товара, собственной стоимостью и принадлежащих на праве собственности другому лицу, может выступать предметом хищения в преступлениях, предусмотренных статьями 159, 159.6 и 160 УК РФ.

Исследуя особенности субъективной стороны экономических киберпреступлений, делается вывод, что подавляющее число экономических киберпреступлений совершаются из корыстной заинтересованности.

В целом содержание параграфа позволяет выделить основные особенности экономических преступлений, совершаемых в киберпространстве.

Во втором параграфе «Преступления против собственности, совершаемые в киберпространстве» исследованы составы преступлений против собственности, совершаемых в киберпространстве, с целью выявления их

специфических признаков, даны научно обоснованные рекомендации по совершенствованию отечественного уголовного законодательства, а также рекомендации правоприменительного характера.

Исследуя хищение чужого имущества или приобретение права на чужое имущество путем ввода, удаления, блокирования, модификации компьютерной информации, делается вывод, что деяние, предусмотренное в диспозиции статьи 159.6 УК РФ, является новой самостоятельной формой хищения. Научно обосновано предложение по редакции уголовно-правовой нормы, содержащейся в статье 159.6 УК РФ.

Статья 159.6. Хищение в сфере компьютерной информации

Хищение в сфере компьютерной информации, то есть хищение чужого имущества или приобретение права на чужое имущество путем ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей.

Исследуя вымогательство в киберпространстве, делается вывод, что вымогательство, совершенное под угрозой применения DDoS-атаки, выходит за пределы статьи 163 УК РФ и не может быть квалифицировано по совокупности ни со статьёй 272 УК РФ, ни со статьёй 273 УК РФ.

Научно обосновано предложение по дополнению уголовно-правовой нормы, содержащейся в статье 163 УК РФ, новым характером угрозы.

Статья 163. Вымогательство

1. Вымогательство, то есть требование передачи чужого имущества или права на имущество или совершения других действий имущественного характера, совершенное:

а) под угрозой применения насилия либо уничтожения или повреждения чужого имущества;

б) под угрозой распространения сведений, позорящих потерпевшего или его близких, либо иных сведений, которые могут причинить существенный вред правам или законным интересам потерпевшего или его близких;

в) под угрозой удаления, блокирования либо модификации компьютерной информации, а равно под угрозой иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей, которое может причинить существенный вред правам или законным интересам потерпевшего или его близких.

Исследуя причинение имущественного ущерба путём обмана или злоупотребления доверием, делается вывод, что причинение имущественного ущерба путём вмешательства в информационно-телекоммуникационную сеть является самостоятельным преступлением против собственности. Обосновывается необходимость принятие новой нормы – статьи 165.1 УК РФ «Причинение имущественного ущерба в сфере компьютерной информации».

Статья 165.1 Причинения имущественного ущерба в сфере компьютерной информации

1. Причинение имущественного ущерба собственнику или иному владельцу имущества при отсутствии признаков хищения, совершённое путём ввода, удаления, блокирования, модификации компьютерной информации либо путём иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей, в крупном размере

наказывается…

2. То же деяние, совершенное с использованием вредоносных компьютерных программ,

наказывается…

3. Деяние, предусмотренное частями первой или второй настоящей статьи, совершенное группой лиц по предварительному сговору, организованной группой либо в особо крупном размере,

наказывается…

Одновременно с введением данной нормы научно обосновывается необходимость признать утратившими силу части 2 статьи 272 и части 2 статьи 273 УК РФ. Автор указывает, что это позволит избежать проблем квалификации таких деяний и положительно повлияет на систему отечественного уголовного законодательства.

В параграфе также исследованы способы и особенности совершения в киберпространстве таких преступлений против собственности, как мошенничество (ст. 159 УК РФ) и умышленное уничтожение или повреждение чужого имущества (ст. 167 УК РФ). В конце параграфа даны уголовно-правовые и правоприменительные меры противодействия преступлениям против собственности, совершаемым в киберпространстве.

В третьем параграфе «Преступления в сфере экономической деятельности, совершаемые в киберпространстве» исследованы составы преступлений в сфере экономической деятельности, совершаемых в киберпространстве, с целью выявления их специфических признаков. Даны научно обоснованные рекомендации по совершенствованию отечественного уголовного законодательства, а также рекомендации правоприменительного характера.

Исследуя состав принуждения к совершению сделки или к отказу от её совершения, делается вывод, что, как и в случае с вымогательством, угроза уничтожения, блокирования либо модификации компьютерной информации выходит за пределы объективной стороны преступления, указанного в статье 179 УК РФ. Дополнительная квалификация по совокупности со статьями 272 или 273 УК РФ не решает проблему квалификации. Научно обосновано предложение по дополнению уголовно-правовой нормы, содержащейся в статье 179 УК РФ, новым характером угрозы.

Статья 179. Принуждение к совершению сделки или к отказу от ее совершения

1. Принуждение к совершению сделки или к отказу от ее совершения, при отсутствии признаков вымогательства:

а) под угрозой применения насилия, уничтожения или повреждения чужого имущества;

б) под угрозой распространения сведений, которые могут причинить существенный вред правам и законным интересам потерпевшего или его близких;

в) под угрозой удаления, блокирования либо модификации компьютерной информации, а равно под угрозой иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей, которое может причинить существенный вред правам или законным интересам потерпевшего или его близких.

В параграфе также исследованы способы и особенности совершения в киберпространстве преступлений в сфере экономической деятельности, предусмотренных статьями 170.1, 171, 171.2, 172, 174, 174.1, 176, 180, 183, 185.3, 185.6, 193.1, 193.2, 197, 198 и 199 УК РФ. В конце параграфа даны уголовно-правовые и правоприменительные меры противодействия преступлениям в сфере экономической деятельности, совершаемым в киберпространстве.

Глава 3 «Криминологическая характеристика экономических преступлений, совершаемых в киберпространстве» состоит из трёх параграфов.

В первом параграфе «Причины и условия совершения экономических киберпреступлений» с использованием криминологической методологии определены конкретные детерминанты экономической киберпреступности и выявляется уровень её латентности.

Делается вывод, что основным социально-экономическим условием экономической киберпреступности является возможность извлечения в киберпространстве крупного дохода при минимальных затратах и невысоком риске. При этом важным условием экономической киберпреступности, как и всей киберпреступности в целом, также является низкий уровень

осведомлённости в области информационной безопасности у пользователей систем Интернет-банкига (дистанционного банковского обслуживания) и пользователей Онлайн-кошельков, в частности, у мобильных пользователей данных систем.

Основными техническими условиями экономической киберпреступности автором названы: анонимность пользователей глобальной информационной сети «Интернет», существование иных анонимных информационно-телекоммуникационных сетей, таких как «TOP», анонимность финансовых операций, проходящих в информационно-телекоммуникационных сетях; наличие программных уязвимостей разного уровня практически во всех экономически значимых информационных системах глобальной сети «Интернет», позволяющих нейтрализовать систему защиты, используя вирусы и иные вредоносные программы.

Далее исследован уровень латентности экономических преступлений, совершаемых в киберпространстве, на примере самого распространённого киберпреступления – мошенничества – по данным официальной статистики МВД, Банка России, а также по статистике международной компании по предотвращению и расследованию киберпреступлений и мошенничеств «Group-IB» за 2012 год. Делается вывод о невероятно высоком уровне латентности экономических преступлений, совершаемых в киберпространстве, который составляет от 74,2% до 83,58%.

В целом положения параграфа позволяют сделать вывод об основных детерминантах экономической киберпреступности и уровне её латентности.

Во втором параграфе «Личность киберпреступника и его жертвы» на основе эмпирического материала сформулирован криминологический портрет киберпреступника и портрет его жертвы, дана классификация и типологизация киберпреступников, определены наиболее виктимные группы населения.

В результате исследования 100 уголовных дел об экономических преступлениях, совершённых в киберпространстве, автор составил

криминологический портрет лица, совершающего экономические преступления в киберпространстве. Это:

мужчина, средний возраст 24 года, ранее не судимый, не состоящий в браке, не имеющий постоянного места работы, житель крупного города, с развитой информационно-телекоммуникационной инфраструктурой, образованный, выпускник или учащийся высшего учебного заведения, имеющий высокий навык работы с компьютерной техникой, информационно-телекоммуникационными сетями и (или) вредоносным программным обеспечением, осознающий противоправность своих действий и движимый корыстными побуждениями.

Выделено два основных типа киберпреступников:

– первый тип – традиционные киберпреступники, т.е. лица, совершающие традиционные преступления (мошенничество, присвоение, растрату, вымогательство, незаконное использование товарного знака и другие) с использованием общедоступных ресурсов и возможностей киберпространства (таких как электронная почта или социальные сети);

– второй тип – хакеры, т.е. лица, совершающие экономические киберпреступления (мошенничество в сфере компьютерной информации, незаконное собирание сведений составляющих коммерческую, налоговую либо банковскую тайну и другие) посредством неправомерного доступа к компьютерной информации либо с использованием вредоносного программного обеспечения в киберпространстве (вирусов, троянских программ, DDoS-программ и т.д.).

Проведён анализ личности жертвы экономических киберпреступлений на основе статистических данных о возрасте, поле, образовании, уровне осведомлённости об информационной безопасности и характере поведения в киберпространстве.

Составлен криминологический портрет жертвы экономического киберпреступника: лица не зависимо от пола, в возрасте от 18 до 34 лет, доверчивые, являющиеся активными пользователями электронных кошельков и

(или) систем дистанционного банковского обслуживания (Онлайн-банкинга), с низкой культурой информационной безопасности, как правило, пользователи мобильных устройств, пренебрегающие средствам компьютерной защиты (антивирусами) либо использующие контрафактные средства защиты.

В третьем параграфе «Правовые и криминологические меры противодействия экономическим преступлениям, совершаемым с использованием киберпространства в России» выработаны научно обоснованные рекомендации по совершенствованию правовых и организационных мер противодействия экономическим преступлениям, совершаемым в киберпространстве, рекомендации по совершенствованию действующего уголовного законодательства в части охраны прав и интересов пользователя киберпространства, а также рекомендации по практике его применения.

Автором отмечено, что по способу противодействия меры противодействия экономическим киберпреступлениям следует разделить на две основные группы: правовые и криминологические. Последние разделены на организационные и технические меры.

В качестве правовых мер предлагается совершенствование отечественного уголовного законодательства, включающее как оговорённые выше редакции статей 63, 159.6, 163, 165.1 и 179 УК РФ, так и новые предложения. В целях противодействия субкультуре хакеров, а также рынку вредоносного программного обеспечения научно обосновывается предложение по дополнению статьи 273 УК РФ новой нормой:

«2.1. Сбыт компьютерных программ либо иной компьютерной информации, заведомо предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации».

В качестве мер организационного характера разработаны предложения по принятию Национальной Стратегии Кибербезопасности Российской Федерации; разработан комплекс предложений по дополнению Постановлений

Пленума Верховного Суда Российской Федерации «О судебной практике по делам о мошенничестве, присвоении и растрате», «О судебной практике по делам о вымогательстве», «О судебной практике по делам о незаконном предпринимательстве и легализации (отмывании) денежных средств или иного имущества, приобретенных преступным путем»; предложена концепция Постановления Пленума Верховного Суда Российской Федерации «О судебной практике по делам о компьютерных преступлениях»; также предложен комплекс профилактических мер противодействия экономическим преступлениям, совершаемым в киберпространстве.

В качестве организационно-технических меры предложена система персонализации пользователей информационных ресурсов в киберпространстве, основанная на биометрических особенностях пользователя цифрового устройства (сканер отпечатков пальцев, сканер лица).

В **заключении** подведены итоги исследования, сформулированы основные выводы и рекомендации.

Основные положения диссертационного исследования опубликованы в следующих работах автора:

I. В рецензируемых научных изданиях, рекомендованных Высшей аттестационной комиссией при Министерстве образования и науки Российской Федерации:

1. Простосердов, М.А. Легализация (отмывание) денежных средств в киберпространстве / М.А. Простосердов // Российское правосудие. – 2014. – № 9 (101) – С. 75-80 (0,25 п. л).

2. Простосердов, М.А. Вымогательство, совершенное в сети Интернет / М.А. Простосердов // Библиотека криминалиста. Научный журнал. – 2013. − №6 − С. 150-152. (0,25 п. л.).

3. Простосердов, М.А. Проблемы квалификации компьютерных преступлений / М.А. Простосердов // Российское правосудие. – 2012. − № 6 (74). – С. 106-108 (0,25 п. л).

II. В иных научных изданиях:

4. Простосердов, М.А. Мошенничество, совершаемое в киберпространстве, и его виды / М.А. Простосердов // Актуальные проблемы теории и практики применения уголовного закона: Сборник материалов Научно-практической конференции (22 октября 2014 года) / Под ред. А.В. Бриллиантова и Ю.Е. Пудовочкина. − М.: РГУП, 2015. – С. 334-351. (1,25 п. л.).

5. Простосердов, М.А. Экономические преступления, совершаемые в киберпространстве, и меры противодействия им / М.А. Простосердов // Судебные известия. Информационный бюллетень Управления Судебного департамента в Тамбовской области. – 2014. − №15(2) – С. 49-53. (0,3 п. л).

6. Простосердов, М.А. Сравнительный анализ зарубежного законодательства в сфере противодействия виртуальным преступлениям / М.А. Простосердов // Актуальные проблемы уголовного права и криминологии: Сборник научных трудов кафедры уголовного права. Вып.4 / Под ред. А.В. Бриллиантова. − М.: РАП, 2014. − С. 133-153 (1,25 п. л.).

7. Простосердов, М.А. Преступления, совершаемые в информационном пространстве стран ЕврАзЭС // Информационное пространство ЕврАзЭС: правовые основы интеграции: монография / А.А. Арямов, И.В. Афанасьева, И.Л. Бурова, С.П.Гаврилов, Ш.Х. Заман, Л.В. Каткова, Д.Г. Коровяковский, С.В. Лобачев, А.В. Никитова, М.А. Простосердов, Н.Н. Телешина, Е.А. Шарафутдинов, Н.Н. Штыкова; под ред. Н.Н. Лебедевой, А.В. Никитовой. − М.: РГУИТП, 2013. – С. 144-162 (авт. 1,18 п. л.).

8. Простосердов, М.А. Виртуальное пространство: криминологические проблемы и общественная опасность преступлений, совершенных в сети Интернет / М.А. Простосердов // Преступления в информационной сфере: проблемы расследования, квалификации, реализации ответственности и предупреждения: материалы Международной научно-практической конференции 14-15 февраля 2013 г. / М-во обр. и науки РФ, ФГБОУ ВПО «Тамб.гос. ун-т им. Г.Р. Державина»; ред. кол.: А.В. Шуняева, Е.А. Попова, С.А. Пучнина. − Тамбов: Издательский дом ТГУ имени Г. Р. Державина, 2013. – С. 64-69 (0,25 п. л.).

9. Простосердов, М.А. К вопросу об оценке общественной опасности преступлений, совершаемых в сети Интернет / М.А. Простосердов // Актуальные проблемы уголовного права и криминологии: Сборник научных трудов кафедры уголовного права. Вып. 3 / Под ред. Ю.Е. Пудовочкина и А.В. Бриллиантова. − М.: РАП, 2013. – С. 198-209 (0,5 п. л.).