Простосердов Михаил Александрович. Экономические преступления, совершаемые в киберпространстве, и меры противодействия им: диссертация ... кандидата Юридических наук: 12.00.08 / Простосердов Михаил Александрович;[Место защиты: Российский государственный университет правосудия].- Москва, 2016.- 232 с.

**Содержание к диссертации**

Введение

**Глава 1. Понятие и признаки киберпространства и экономических киберпреступлений**

1. Понятие и общая характеристика киберпространства 14

2. Понятие и общественная опасность киберпреступления 24

3. Международный опыт в сфере противодействия экономическим преступлениям, совершаемым в киберпространстве 39

**Глава 2. Уголовно-правовая характеристика экономических преступлений, совершаемых в киберпространстве**

1. Общая характеристика экономических преступлений, совершаемых в киберпространстве 58

2. Преступления против собственности, совершаемые в киберпространстве 77

3. Преступления в сфере экономической деятельности, совершаемые в киберпространстве 107

**Глава 3. Криминологическая характеристика экономических преступлений, совершаемых в киберпространстве**

1. Причины и условия экономической киберпреступности 140

2. Личность киберпреступника и его жертвы 157

3. Правовые и криминологические меры противодействия экономическим преступлениям, совершаемым в киберпространстве России 172

Заключение 190

Список использованной литературы

**Введение к работе**

**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 «ТОР», 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.

1. 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.
2. 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.).

1. 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.
2. 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.

## Понятие и общественная опасность киберпреступления

Поэтому для единообразия терминологии и в связи с тематикой исследования в данной работе будут использованы такие термины, как «киберпространство», «киберпреступность» и «киберпреступление».1

Массовое распространение компьютеров и появление информационных сетей спровоцировало появление нового вида преступности - киберпреступность, историю становления которой в России и мире можно условно разделить на два этапа: до и после появления глобальной информационной сети «Интернет», которая и породила киберпространство в привычном нам виде.

Первый этап (1960-1991 гг.). В 1960-х годах в США компьютеры использовались лишь некоторыми государственными органами из-за огромной их стоимости. Компьютерные преступления 1960-х годов были единичными и заключались в неправомерном доступе к компьютерной информации и персональным данным, их модификации либо удалении, а из-за неточного и неполного законодательного регулирования и отсутствия способов получения доказательственной базы большинство дел разваливалось2.

«Компьютерный бум» и, как следствие, появление новых видов киберпреступности, произошел в конце 1970-х – начале 1980-х годов в США с появлением первых персональных компьютеров IBM 5100 и Apple I, а также с появлением прародителя сети «Интернет» – «Арпанет».

В 1975 году Агентство передовых исследований Министерства обороны США (Advanced Research Agency - ARPA) совместно со Стенфордским и Калифорнийским университетами запустили в рабочем режиме первую информационно-телекоммуникационную сеть «Арпанет» (англ. «Arpanet»), использующую протокол передачи данных TCP/IP, который в настоящее время используется в сети «Интернет»1. В то же время массово проявились случаи преступлений, совершённых с использованием компьютеров и сети «Арпанет»2.

Государство отреагировало на новую угрозу только спустя два года. В 1977 году был одобрен первый законопроект «О защите федеральных компьютерных систем», на основе которого в 1986 году был принят Закон №1030 «О мошенничестве и злоупотреблениях с использованием компьютера»3.

Первые локальные компьютерные сети в СССР появились также в конце 1970-х - начале 1980-х гг. Они представляли собой высокотехнологичные и инновационные, но все же разрозненные компьютерные системы. Первое преступление с использованием компьютера в СССР было зарегистрировано в 1979 году в Вильнюсе, им стало хищение 78 584 рублей. Данное преступление было занесено в международный реестр правонарушений и является отправной точкой в развитии компьютерных преступлений в СССР и России4. В 1983 году было зафиксировано причинение имущественного ущерба уже в 1 млн. рублей посредством модификации программы для ЭВМ в г. Тольятт..5

В начале 1980-х в США появилась информационно-телекоммуникационная сеть «Милнет» («Milnet», Military Network - военная сеть), которая использовалась лишь Министерством обороны США. Спустя некоторое время «Арпанет» и часть «Милнет» были интегрированы, а для их общего обозначения было придумано специальное название «Интернет» (англ. «Internet»). Сеть «Интернет» в этот период времени была сравнительно небольшой и не являлась «глобальной информационной сетью», поэтому конкурировала с другими информационными сетями. В то же время появились такие сети, как «NSFNet» («Информационно телекоммуникационная сеть Национального научного фонда США») и «USEnet» («Пользовательская сеть»). Количество подключаемых пользователей ко всем компьютерным сетям достигло 10 000 человек в год1, а занятие «хакерством» стало популярным в обществе. Отчасти этому поспособствовали кинематограф и научно-фантастические романы: к середине 80-х на большой экран вышло множество фильмов о хакерах («Трон» 1982 г., «Военные игры» 1983 г., «Настоящий гений» 1985 г. и др.)2, а в 1984 году вышел роман Уильяма Гибсона «Нейромант», описавший идею киберпространства.

В результате последовал всплеск киберпреступности. Как отмечает Т.Л. Тропина, в этот период времени произошло ограбление «Security Pacific Bank» (10.2 млн. долл), появился первый в мире компьютерный вирус (1984 г.) и было совершено причинение имущественного ущерба в 1,2 млн. долл. компании ВВС «Robbins» 17-летним хакером (1987 г.)3.

О «Всепланетной компьютерной сети» в СССР заговорили в конце 1980-х годов. Так, компьютеры «Всесоюзного НИИ прикладных автоматизированных систем» в 1988-1989 годах имели свободный доступ к национальной сети ЭВМ всех соцстран, а также Австрии и Финляндии. В экспериментальном режиме шла передача данных с компьютерами из Кубы и США4.

Конец 1980-х годов также связан с глобализацией информационных сетей. «Европейский совет по ядерным исследованиям» (ЦЕРН) в 1989 году предложил идею «Всемирной паутины», использующей протокол передачи данных HTTP, то есть гипертекст (ссылки). К данному времени сложились все технические условия для появления киберпространства.

Второй период (1991 г. - по наше время). В 1991 году «Интернет» стал мировой информационной сетью, а это значит, что хакеры разных стран получили возможность беспрепятственно совершать преступления по всему миру, а компьютерная преступность приобрела трансграничный признак. В 1990 году на базе Института атомной энергии им. И. В. Курчатова была разработана отечественная компьютерная сеть «Релком», (англ. Russian Electronic Communication Network), в то же время появляется доменное имя «.su» (англ. Soviet Union)1. В 1994 году было зарегистрировано доменное имя «.ru» и тогда же появился «Рунет» (Национальный сегмент сети «Интернет» Российской Федерации).

В 1990-х в России стало уделяться особое внимание преступлениям, совершаемым с использованием средств компьютерной техники и информационно-телекоммуникационных сетей. В 1992 году прошел первый межведомственный семинар для сотрудников Министерства внутренних дел Российской Федерации «Криминалистика и компьютерная преступность»2, а в 1996 году был принят новый Уголовный кодекс Российской Федерации, который включал Главу 28 «Преступления в сфере компьютерной информации».

В 1995 году появился первый Интернет-магазин «Amazon»3, в тот же год появилась первая социальная сеть «Classmates»4 и первый виртуальный банк «Security First Network Bank»5. На наш взгляд, киберпространство в том виде, что мы сегодня наблюдаем, появилось именно в этот период времени. Спустя год Верховный Суд США впервые дал легальное определение киберпространству6.

## Международный опыт в сфере противодействия экономическим преступлениям, совершаемым в киберпространстве

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.2 Ещё одной трудностью при квалификации «мошенничества» в сфере компьютерной информации является смешение данного понятия с «хищением» персональных данных, таких как логины и пароли, номера кредитных карт, совершенных путём обмана или злоупотребления доверием. Так, М.А. Мутасова выделяет следующие виды «хищений» персональных данных: «фишинг», «вишинг» и «фарминг»3.

Фишинг (англ. phishing, от fishing – рыбалка) заключается в хищении личных конфиденциальных данных, таких как пароли доступа, логины, данные банковских и идентификационных карт, с помощью СПАМа, посылаемого по электронной почте («почтовый фишинг»), по переписке в социальной сети или на других сайтах («онлайновый фишинг») или использующий оба способа («комбинированный фишинг»).

Вишинг (англ. voice phishing – голосовой фишинг) – использование автонабирателей и/или возможностей Интернет-телефонии для хищения персональных данных о логинах и паролях.

Фарминг (англ. pharming, от farming – фермерство) – нарушение навигационной структуры браузера с целью скрытного перенаправления жертвы на ложный IP-адрес для завладения её персональными данными о логинах и паролях. Согласно статистическим данным компании «Group-IB» в 2013 году было зафиксировано более 1000 обращений, связанных с российскими «фишинговыми сайтами»1.

Данные деяния нередко называются «компьютерным мошенничеством», поскольку они совершаются обманным путём с использованием средств компьютерной техники. Однако все эти деяния заключаются лишь в получении информации о логинах и паролях к аккаунтам Интернет-банков или виртуальных кошельков. Обман в данном случае – это способ получения персональных данных, а не имущества. Другими словами, предметом «фишинга», «вишинга» и «фарминга» является информация, а предметом мошенничества – чужое имущество. В связи с этим подобные деяния, на наш взгляд, следует квалифицировать как неправомерный доступ к компьютерной информации, повлекший её копирование (ст. 272 УК РФ). В случае если после получения логина и пароля обманным путем виновный введёт их в систему и осуществит хищение денежных средств, то такое деяние перерастает в мошенничество в сфере компьютерной информации, и его необходимо будет квалифицировать только по статье 159.6 УК РФ.

«Мошенничество» в сфере компьютерной информации следует отличать от присвоения и растраты (ст. 160 УК РФ). Основное отличие между этими двумя формами хищения заключается в том, что при присвоении или растрате совершается хищение вверенного имущества1. Представляется, что хищение вверенного имущества путём ввода компьютерной информации также возможно, например, сотрудником коммерческой организации, которому были вверены электронные денежные средства. В таком случае содеянное необходимо квалифицировать по статье 160 УК РФ, поскольку похищенное имущество было вверенным.

Так, в августе 2013 года А., являясь пользователем социальной сети «Одноклассники», имея профиль под ником «Интернет-магазин Престиж», получила от Б. на систему «QIWI Кошелек» с абонентским номером 1111111 денежные средства в сумме 4004 рубля с целью приобретения товара. А. перенаправила заказ на сайт «Интернет-магазина Престиж», однако данного товара в наличии не оказалось, о чем Б. в известность не поставила. После чего А, зная, что денежные средства в сумме 4004 рубля вверены ей Б. для приобретения товара, присвоила их, переведя со своего «QIWI Кошелька» на свой лицевой счет, открытый в дополнительном офисе Сбербанка России, обратив их в свою собственность, причинив тем самым Б. значительный ущерб на сумму 4004 рубля2.

Несмотря на то, что А. совершила данное хищение путём ввода компьютерной информации (переведя деньги со счета на счет через систему QIWI), она была признана виновной в совершении преступления, предусмотренного частью 2 статьи 160 УК РФ, поскольку похищенное имущество было её вверено. Другим примером присвоения вверенного имущества путём ввода компьютерной информации является приговор Октябрьского районного суда города Пензы. Л., занимая должность главного бухгалтера ООО, вопреки законным интересам ООО, находясь в своей квартире, используя персональный компьютер, подключенный к сети «Интернет», и вверенную ей электронную подпись генерального директора ООО, содержащуюся на электронном носителе, осуществила вход в систему дистанционного банковского обслуживая ООО на сайте Сбербанка. Л. перечислила с расчетного счета ООО на свой расчетный счет вверенную ей денежную сумму в размере 7 109 200 рублей1.

Л. была признана виновной в совершении преступления, предусмотренного частью 4 статьи 160 УК РФ, ей было назначено наказание в виде лишения свободы на срок 3 года в колонии общего режима. Подводя итог по данному составу киберпреступления, можно с определённой уверенностью выделить следующие положения: 1. термин «мошенничество» применительно к составу преступления, указанному в диспозиции статьи 159.6 УК РФ, применён некорректно; 2. преступление, указанное в диспозиции статьи 159.6 УК РФ, является новой, самостоятельной формой хищения; 3. под вводом компьютерной информации, на наш взгляд, следует считать внедрение сторонней компьютерной информации, которое нарушает функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей (к примеру, вирусов или иных вредоносных программ); позволяет обойти систему защиты компьютера; открывает доступ к средствам хранения, обработки или передачи компьютерной информации;

## Преступления в сфере экономической деятельности, совершаемые в киберпространстве

С помощью них З. совершал неправомерный доступ к охраняемой законом компьютерной информации, хранящейся в чужих компьютерах, что повлекло блокирование и модификацию данной информации. Как следует из приговора, в действиях З. имела место совокупность преступлений, предусмотренных статьями 273 и 183 УК РФ, так как, применяя вредоносную программу, З. осуществил сбор сведений, составляющих коммерческую тайну, находившихся в компьютере потерпевшего Г.1

В данном случае действия виновного явно выходят за пределы статьи 183 УК РФ, которой не охватывается использование вредоносной программы, и суд правильно квалифицировал данное деяние по совокупности со статьёй 273 УК РФ.

Стоит учесть, что наименее латентным составом преступления в данной статье следует признать незаконное разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну (ч. 2 ст. 183 УК РФ).

Представляется, что незаконное распространение объективно легче совершить в киберпространстве, чем незаконное получение сведений, составляющих такую тайну. Во-первых, как указывает Б.В. Волженкин, данное преступление следует считать оконченным, если тайна стала известна хотя бы одному человеку2. Во-вторых, само киберпространство создано для распространения информации: сведения, составляющие коммерческую, налоговую или банковскую тайну, можно распространить как в социальной сети или в Интернет-газете, так и при личном общении через текстовый, аудио- или видео-чат («Skype»), по электронной почте либо любым иным возможным способом. При этом особенностью данного преступления является то, что за рекордно короткое время доступ к тайне могут получить миллионы людей, что способно причинить вред компании в миллиарды рублей.

Основываясь на вышесказанном, по данному составу киберпреступления можно сделать следующие выводы: 1. несмотря на то, что неправомерное копирование файла, содержащего коммерческую, налоговую либо банковскую тайну, нарушает сразу две группы общественных отношений (в сфере экономической деятельности и компьютерной информации), объективная сторона преступления полностью поглощается частью 1 статьи 183 УК РФ. Такие деяния следует квалифицировать по совокупности только тогда, когда помимо копирования сведений виновное лицо совершит их модификацию, уничтожение или блокирование; 3. в отличие от собирания сведений, содержащих коммерческую, налоговую либо банковскую тайну, их разглашение в киберпространстве совершить объективно легче, что связано с его возможностями по передаче компьютерной информации.

Иные экономические киберпреступления. К иным киберпреступлениям, редко совершаемым в сфере экономической деятельности, можно отнести фальсификацию Единого Государственного Реестра юридических лиц, преступления, связанные с использованием инсайдерской информации, валютные, налоговые преступления, фиктивное банкротство и коммерческий подкуп. С 31 мая 2012 года на всей территории Российской Федерации появилась возможность зарегистрировать юридическое лицо через сеть «Интернет», подав в Федеральную налоговую службу электронные документы для государственной регистрации через официальный сайт Федеральной налоговой службы, подкрепив их электронной подписью1. Следовательно, с появлением нового способа предоставления документов появился и новый способ совершения фальсификации Единого Государственного Реестра юридических лиц, Реестра владельцев ценных бумаг или системы депозитарного учета (170.1 УК РФ)1.

Объективная сторона данного преступления заключается в предоставлении в орган, осуществляющий государственную регистрацию юридических лиц и индивидуальных предпринимателей, или в организацию, осуществляющую учет прав на ценные бумаги, документов, содержащих заведомо ложные данные со специальной целью внесения определённых сведений в реестр, либо в иных целях, направленных на приобретение права на чужое имущество.

Предоставление в налоговый орган электронных документов, содержащих заведомо ложные сведения, на наш взгляд, является таким же уголовно наказуемым деянием, как и предоставление бумажных документов, содержащих ложные сведения, так как оба деяния направлены на один и тот же объект (отношения в сфере экономической деятельности) и могут привести к одинаковым последствиям – неправомерной регистрации юридического лица.

Поскольку виновный для совершения киберпреступления использовал уже существующую инфраструктуру (сайт ФНС) и не причинил вреда отношениям в сфере компьютерной информации, то квалификации по совокупности со статьёй 272 УК РФ (неправомерный доступ к компьютерной информации) в данном случае не требуется.

Однако часть 2 статьи 170.1 УК РФ содержит другой состав преступления, заключающийся во внесении заведомо недостоверных сведений в Реестр владельцев ценных бумаг, в систему депозитарного учета путем неправомерного доступа к Реестру владельцев ценных бумаг, к системе депозитарного учета, который может быть осуществлён дистанционно с помощью средств компьютерной техники.

## Правовые и криминологические меры противодействия экономическим преступлениям, совершаемым в киберпространстве России

Однако межгосударственные соглашения, на наш взгляд, являются лишь первым этапом в реальном международном противодействии киберпреступности. На этом этапе вводятся основные правила и принципы противодействия, определяются основные термины и понятия, устанавливаются основные направления противодействия. Представляется, что следующим этапом должно стать принятие Конвенции под эгидой ООН.

На наш взгляд, Конвенция должна состоять из двух частей. В первой части необходимо дать определение киберпреступления и киберпространства, а также исчерпывающий перечень видов киберпреступлений. Во второй части необходимо установить комплекс мер противодействия трансграничному характеру киберпреступлений, определить юрисдикцию государств и основы международного сотрудничества в данной сфере. Представляется, что положения данной Конвенции не должны нарушать суверенитет государств и их законные интересы. Меры противодействия в данной Конвенции должны быть направлены на защиту прав и свобод граждан, лишение или ущемление которых, на наш взгляд, недопустимо.

Совершенствование отечественного законодательства. Основываясь на данном исследовании, можно сделать уверенный вывод, что отечественный законодатель не уделяет должного внимания противодействию экономическим киберпреступлениям. Лишь в двух статьях Уголовного кодекса Российской

Федерации (ст. 171.2 и 185.3 УК РФ) о преступлениях в сфере экономической деятельности содержится упоминание сети «Интернет» как средства совершения преступления, и только в одной статье (ст. 159.6 УК РФ) установлен специальный способ совершения преступления против собственности – путём ввода, удаления, блокирования или модификации компьютерной информации. При этом некоторые из существующих статей составлены некорректно и требуют скорейшего изменения.

На наш взгляд, в первую очередь необходимо признать использование киберпространства в целях совершения преступления обстоятельством, повышающим его общественную опасность. Предлагается 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: 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».

Предлагается изложить название и диспозицию статьи 159.6 УК РФ в следующей редакции:

Статья 159.6. Хищение в сфере компьютерной информации 1. 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. Предлагается внести в основной состав статей 163 УК РФ «Вымогательство» и 179 УК РФ «Принуждение к совершению сделки или к отказу от ее совершения» такой признак, как совершение указанных преступлений: «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».

Предлагается дополнить статьи 170.1 УК РФ «Фальсификация Единого государственного реестра юридических лиц, Реестра владельцев ценных бумаг или системы депозитарного учета» и 183 УК РФ «Незаконное получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну» новым квалифицирующим признаком: «деяние, сопряженное с неправомерным доступом к компьютерной информации».

В целях противодействия субкультуре хакеров, а также рынку вредоносного программного обеспечения предлагается дополнить статью 273 УК РФ новой частью: «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 связи с появлением новых понятий также необходимо будет их согласовать с другими федеральными законами Российской Федерации и внести соответствующие изменения в Федеральный закон «Об информации, информационных технологиях и защите информации». Предлагается дать законодательное определение киберпространства и распространить на него действие данного Федерального закона.