Федеральное государственное бюджетное образовательное учреждение
высшего образования
«РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ПРАВОСУДИЯ»

На правах рукописи

ПРОСТОСЕРДОВ МИХАИЛ АЛЕКСАНДРОВИЧ

Экономические преступления, совершаемые в киберпространстве, и меры противодействия им

Специальность 12.00.08 - уголовное право и криминология; уголовно-исполнительное право

Диссертация на соискание ученой степени
кандидата юридических наук

Научный руководитель
заслуженный юрист
Российской Федерации,
доктор юридических наук, профессор
Бриллиантов Александр Владимирович

Москва – 2016

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

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. Определяется понятие киберпреступления как преступления, причиняющего вред разнородным общественным отношениям, совершаемого дистанционно, путём использования средств компьютерной техники,

информационно-телекоммуникационных сетей и образованного ими киберпространства.

2. Даётся авторская 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. 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. Определяются 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 «TOR», 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. Даётся 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. Предлагается авторская 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. Даётся 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 предлагается комплекс мер противодействия экономическим преступлениям, совершаемым в киберпространстве, включающий в себя меры уголовно-правового характера (предложение о включении в перечень обстоятельств, отягчающих наказание следующее обстоятельство «совершение преступления дистанционно с использованием средств компьютерной техники, информационно-телекоммуникационных сетей и киберпространства»; положения о внесении изменений в уголовное законодательство Российской Федерации (ст. 159.6 , 163, 179, ч. 2 ст. 272, ч. 2 ст. 273 УК РФ); положение о внесении дополнений в уголовное законодательство Российской Федерации статьи 165.1 «Причинение имущественного ущерба в сфере компьютерной информации»; положение о внесении дополнений в уголовное законодательство Российской Федерации части 2.1 статьи 273 УК РФ «сбыт компьютерных программ либо иной компьютерной информации, заведомо предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации») и криминологического характера (положение о принятии Национальной Стратегии кибербезопасности Российской Федерации; положение о принятии Постановления Пленума Верховного Суда Российской Федерации «О судебной практике по делам о компьютерных преступлениях»; положение о принятии разработанного комплекса профилактических мер противодействия экономическим преступлениям, совершаемым в киберпространстве; положение о принятии комплекса технических мер противодействия экономическим преступлениям, совершаемым в киберпространстве - системы персонализации пользователей информационных ресурсов в киберпространстве, основанной на биометрических признаках пользователя цифрового устройства).

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.

ГЛАВА 1
ПОНЯТИЕ И ПРИЗНАКИ КИБЕРПРОСТРАНСТВА И ЭКОНОМИЧЕСКИХ КИБЕРПРЕСТУПЛЕНИЙ

§1. Понятие и общая характеристика киберпространства

Информационная сфера сегодня - это одна из наиболее динамичных и быстро развивающихся сфер общественных отношений, нуждающихся в адекватном правовом регулировании[1]. «Интернет» стал неотъемлемой частью жизни современного общества, в нем появилась собственная инфраструктура: собственный язык, сетевая культура, магазины, публичные форумы, образовательные курсы и школы. В «Интернете» нашло своё проявление такое новое явление, как киберпространство.

Сейчас термины «киберпространство», «информационное пространство», «виртуальное пространство» и «Интернет-пространство» являются общеупотребительными, как на бытовом, так и на законодательном уровне, в том числе и в научных кругах. Однако данные понятия отличаются как по своей природе, так и по своему значению, а их неверное употребление может создать множество терминологических трудностей и проблем. Следовательно, в первую очередь необходимо внести ясность в используемую терминологию.

«Информационное пространство» слишком широкое понятие и по своей природе включает любую сферу жизни общества, где присутствует информация (СМИ, телевидение, телефония, книги и иная печатная продукция). «Киберпространство» является лишь частью «информационного пространства»[2].

Термин «виртуальное пространство» также является слишком широким, поскольку «виртуальное» как синоним слова «воображаемое», охватывает куда

---

[1]Дворецкий М.Ю., Копырюлин А.Н. Оптимизация уголовной ответственности и проблемы квалификации преступлений в сфере компьютерной информации: Монография. / Дворецкий М.Ю., Копырюлин А.Н. Тамбов, ТГУ им. Г.Р. Державина. 2006. С.15.

[2]Концепция Стратегии кибербезопасности Российской Федерации. [Электронный ресурс] //URL:http://www.councils.gov.ru/media/files/41d4b3dfbdb25cea8a73.pdf (Дата обращения: 28.04.2012).

больший круг явлений, нежели те, что ограничены компьютерными технологиями.

«Интернет-пространство», наоборот, является слишком узким термином, так как помимо сети «Интернет» существуют и другие, более мелкие информационно-телекоммуникационные сети («FidoNet», «CREN», «EARNet», «EUNe», «TOP», «ANts P2P», «Freenet»). Более того, «Интернет» является именем собственным и, возможно, в будущем на его место придёт другая всемирная информационно-телекоммуникационная сеть, с другим именем, а киберпространство в нём останется неизменным.

Термин «киберпространство» употребляется в зарубежном законодательстве и литературе. В английском языке «cyber» является не самостоятельным словом, а префиксом, то есть начальным элементом сложных слов, а на русский язык он переводится как «связанный с компьютерами, информационными технологиями, «Интернетом»[1]. Во избежание терминологической путаницы многие авторитетные ученые (В.А. Номоконов, Т.Л. Тропина) не переводят данный термин и используют приставку «кибер». Однако, по мнению других авторитетных ученых (В.Г. Степанов-Егиянц, Р.И. Дремлюга), использование термина «киберпространство» в российской криминологической науке пока под вопросом[2], и для избежания использования англицизмов всё же необходимо применять иную терминологию[3].

По нашему мнению, термин «киберпространство» является самым оптимальным из всех существующих, а использование данного термина позволит в полной мере раскрыть природу явлений, происходящих в информационных сетях, одной из которых является «Интернет». Более того, в связи с готовящейся Стратегией кибербезопасности Российской Федерации использование данного термина является наиболее актуальным.

---

[1]Дворецкий М.Ю., Копырюлин А.Н. Указ. соч. С.35.

[2]Дремлюга Р.И. Интернет-преступность: Монография. Владивосток, Изд. Дальневосточного университета. 2008. С. 42.

[3]Степанов-Егиянц В.Г. Преступления сфере безопасности обращения компьютерной информации: сравнительный анализ: дис. …канд. юрид. наук. М., 2005. С.11.

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 разваливалось[2].

«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

[1] 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..

[2] Информационный ресурс «Улфек». Компьютерная преступность. [Электронный ресурс] // URL: http://ulfek.ru/osnovy-bezopasnosti-informatsionnykh-tekhnologij/3469-kompyuternaya-prestupnost.html (Дата обращения: 1.05.2012).

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 России[4]. 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

[1]Волеводз А.Г. Противодействие компьютерным преступлениям: правовые основы международного сотрудничества. М., Юрлитинформ, 2001. С.15.

[2]Информационный ресурс «BugTraq.Ru» История компьютерного андеграунда Хакеры 80-х [Электронный ресурс] // URL: http://bugtraq.ru/library/underground/underground4.html (Дата обращения: 1.05.2012).

[3]Волеводз А.Г. Противодействие компьютерным преступлениям: правовые основы международного сотрудничества. М., Юрлитинформ, 2001. С.15.

[4]Батурин Ю.М. Проблемы компьютерного права. М., Юридическая литература. 1991. С. 126.

[5]Тропина Т.Л. Киберпреступность: понятие, состояние, уголовно-правовые меры борьбы: дис. …канд. юрид. наук. Владивосток, 2005. С.27

пользователей ко всем компьютерным сетям достигло 10 000 человек в год[1], 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 США[4].

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.

---

[1]Волеводз А.Г. Там же.

[2]Информационный ресурс «Компьютерная газета». [Электронный ресурс]URL: http://www.nestor.minsk.by/kg/2002/31/kg23101a.html (Дата обращения: 27.05.2012)

[3]Тропина Т.Л. Киберпреступность: понятие, состояние, уголовно-правовые меры борьбы: дис. …канд. юрид. наук. Владивосток, 2005. С. 28.

[4]Сухомлинов В.В. Вопрос - Ответ // Юный техник. 1989. №5. С.78.

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. **S**oviet **U**nion)[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 киберпространству[6].

В этот период времени в России появилась первая официальная статистика о компьютерной преступности[7]. Так, в 1997 году в России было зарегистрировано 33 факта совершения компьютерных преступлений.

30 сентября 1998 года доступ к сети «Интернет» появился у одного миллиона россиян, что спровоцировало дальнейший рост киберпреступности. В

---

[1]Информационный ресурс «Русский проект». Мобильная связь и компьютерные сети в СССР. [Электронный ресурс] // URL: http://www.rusproject.org/node/72 (Дата обращения: 05.05.2012).

[2]Нургалиев Р. Электронный патруль // Правовые вопросы национальной безопасности . 2009. № 5-6. С. 25-29.

[3]Официальный сайт магазина «Амазон» [Электронный ресурс] // URL: www.amazon.com (Дата обращения: 05.05.2012).

[4]Социальная сеть «Classmates». [Электронный ресурс] // URL: http://www.classmates.com/ (Дата обращения: 05.05.2012).

[5]Дадали А. Электронный банкинг [Электронный ресурс] // URL:http://www.compress.ru/article.aspx?id=10653&iid=434 (Дата обращения: 05.05.2012).

[6]Информационный ресурс «Ciec.org». Reno vs. ACLU, 117 S.Ct. 2329 (1997) (casebook at 932-53). [Электронный ресурс] // URL:http//ciec.org/SC_appeal/opinion.shtml. (Дата обращения: 27.05.2012).

[7]Статистика базировалась на преступлениях в сфере компьютерной информации, предусмотренных статьями главы 28 УК РФ.

1998 году было зарегистрировано уже 64 факта совершения компьютерных преступлений, в 1999 году – 285, а в 2000 году –800[1]. Пик пришелся на 2009 год – тогда было зарегистрировано 11 636 компьютерных преступлений[2].

К 2012 году Российская Федерация вышла по показателям численности пользователей сети «Интернет» на первое место в Европе. Примерно 60% населения России старше 12 лет хотя бы раз в месяц пользуются «Интернетом», что составляет 74,4 миллиона человек[3].

Проанализировав историю возникновения киберпространства и киберпреступности, с полной уверенностью можно сделать вывод, что данные явления напрямую связаны с развитием информационных технологий. С появлением новых технологий наблюдается появление нового, более сложного вида преступности. 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.

Однако, что же собой представляет киберпространство? Этим вопросом задались многие учёные и философы. Так, С.Н. Хуторной в своём диссертационном исследовании указывает, что киберпространство представляет собой компьютерно-технологическую виртуальную реальность, характеризующуюся соединением гипертекста и гиперреальности, интерактивностью, модификацией пространственно-временных черт, разнонаправленностью пространственно-временных потоков и их многомерностью и дискретностью[4].

По мнению Р.И. Выкова, киберпространство – это принципиально новый вид проективного пространства культуры, который соединяет знаковую

---

[1]Дремлюга Р.И. Интернет-преступность: монография. С. 76.

[2]Официальный сайт МВД РФ [Электронный ресурс] // URL:https://mvd.ru/upload/site1/import/65afff0dd0.pdf (Дата обращения: 20.01.2015)

[3]Смирнов А.А. Сеть «Интернет» в механизме криминологической детерминации. // Библиотека криминалиста. 2013. №5(10) С.161.

[4]Хуторной С.Н. Киберпространство и становление сетевого общества: дис… канд. фил. наук. Воронеж, 2013. С.7.

реальность и современную технологию, облегчающую и существенно ускоряющую мыслительную деятельность людей[1].

Р.А. Барышев указывает, что киберпространство – это одна из множества форм виртуальной реальности, при этом если виртуальная реальность обозначает большой круг явлений от кинематографа и музыкального произведения до зеркального отражения, снов и фантазий, то киберпространство в свою очередь четко очерчивает виртуальную реальность границами взаимодействия человека и компьютера ... – это метафизическая абстракция, применяемая для описания объектов, широко распространённых в компьютерной сети[2].

Проанализировав работы данных авторов, можно выделить одну общую черту: все они представляют киберпространство как некую абстрактную виртуальную реальность, существование которой возможно лишь в рамках средств компьютерной техники. То есть киберпространство – это не просто объединение компьютеров (сеть), а нечто иное. Тогда встаёт вопрос: в чём же отличие киберпространства от информационной сети, например, от сети «Интернет»?

Как правильно указывает А.Г. Волеводз, сеть «Интернет», включающая разветвленную систему серверов, поставляющих информацию, создаёт мировое информационное пространство[3].

Сеть «Интернет» – это материальное отражение киберпространства в реальном мире. «Интернет» состоит из отдельных компьютеров, серверов и других технических устройств, объединённых между собой проводным и беспроводным путём по всему миру (через спутник, микроволновые и электромагнитные сигналы, Wi-Fi, 3G, LTE), то есть это всемирная информационно-телекоммуникационная сеть.[4]

---

[1]Вылков Р. И. Киберпространство как социокультурный феномен, продукт технологического творчества и проективная идея: дис. …канд. фил. наук. Екатеринбург, 2009. С.128, 129.

[2]Барышев Р. А. Киберпространство и проблема отчуждения: дис. …канд. фил. наук. Красноярск, 2009. С 56.

[3]Противодействие компьютерным преступлениям: правовые основы международного сотрудничества. М., Юрлитинформ, 2001. С.17, 18.

[4] 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

Киберпространство – это искусственно созданная среда, существование которой ограничено информационно-телекоммуникационной сетью, пользователи которой могут свободно вступать в административные, гражданские, уголовные и другие правоотношения. Киберпространство может появиться в любой информационно-телекоммуникационной сети. Например, в рамках сети «Интернет» можно говорить об «Интернет-пространстве». Следовательно, «Интернет» – это не само «киберпространство», а лишь условие, в котором оно может существовать.

Такая же точка зрения была высказана Верховным Судом США ещё в 1997 году в деле Рино против Американского союза гражданских свобод[1].

Согласно решению Верховного Суда США, под киберпространством понимается «уникальная среда, не расположенная в географическом пространстве, но доступная каждому в любой точке мира, посредством доступа в сеть «Интернет».

«Интернет» Верховный Суд США определяет как «глобальное объединение компьютерных сетей и информационных ресурсов, не имеющее четко определённого собственника и служащее для интерактивной коммуникации физических и юридических лиц».

В России, на официальном уровне, термин «киберпространство» впервые был применён только в 2013 году в Проекте Концепции Стратегии кибербезопасности Российской Федерации, опубликованной Советом Федерации ФС РФ[2].

«Киберпространство», согласно данному Проекту – *это сфера деятельности в информационном пространстве*[3]*, образованная совокупностью*

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

[1]Информационный ресурс «Ciec.org». Reno vs. ACLU, 117 S.Ct. 2329 (1997) (casebook at 932-53). [Электронный ресурс] // URL:http//ciec.org/SC_appeal/opinion.shtml. (Дата обращения: 27.05.2012).

[2]Концепция Стратегии кибербезопасности Российской Федерации.[Электронный ресурс] // URL:http://www.council.gov.ru/media/files/41d4b3dfbdb25cea8a73.pdf (Дата обращения: 28.04.2012).

[3]Согласно данному Проекту, под «информационным пространством» понимается сфера деятельности, связанная с формированием, созданием, преобразованием, передачей, использованием, хранением информации, оказывающая воздействие, в том числе на индивидуальное и общественное сознание, информационную инфраструктуру и собственно информацию.

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).

На наш взгляд, определение, данное в Концепции Стратегии кибербезопасности России, наиболее полно раскрывает природу киберпространства. В нём отражено отношение информационного пространства к киберпространству, как общего к частному. Специально подчеркнуто отличие информационно-телекоммуникационной сети как материальной составляющей киберпространства, и самого киберпространства как уникальной среды или сферы человеческой активности, а также то, что сеть «Интернет» не единственная из существующих информационно-телекоммуникационных сетей. Поэтому в данной работе будет использовано именно это определение.

Основываясь на вышесказанном, можно сделать следующие выводы:

1. понятие «киберпространство» шире понятия «Интернет-пространство» и включает его;

2. киберпространство – *это 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);*

3. сеть «Интернет» – это материальное отражение киберпространства в реальном мире: это не само «киберпространство», а лишь условие, в котором оно может существовать;

4. с появлением новых технологий (киберпространства) наблюдается появление нового, более сложного вида преступности (киберпреступность). 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.

§2. Понятие и общественная опасность киберпреступления

Понятие «киберпреступление» нередко путают с понятиями «компьютерное преступление» и «преступление в сфере компьютерной информации», поскольку всех их объединяет одно – это использование средств компьютерной техники для совершения преступления, однако имеются существенные отличия.

Так, в научной литературе закрепилось мнение, что термин «компьютерное преступление» гораздо шире понятия «преступление в сфере компьютерной информации»[1]. Данное мнение базируется на том, что объектом компьютерного преступления могут быть не только отношения, складывающиеся в сфере нормального оборота компьютерной информации, но и другие охраняемые уголовным законом общественные отношения, такие как отношения собственности, честь, достоинство, деловая репутация, общественный порядок, даже мир и безопасность человечества.[2]

Так, В.Б. Вехов даёт следующее определение компьютерного преступления: это предусмотренное уголовным законом общественно опасное действие, совершенное с использованием средств электронно-вычислительной (компьютерной) техники. При этом не имеет значения, на какой стадии совершения преступления данная техника была использована: в ходе подготовки, в процессе совершения преступления или для сокрытия следов совершения преступления[3].

---

[1]См.: Зыков Д.А. Виктимологические аспекты предупреждения компьютерного мошенничества: дис. … канд. юрид. наук. Владимир, 2002. С. 17.; Жмыхов А.А. Компьютерная преступность за рубежом и ее предупреждение: дис. … канд. юрид. наук. М., 2003. С.18.; Дремлюга Р.И. Интернет-преступность: монография. С. 38.

[2] Простосердов, М.А. Проблемы квалификации компьютерных преступлений / М.А. Простосердов // Российское правосудие. – 2012. − № 6 (74). – С. 106-108.

[3]Вехов В.Б. Криминалистическая характеристика и совершенствование практики расследования и предупреждения преступлений, совершаемых с использованием компьютерной техники: автореф. дис. … канд. юрид. Наук. Волгоград, 1995. С.13

Следовательно, под понятие «компьютерное преступление» может подпадать любое преступление, совершённое с использованием средств компьютерной техники (мошенничество, вымогательство, клевета, шпионаж, террористический акт, призывы к развязыванию агрессивной войны и многие другие), в то время как преступлениями в сфере компьютерной информации следует считать более узкий круг преступлений, объектом которых и являются отношения, складывающиеся в сфере нормального оборота компьютерной информации (неправомерное использование компьютерной информации; создание, использование и распространение вредоносных компьютерных программ; нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей).

В свою очередь, все компьютерные преступления могут быть совершены как в материальном мире, так и в киберпространстве. Преступления, совершаемые в киберпространстве, обладают спецификой, так как отличаются повышенной степенью общественной опасности от смежных преступлений. На основании этого многие ученые выделяют такие преступления в самостоятельную группу[1]. Они могут быть направлены на любые общественные отношения, в том числе и на отношения, складывающиеся в сфере нормального оборота компьютерной информации, отношения собственности, отношения в сфере экономической деятельности и т.д. Наглядно разницу между данными видами преступлений можно продемонстрировать на Рисунке 1.[2]

Представляется, что киберпреступления – это самостоятельный вид компьютерных преступлений, имеющий объектом разнородные общественные отношения. Экономические киберпреступления являются лишь частью всего

[1]См.: Гаджиев М.С. Криминологический анализ преступности в сфере компьютерной информации (по материалам Республики Дагестан): дис. … канд. юрид. наук. Махачкала, 2004. С. 19; Дремлюга Р.И. Интернет-преступность: монография. С.40-46; Кесареева Т.П. Криминалистическая характеристика и проблемы предупреждения преступности в российском сегменте сети Интернет: дис…. канд. юрид. наук. 2002. С.56; Рассолов И.М. Право и «Интернет»: теоретические проблемы. 2-е изд., доп. М., Норма, 2009. С. 251–253; Тропина Т.Л. Киберпреступность: понятие, состояние, уголовно-правовые меры борьбы: дис. …канд. юрид. наук. Владивосток. 2005. С. 38.

[2] См.: Приложение №1.

спектра преступлений, совершаемых в киберпространстве, однако именно о них и будет идти речь в настоящем диссертационном исследовании.

В научной литературе существует множество определений данного вида преступлений. По мнению Т.Л. Тропиной, под киберпреступлением следует понимать «виновное совершенное общественно опасное уголовно наказуемое вмешательство в работу компьютеров, компьютерных программ, компьютерных сетей, несанкционированная модификация компьютерных данных, а также иные общественно опасные деяния, совершаемые с помощью или посредством компьютеров, компьютерных сетей и программ, а также с помощью или посредством иных устройств доступа к моделируемому с помощью компьютера пространству».[1]

Данное определение, на наш взгляд, раскрывает природу преступления, совершённого с использованием компьютерных средств, однако является слишком широким и неточным. Так, можно предположить, что под «иные общественно опасные деяния, совершаемые с помощью компьютера» могут попадать и такие преступления, в которых компьютер был применён не по своему основному назначению, например, в случае если компьютером был нанесён удар другому человеку. При этом в таких преступлениях разная степень использования компьютера, разные способы совершения преступления, разные объекты и предметы посягательства, и, как следствие – иные характер и степень общественной опасности.

Другое определение киберпреступления было дано И.М. Рассоловым как общественно опасное деяние, которое совершается с использованием средств компьютерной техники в отношении информации, обрабатываемой и используемой в «Интернете»[2]. По нашему мнению, данное определение является слишком узким, поскольку, во-первых, существуют и другие информационно-телекоммуникационные сети, образующие киберпространство, кроме сети «Интернет» («FidoNet» либо любые частные локальные сети); во-вторых, в

[1]Тропина Т.Л. Киберпреступность: понятие, состояние, уголовно-правовые меры борьбы: дис. …канд. юрид. наук. Владивосток. 2005. С.10.

[2]Рассолов И.М. Право и «Интернет»: теоретические проблемы. 2-е изд., доп. М., Норма. 2009. С.135.

киберпространстве совершаются преступления в отношении не только информации, но и собственности, а также других общественных отношений (общественной безопасности, общественной нравственности).

Р.И. Дремлюга дал иное определение «Интернет-преступления». По его мнении, это компьютерное преступление, … совершаемое посредством сети Интернет.[1]

Данное определение разделяет понятие «компьютерное преступление» и «киберпреступление» (или в данном случае «Интернет-преступление»), как общее и частное, а также устанавливает отличительный признак последнего. Интернет-преступление должно совершаться исключительно посредством сети «Интернет», так же как и киберпреступление должно совершаться исключительно посредством киберпространства.

Как указывает О.С. Гузеева, киберпреступление – предусмотренное уголовным законодательством общественно опасное, противоправное деяние, совершённое посредством удалённого доступа к объекту посягательства с использованием глобальных компьютерных сетей в качестве основного средства достижения цели.[2] В данном определении, как и в предыдущем, возможности киберпространства также оцениваются как средство совершения преступления.

Т.П. Кесареева также выделяет преступления в сети «Интернет» как преступления, совершенные путем вхождения в сеть «Интернет»[3]. Данное определение, на наш взгляд, является слишком абстрактным и неточным, поскольку под него могут подпадать любые преступления, при совершении которых преступник пользовался сетью «Интернет», например, для поиска информации о жертве или для поиска соучастников.

Представляется, что при определении киберпреступления необходимо учитывать особенности, характерные для всех киберпреступлений, а не только

---

[1]Дремлюга Р.И. Интернет-преступность: монография. С.45.

[2]Гузеева О.С. Предупреждение размещения информации, способствующей распространению наркотических средств, в российском сегменте сети Интернет (криминологические и уголовно-правовые проблемы). автореф. дис. … канд. юрид. наук. М., 2008. С. 12.

[3]Кесареева Т.П. Криминалистическая характеристика и проблемы предупреждения преступности в российском сегменте сети Интернет: дис…. канд.юрид.наук. М., 2002. С. 56.

для преступлений в сфере компьютерной информации или преступлений, совершённых с использованием сети «Интернет». На наш взгляд, необходимо проанализировать такие признаки киберпреступления, как анонимность, трансграничность, дистанционность, а также использование компьютера, вирусов (иных вредоносных программ), информационно-телекоммуникационных сетей и киберпространства.

Во-первых, киберпреступление, каким бы способом оно ни совершалось, является преступлением, то есть виновным, совершённым, общественно опасным деянием, запрещённым Уголовным кодексом Российской Федерации под угрозой наказания. В самом термине «киберпреступление» уже используется понятие «преступление», что освобождает нас от повторения его основных признаков.

Во-вторых, киберпреступления способны причинить вред всем охраняемым уголовным законом общественным отношениям, а не только отношениям в сфере компьютерной информации. Следовательно, не представляется возможным классифицировать киберпреступления по одному лишь объекту посягательства и просто выделить их в отдельный раздел или главу Уголовного кодекса Российской Федерации.

В-третьих, несмотря на то, что киберпространство трансгранично, не все киберпреступления также носят трансграничный характер (например, если виновный и потерпевший живут в одной стране). То же можно сказать и о таких признаках киберпреступлений, как анонимность или об использовании вредоносных программ. Не все киберпреступления совершаются анонимно, многие (такие как клевета или публичные призывы к осуществлению террористической деятельности или публичное оправдание терроризма) совершаются открыто с использованием реальных имён и фамилий. Точно так же, как и не все киберпреступления совершаются с использованием вирусов или иных вредоносных программ (вымогательство в социальной сети или через электронную почту). Данные признаки киберпреступлений являются неосновными (факультативными), то есть они могут быть присущи лишь отдельным киберпреступлениям, но не всем.

Представляется, что объединяющими признаками всех киберпреступлений являются средства их совершения – киберпространство, информационно-телекоммуникационные сети и средства компьютерной техники.

Как было сказано ранее, киберпространство, как некая сфера деятельности (виртуальная реальность), может существовать лишь в рамках информационно-телекоммуникационной сети. Подобная сеть сформирована из множества устройств и каналов связи, позволяющих получить доступ в киберпространство. Устройства могут быть различными (настольный компьютер, ноутбук, планшет или смартфон), как и информационно-телекоммуникационные сети («Internet», «FidoNet», «CREN», «EARNet», «EUNe»). При этом один компьютер может быть подключён сразу к нескольким информационно-телекоммуникационным сетям. Поэтому ограничивать понятие «киберпреступление» лишь использованием персонального компьютера или сети «Интернет» является в корне неверным. Преступник использует разнообразные устройства и информационно-телекоммуникационные сети для доступа именно в киберпространство. Следовательно, киберпространство является обязательным условием совершения киберпреступления.

Наличие информационно-телекоммуникационной сети тоже является обязательным условием совершения киберпреступления, поскольку без неё не будет киберпространства. Использование средств компьютерной техники для доступа в киберпространство также является неотъемлемым признаком всех киберпреступлений, поскольку никаким другим образом в киберпространство попасть нельзя.

Преступник использует компьютер в первую очередь для доступа в киберпространство. В случае если виновное лицо просто возьмёт компьютер в руки и умышленно причинит им кому-либо вред здоровью, то такое деяние нельзя назвать киберпреступлением. Получив доступ в киберпространство, преступник получил новые возможности – теперь он способен совершать преступления дистанционно, не выходя из дома.

Представляется, что дистанционное совершение преступления также является неотъемлемой характеристикой способа совершения всех киберпреступлений. Виновное лицо осознано использует возможности киберпространства таким образом, чтобы между ним и потерпевшим было безопасное расстояние.

Основываясь на вышесказанном, нами предлагается следующее определение киберпреступления:

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.

Данное определение раскрывает понятие «киберпреступление» через его обязательные признаки, такие как средство (киберпространство) и способ (дистанционный способ). Также оно является ёмким, поскольку не дублирует все признаки преступления. Данное определение не ограничено ни объектом посягательства, ни конкретной информационно-телекоммуникационной сетью, что делает его достаточно гибким: киберпреступлением будет считаться как мошенничество в сети «Интернет», так и неправомерный доступ к компьютерной информации в сети «FidoNet» или «TOP».

Следуя данной логике, *экономическим киберпреступлением будет считаться такое киберпреступление, родовым объектом которого являются экономические отношения.*

Раскрыв понятие киберпреступления, на наш взгляд, необходимо подробнее остановиться на определении характера и степени общественной опасности данной группы преступлений. Многие ученые сходятся во мнении, что киберпреступления обладают более высокой степенью общественной опасности, нежели аналогичные преступления, совершаемые в материальном мире.

Так, Н.А. Коменский указывает, что использование компьютерной информации и информационных технологий в качестве средства совершения преступления повышает его общественную опасность, и считает целесообразным

закрепить данный признак в качестве обстоятельства, отягчающего наказание[1]. С похожим предложением выступает С.С. Медведев. Он предлагает дополнить статью 63 УК РФ новым обстоятельством, отягчающим наказание: «с использованием результатов автоматизированной обработки данных»[2]. Р.И. Дремлюга также предлагает дополнить статью 63 УК РФ новым обстоятельством: «совершение преступления посредством компьютерной сети»[3]. По мнению В.Г. Степанова-Егиянца, «использование компьютера государственного органа» для совершения преступления повышает общественную опасность преступления и требует более строгого наказания»[4]. По мнению Т.Л. Тропиной, «киберпреступность обладает повышенной общественной опасностью вследствие возможности причинения крупного ущерба при минимальных затратах и невысоком риске»[5].

Рассмотрим общественную опасность экономических киберпреступлений.

Согласно пункту 1 Постановления Пленума Верховного Суда Российской Федерации от 11.06.1999 г № 40 "О практике назначения судами уголовного наказания", **характер** общественной опасности преступлений зависит от объекта посягательства, способа совершения преступления, формы вины и отнесения Уголовным кодексом Российской Федерации преступного деяния к соответствующей категории преступлений; **степень** общественной опасности определяется обстоятельствами содеянного: размером вреда или тяжестью наступивших последствий, ролью виновного при совершении преступления в соучастии[6]. В связи с тематикой исследования наибольший интерес вызывают

[1]Коменский Н.А. Компьютерная информация и информационные технологии как средство совершения преступления. // 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.138-139.

[2]Медведев С.С. Мошенничество в сфере высоких технологий: дис...канд.юрид.наук. Краснодар, 2008. С.46.

[3]Дремлюга Р.И. Интернет-преступность: монография. С.218.

[4]Степанов-Егиянц В.Г. Преступления сфере безопасности обращения компьютерной информации: сравнительный анализ: дис. …канд. юрид. наук. М., 2005. С.124.

[5]Тропина Т.Л. Киберпреступность: понятие, состояние, уголовно-правовые меры борьбы: дис. …канд. юрид. наук. Владивосток. 2005. С.210.

[6]Постановление Пленума Верховного Суда РФ от 11.06.1999 № 40 «О практике назначения судами уголовного наказания» // Бюллетень Верховного Суда РФ. 1999. N 8.

такие признаки, как объект посягательства, способ совершения преступления, а также размер причинённого вреда.

При анализе **характера общественной опасности** экономических киберпреступлений в первую очередь следует рассмотреть объект посягательства и способ совершения преступления. По нашему мнению, в киберпространстве существует реальная возможность совершения двух групп экономических киберпреступлений, отличие между которыми проявляется именно в объекте и способе.

В зависимости от способа совершения все экономические киберпреступления можно разделить на:

- экономические киберпреступления, совершаемые путём психологического воздействия на человека (обман, введение в заблуждение, угрозы);
- экономические киберпреступления, совершаемые путём воздействия на оборудование (компьютеры, смартфоны, маршрутизаторы и иное оборудование).

Такое деление обуславливается тем, что в первую группу экономических киберпреступлений входят такие общественно опасные деяния, при совершении которых причиняется вред только лишь одному непосредственному объекту – экономическим отношениям. При совершении экономических киберпреступлений второй группы преступник причиняет вред дополнительному объекту – отношениям, по правомерному и безопасному использованию компьютерной информации.

Киберпреступления первой группы отличаются тем, что при их совершении используются уже существующие сайты, форумы и готовые программы. Преступникам нет необходимости совершать неправомерный доступ к компьютерной информации, они работают с тем, что им предоставляет киберпространство само по себе.

К таким киберпреступлениям можно отнести основной состав мошенничества (ст. 159 УК РФ), вымогательство (ст. 163 УК РФ), причинение имущественного ущерба путём обмана и злоупотребления доверием (ст. 165 УК

РФ), фальсификацию единого государственного реестра юридических лиц (ч. 1 ст. 170.1 УК РФ), незаконное предпринимательство (ст. 171 УК РФ), незаконное использование средств индивидуализации товаров, работ и услуг (ст. 180 УК РФ), незаконное разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну (ч. 2 ст. 183 УК РФ), и другие.

Способ совершения данных киберпреступлений мало чем отличается от способа совершения аналогичных преступлений в материальном мире: при мошенничестве – обман либо злоупотребление доверием; при вымогательстве – угроза; при фальсификации – предоставление заведомо ложных данных и т.д. Обман в киберпространстве несёт тот же характер общественной опасности, что и обман в материальном мире, однако теперь они осуществляются дистанционно. То же проявляется и с угрозами и с другими ранее оговорёнными способами.

К преступлениям второй группы можно отнести мошенничество в сфере компьютерной информации (ст. 159.6 УК РФ), внесение заведомо недостоверных сведений в реестр владельцев ценных бумаг либо систему депозитарного учёта (ч. 2 ст. 170.1 УК РФ), незаконное получение сведений, составляющих коммерческую, налоговую или банковскую тайну (ч. 1 ст. 183 УК РФ), и другие.

При совершении данных преступлений лицо может использовать специальные программы, позволяющие беспрепятственно осуществить неправомерный доступ к компьютерной информации («BruteForce», «Public Brute/Checker»), либо использовать вирусы («Creeper», «Elk Cloner», «Brain», «Jerusalem», «March6», «CIH», «Nimda»), троянские программы («Win64/HackKMS.A»), компьютерные черви («Melissa», «Sasser», «My Doom», «Conficker») и другие вредоносные программы. Используя данное вредоносное программное обеспечение при совершении экономических киберпреступлений, виновное лицо причиняет вред сразу двум объектам – экономическим отношениям и отношениям в сфере компьютерной информации.

Представляется, что двухобъектная природа данной группы преступлений является обстоятельством, повышающим их общественную опасность. Квалифицировать данные преступления необходимо по совокупности со ст. 272

«Неправомерный доступ к компьютерной информации» и 273 УК РФ «Создание, использование и распространение вредоносных компьютерных программ» в зависимости от конкретных обстоятельств дела.

При анализе **степени общественной опасности** экономических киберпреступлений особое внимание следует уделить размеру причиняемого вреда. Как указывает А.К. Киселёв, ущерб от киберпреступлений в 2007 – 2008 годах во всём мире оценивался в 8 миллиардов долларов[1]. По последним данным, приведённым в июле 2013 года в совместном анализе американского центра стратегических и международных исследований и компании «McAfee», ежегодные потери мировой экономики от киберпреступлений достигли уже 500 миллиардов долларов[2]. По мнению многих ученых (Т.М.Лопатиной, В.А. Номоконов, Т.Л. Тропина), доходы теневого бизнеса в сети «Интернет» могут сравниться с прибылью от незаконной торговли наркотиками[3].

При этом согласно данным о преступлениях, совершенных русскими хакерами на территории России, финансовые показатели преступников в 2010 году составили 1,3 миллиарда долларов. В 2011 году российские хакеры заработали около 3,7 миллиарда долларов, а в 2013 году ожидалось удвоение данного показателя[4].

В свою очередь, по подсчетам компании «Group-IB»[5], в 2011 году киберпреступники из России, стран СНГ, Балтии и стран бывшего СССР заработали 4,5 млрд. долл. Наибольший ущерб российским пользователям причинили Интернет-мошенники, суммарно похитившие примерно 942 млн. долл. Основная часть этих средств приходится на мошенничества в системах Интернет-банкинга – 21,3%, на фишинг (2,4%) и на хищение электронных денег (1,3%). При

---

[1]Киселёв А.К. Киберпреступность – взгляд из Европы. // Библиотека криминалиста. − 2013. − №5(10). - С.311.

[2]Номоконов В.А., Тропина Т.Л. Киберпреступность: прогнозы и проблемы борьбы. // Библиотека криминалиста. 2013. №5(10). С.151.

[3]Лопатина Т.М. Проблемы формирования уголовно-правового способа борьбы с компьютерным мошенничеством. // Библиотека криминалиста. 2013. №5(10). С.34.

[4]Там же. – С.153.

[5]Информационный ресурс Group-IB. Русский рынок компьютерных преступлений: состояние и тенденции 2011. [Электронный ресурс] // URL:http://www.group-ib.ru/images/analytics/group-ib_report_2011_rus.pdf (Дата обращения: 26.04.2015).

этом в России ежедневно совершалось 44 факта хищения из систем дистанционно-банковского обслуживания, средняя сумма хищений у юридических лиц составила 1 641 000 рублей, а у физических лиц — 75 000 рублей[1].

По данным разных исследовательских компаний, на 2012 год ущерб россиян только от кибермошенничества в финансовой сфере варьируется от 615 миллионов до 2 миллиардов долларов США (18,5 – 60,2 миллиарда рублей)[2]. Для сравнения ущерб от всех преступлений экономической направленности (как киберпреступлений, так и преступлений, совершаемых в материальном мире) по официальным данным МВД РФ в 2012 году составил 144,85 миллиарда рублей[3].

Из приведённых данных следует, что размер вреда от экономических киберпреступлений очень высок, что свидетельствует о повышенной степени общественной опасности таких преступлений. Однако данным цифрам может быть и иное объяснение: один человек с возможностями киберпространства может совершить гораздо больше преступлений, нежели без таких возможностей. Так, например, за одно и то же время хакер может совершить десять хищений, в то время как обычный преступник – всего одно. Также с возможностями киберпространства виновный может одновременно совершать преступления по отношению сразу к нескольким протерпевшим, приумножая тем самым причиняемый вред.[4]

С другой стороны, существуют и такие примеры, в которых использование киберпространства не повышает степень общественной опасности преступлений, например, если при вымогательстве виновное лицо требует перечислить

---

[1]Доклад компании Group-IB «Threat Intelligence Report 2012 – 2013 H1» [Электронный ресурс] // URL: http://report2013.group-ib.ru/ (Дата обращения: 26.04.2012).

[2]Официальный сайт «ИТАР-ТАСС» [Электронный ресурс] // URL: http://tasstelecom.ru/news/one/23775 (Дата обращения: 27.05.2012); Информационный ресурс «Икс Медиа». Серый, черный, белый Интернет [Электронный ресурс] //URL: http://www.iksmedia.ru/articles/4808504.html (Дата обращения: 27.05.2012).

[3]Официальный сайт МВД РФ [Электронный ресурс] // URL: https://mvd.ru/folder/101762/item/804701/ (Дата обращения: 20.01.2015).

[4] 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.

определённую денежную сумму под угрозой распространения порочащих сведений всего у одного потерпевшего. Преступник в данном случае использует киберпространство лишь в качестве средства коммуникации (телефон или обычную почту), что не может повлиять на общественную опасность вымогательства. В данном случае нет особой разницы, как было совершено вымогательство – с использованием киберпространства либо без.

Представляется, что на общественную опасность киберпреступлений может повлиять не само по себе киберпространство, а то, каким образом его используют.

В случае если виновное лицо при хищении (ст. 159.6 УК РФ) использует возможности киберпространства, чтобы получить доступ сразу к нескольким банковским счетам, причиняя бóльший вред, то такое использование киберпространства напрямую повышает общественную опасность данных преступлений.

В то же время, если виновное лицо при совершении какого-либо преступления использует возможности киберпространства незначительно, только лишь в качестве средства коммуникации либо поиска, хранения информации (т.е. по его основному назначению), то такое использование киберпространства не может повлиять на общественную опасность данных преступлений. Однако это может выяснить только суд, в зависимости от конкретного преступления, конкретных обстоятельств дела и личности виновного.

Из этого следует, что в отдельных случаях использование киберпространства может быть признано обстоятельством, повышающим общественную опасность преступления, поскольку данный способ может причинить вред дополнительному объекту, способствует причинению большего вреда и облегчает совершение преступления.

На наш взгляд, следует согласиться с Р.И. Дремлюгой и С.С. Медведевым в части включения использования киберпространства в перечень обстоятельств, отягчающих наказание. Однако одновременно с этим необходимо дать суду возможность самому решать, является ли в деле использование конкретных информационных ресурсов и технологий обстоятельством, повышающим

общественную опасность конкретного преступления. Это позволит сделать норму более гибкой, а сложности правоприменения могут быть решены на уровне Постановления Пленума Верховного Суда Российской Федерации.

Норма, подобная предлагаемой нами, уже существует в действующем уголовном законодательстве касательно другого обстоятельства, отягчающего наказание, – состояния опьянения.

Согласно части 1.1. статьи 63 УК РФ суд в зависимости от характера и степени общественной опасности преступления, обстоятельств его совершения и личности виновного может признать отягчающим обстоятельством совершение преступления в состоянии опьянения, вызванном употреблением алкоголя, наркотических средств или других одурманивающих веществ.

На наш взгляд, подобную законодательную конструкцию можно использовать и в отношении такого обстоятельства, как «совершение преступления дистанционно с использованием средств компьютерной техники, информационно-телекоммуникационных сетей и киберпространства». Однако с точки зрения юридической техники норма нуждается в небольшой редакции.

В настоящем виде часть 1.1. статьи 63 УК РФ нарушает один из основополагающих принципов назначения наказания: перечень обстоятельств, отягчающих наказание, закрыт, и ни одно обстоятельство, не вошедшее в перечень, не может быть признано судом отягчающим. Состояние опьянение не указано в части 1 статьи 63 УК РФ, следовательно, оно не может быть признано отягчающим.

Юридически правильным решением, на наш взгляд, было бы включить состояние опьянения в перечень обстоятельств, отягчающих наказание (ч. 1 ст. 63 УК РФ), и дать суду право в зависимости от характера и степени общественной опасности преступления, обстоятельств его совершения и личности виновного, наоборот, не признавать его отягчающим обстоятельством.

Суть нормы не изменится – состояние опьянения в конкретных случаях будет признаваться отягчающим обстоятельством, но принцип закрытого перечня

будет соблюдён. Также часть 1.1. статьи 63 УК РФ не будет усугублять положение виновного, а наоборот, смягчит его.

Возвращаясь к теме исследования, нами предлагается взять данную модель законодательной конструкции за основу нормы о назначении наказания за киберпреступления.

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:

«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».

Данное нововведение позволит решить множество проблем в правоприменительной практике, дав суду возможность решать, в каком случае киберпространство использовалось для совершения преступления, а в каком нет; в каком случае его использование стало причиной повышенного вреда, а в каком нет; повлияло использование киберпространства на общественную опасность преступления, либо нет. Более того, применение данной нормы сформирует стабильную судебную практику, которая может быть положена в основу Постановления Пленума Верховного Суда Российской Федерации.

Подводя предварительный итог, следует сделать несколько выводов.

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

2. Даётся авторская 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. Экономическим киберпреступлением следует считать киберпреступление, причиняющее вред экономическим отношениям как родовому объекту.

4. Совершение преступления дистанционно с использованием средств компьютерной техники, информационно-телекоммуникационных сетей и киберпространства может являться обстоятельством, повышающим его общественную опасность.

5. Совершение преступления дистанционно с использованием средств компьютерной техники, информационно-телекоммуникационных сетей и киберпространства необходимо включить в перечень обстоятельств, отягчающих наказание, при этом дав суду возможность применять данную норму на своё усмотрение в зависимости от характера и степени общественной опасности преступления, конкретных обстоятельств его совершения и личности виновного.

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

Киберпреступления являются преступлениями международного уровня, поскольку совершаются вне государственных границ. В связи с этим во многих странах мира сформировались собственные представления о противодействии кибер-угрозе. Представляется, что для разработки наиболее эффективных мер противодействия экономическим киберпреступлениям в Российской Федерации

необходимо обратиться к опыту международных организаций и зарубежных стран.

Из-за трансграничного характера киберпреступлений необходимость в международном урегулировании данной проблемы возникла ещё в 70-х, 80-х годах прошлого века. В то время во многих странах (Италия – 1978, Австралия – 1979, Великобритания – 1981, США – 1980, Дания и Канада – 1985, Германия – 1986, Австрия, Япония и Норвегия – 1987, Франция и Греция – 1988) уже существовали первые нормы об установлении уголовной и административной ответственности за совершение компьютерных преступлений. Однако данные нормы были слишком отличны (слишком отличались) друг от друга, они содержали разные определения одного и того же преступления, которые трактовались так же по-разному и зачастую противоречили друг другу. В связи с этим, в целях унификации национальных законодательств, 13 сентября 1989 года на заседании Комитета министров Совета Европы была принята Рекомендация №(89)9, содержащая списки компьютерных правонарушений. Странам-участницам ЕС было рекомендовано на основе принятых списков разработать единую уголовную стратегию борьбы с киберпреступлениями[1].

Первый список содержал «минимальный» перечень правонарушений, запрещенных на территории ЕС. К ним отнесли:

1) компьютерное мошенничество;
2) компьютерный подлог;
3) повреждение компьютерной информации и компьютерных программ;
4) компьютерный саботаж;
5) несанкционированный доступ к компьютерным сетям;
6) несанкционированный перехват данных;

[1]Побегайло А.Э. Киберпреступность: лекция. М., Академия Генеральной прокуратуры Российской Федерации. 2013. С.13.

7) несанкционированное копирование защищённых компьютерных программ[1].

Второй список содержал дополнительный («необязательный») перечень правонарушений, которые страны-участники ЕС могли запретить по своему усмотрению. К ним отнесли:

1) изменение информации или компьютерных программ;

2) компьютерный шпионаж;

3) противозаконное применение компьютера;

4) несанкционированное применение защищенных компьютерных программ[2].

Данная Рекомендация была одной из первых реакций международного сообщества на кибер-угрозу, и, что примечательно, «минимальный» или обязательный перечень правонарушений, запрещённых на территории ЕС возглавило преступление против собственности – компьютерное мошенничество.

Спустя несколько лет, на 93-м пленарном заседании 56-ой сессии Генеральной Ассамблеи ООН, была принята Резолюция №56/261 от 31 января 2002 года, призывающая к усилению борьбы с компьютерной преступностью. В Резолюции было предложено развивать национальные законодательства стран-членов ООН об уголовной ответственности за киберпреступления и разработать комплекс мер по борьбе с преступлениями, связанными с использованием высоких технологий и компьютеров[3]. В этот день проблема киберпреступности вышла за пределы отдельных стран и стала одной из мировых проблем, наравне с международным терроризмом и торговлей наркотиками.

Особую роль в вопросе противодействия международной киберпреступности выполняла «Большая Восьмерка» (G-8). Так, 26 июня 1996 года во Франции, в городе Лионе состоялось очередное собрание «G-8»,

---

[1]Рекомендация Комитета министров Совета Европы №(89)9 от 13.09.1989 [Электронный ресурс] // URL: https://wcd.coe.int/com.instranet.InstraServlet?command=com.instranet.CmdBlobGet&InstranetImage=610660&SecMode=1&DocId=702280&Usage=2 (Дата обращения: 27.01.2013).

[2]Там же.

[3]Резолюция Генеральной Ассамблеи ООН от 31 января 2002 N 56/261 «Планы действий по осуществлению Венской декларации о преступности и правосудии: ответы на вызовы XXI века» (Принята в г. Нью-Йорке на 93-м пленарном заседании 56-ой сессии Генеральной Ассамблеи ООН) // СПС «КонсультантПлюс».

итогом которого стал Регламент №16, согласно которому государства-члены «G-8» должны изменить законодательные нормы, чтобы гарантировать криминализацию и наказуемость деяний, совершаемых с использованием современных технологий. Государства-члены «G-8» договорились об усовершенствовании связи между сотрудниками правоохранительных органов разных стран в целях обмена опытом и содействия в дальнейшей деятельности.

Во исполнение данного Регламента была создана т.н. «Лионская группа», ставшая крупным международным игроком в сфере противодействия киберпреступлениям. Спустя некоторое время, по примеру Германии и Франции, в остальных странах-членах «G-8» были созданы специальные правоохранительные органы, в круглосуточном режиме осуществляющие комплекс мероприятий по развитию международного сотрудничества в борьбе с компьютерной преступностью[1].

К тому времени в Германии в составе Полицейского управления Мюнхена с 1994 года уже существовала специальная Группа по борьбе с преступлениями в сфере высоких технологий, а во Франции – Служба по противодействию злоупотреблениям в сфере высоких технологий.

В России в 1998 году при Бюро специальных технических мероприятий МВД РФ было образовано Управление «К», целью которого является расследование исключительно компьютерных преступлений.

В Великобритании в 2001 году было создано Национальное подразделение по борьбе с преступлениями в сфере высоких технологий, а 1 апреля 2006 года было создано Национальное агентство по борьбе с организованной преступностью. В связи с реформой 2013 года функции по борьбе с компьютерной преступностью были переданы Национальному подразделению противостояния киберпреступлениям[2].

---

[1]Сухаренко А.Н. Современные криминальные вызовы и угрозы информационной безопасности России [Электронный ресурс] // URL: http://sartraccc.ru/Press/special/contr_terror_1_12.pdf (Дата обращения: 5.08.2015).

[2]Сабадаш В.П. Специальные подразделения и организации по борьбе с Интернт-мошенничеством в различных государствах мира. // Библиотека криминалиста.2013. №5(10) С.329.

В 2013 году власти Японии также сообщили о создании отделения полиции по борьбе с компьютерными преступлениями[1].

Европейский союз также отреагировал на проблему киберпреступности, создав целую сеть правоохранительных органов для борьбы с нею: «Европейский центр киберпреступлений» (European cybercrime centre), или «**EC-3**», который состоит из 10 самостоятельных групп и команд, осуществляющих анализ статистических данных, подготовку специальных способов выявления и поимки киберпреступников и саму их поимку[2].

Ещё одним международным актом, направленным на противодействие компьютерным преступлениям, является Будапештская Конвенция Совета Европы «О киберпреступности» от 23 ноября 2001 года. Конвенция подразделяет все киберпреступления на 5 групп:

1. преступления против конфиденциальности, целостности и доступности компьютерных данных и систем (незаконный доступ, перехват; вмешательство в данные и в систему);

2. преступления, связанные с использованием компьютера как средства совершения преступлений, то есть как средство манипуляции информацией (компьютерное мошенничество и подлог);

3. преступления, связанные с контентом, то есть содержанием данных, размещенных в компьютерных сетях (детская порнография);

4. преступления, связанные с нарушением авторского права и смежных прав;

5. акты расизма и ксенофобии, совершённые посредством компьютерных сетей.

В научном сообществе данная Конвенция считается одной из наиболее строгих мер международного противодействия компьютерным преступлениям. Именно по этой причине, на наш взгляд, она и не была подписана Российской

---

[1]Информационный ресурс «Информационная безопасность». [Электронный ресурс] URL:http://www.itsec.ru/newstext.php?news_id=91024 (Дата обращения: 01.09.2013).

[2]Киселёв А.К. Киберпреступность – взгляд из Европы. // Библиотека криминалиста. 2013. №5(10) С.311, 312.

Федерацией. Многие её положения противоречат национальному законодательству России и нарушают её интересы. Например, статьи 29 и 32 данной Конвенции дают возможность осуществлять вмешательство в компьютерные системы другого государства и предпринимать оперативные меры не зависимо от общественной опасности совершенного деяния без разрешения данного государства.

Существуют и другие разногласия касательно данной Конвенции. Так, по мнению О.С. Гузеевой, ещё одной из причин, не позволяющих России присоединиться к Конвенции, является то обстоятельство, что согласно Конвенции в качестве субъектов преступлений могут выступать не только физические, но и юридические лица[1]. По мнению Р.И. Дремлюги, она вовсе не соответствует действующим реалиям уголовного права Российской Федерации и ряда других стран. По его мнению, необходимо принять как минимум две новые Конвенции под эгидой ООН, одна из которых должна быть направлена на унификацию составов киберпреступлений, а вторая – на унификацию процедур правовой помощи и принятие оперативных мер реагирования[2].

К слову, в 2010 году в Бразилии прошел двенадцатый Конгресс ООН, на котором обсуждались вопросы борьбы с компьютерными преступлениями и государственной кибербезопасности. Данный конгресс примечателен тем, что на нём была рассмотрена рекомендация относительно необходимости изучения вопроса киберпреступности и принятия решения по разработке Глобальной Конвенции по борьбе с ней[3].

Представляется, что на международном уровне проблема противодействия компьютерным преступлениям, в том числе и экономическим преступлениям, совершаемым в киберпространстве, стоит весьма остро.

---

[1] Гузеева О.С. Действие Уголовного кодекса России в отношении интернет-преступлений // Законы России: опят, анализ, практика. 2013. №10. С. 16.

[2] Дремлюга Р.И. Международно-правовое регулирование сотрудничества в сфере борьбы с Интернет-преступностью. // Библиотека криминалиста.− 2013. − №5(10) – С.346.

[3] Дубко М. Международное сотрудничество в сфере уголовно-правовой борьбы с неправомерным завладением компьютерной информацией [Электронный ресурс]// URL:http://www.crime-research.ru/articles/Dubko_0001 (Дата обращения: 27.08.2014).

В то время как на международном уровне разворачиваются дискуссии и споры, на национальном уровне многие государства самостоятельно противодействуют компьютерным преступлениям, принимая государственные стратегии кибербезопасности и совершенствуя уголовное законодательство.

Значение стратегий кибербезопасности разных стран сложно переоценить – они являются универсальным маркером, по которому можно проследить, в какие сферы общественной жизни той или иной страны проникла киберпреступность.

Однако, согласно данным Европейского агентства по сетевой информационной безопасности («ENISA»)[1], не во всех странах существует собственная стратегия кибербезопасности. Так, в Российской Федерации национальная стратегия кибербезопасности на сегодняшний день находится лишь в разработке, на этапе составления концепции, что ещё сильнее актуализирует анализ стратегий кибербезопасности разных стран.

Среди самых распространенных направлений государственной политики по борьбе с киберпреступлениями в разных странах стали:

1. защита стратегических и правительственных информационных систем от кибер-атак и актов кибер-терроризма (Германия, Великобритания, Канада, Литва, Люксембург, Нидерланды, США, Эстония);

2. правовое регулирование, а также совершенствование уголовного и информационного законодательства (Германия, Канада, Люксембург, США, Эстония, Японии);

3. защита информации и персональных данных (Словакия, Франция, Чешская Республика, Литва);

4. государственное и международное сотрудничество (Люксембург, США, Япония).

Среди других направлений можно выделить обучение сотрудников правоохранительных органов и информирование граждан о кибер-угрозе

[1] Парламентская библиотека. Государственные стратегии кибербезопасности [Электронный ресурс] // URL: http://www.securitylab.ru/ (Дата обращения: 27.01.2013).

(Люксембург, Эстония) и продвижение международных стандартов экономической безопасности (США, Люксембург).

Из анализа стратегий кибербезопасности разных стран видно, что наиболее общим направлением государственной политики является защита стратегических и правительственных информационных систем, таких как информационная система на объектах атомной энергетики, объектах бюджетной и финансовой сферы, государственных банках, в нефтепромышленном и военно-промышленном комплексе. Следовательно, большинство стран, принявших национальные стратегии кибербезопасности, приняли угрозу от киберпреступлений всерьёз, как угрозу национальной безопасности. По нашему мнению, данный аспект также должен быть учтён в принятии стратегии кибербезопасности Российской Федерации.

Основной мерой противодействия в большинстве случаев является правовое регулирование: совершенствование уголовного, административного и информационного законодательства, криминализация новых деяний, ужесточение ответственности за уже существующие компьютерные преступления.

Законодательство разных стран об экономических киберпреступлениях имеет множество особенностей и отличий, однако существуют нормы, встречающиеся в Уголовных кодексах почти всех стран, к ним можно отнести:

- компьютерное мошенничество или компьютерное хищение;
- получение сведений, составляющих коммерческую тайну путём неправомерного доступа к компьютерной информации (коммерческий шпионаж);
- вымогательство с использованием средств компьютерной техники.

«Компьютерное мошенничество» или «хищение с использованием средств компьютерной техники» есть в уголовном законодательстве большинства стран, в том числе и в Уголовном кодексе Российской Федерации (ст. 159.6 УК РФ). Особенность данного преступления и его основное отличие от обычного мошенничества в законодательстве всех странах отражены по-своему, но суть остаётся одна – это хищение чужого имущества путём использования средств компьютерной техники.

Уголовный кодекс **Белоруссии**[1] в Примечании 1 к Главе 24 «Преступления против собственности» дает определение хищения как «*умышленное противоправное безвозмездное завладение чужим имуществом или правом на имущество с корыстной целью путем кражи, грабежа, разбоя, вымогательства, мошенничества, злоупотребления служебными полномочиями, присвоения, растраты или использования компьютерной техники»*. Другими словами, хищение, совершенное с использованием компьютерной техники, является самостоятельной формой хищения в Республике Беларусь.

Данная форма хищения предусмотрена статьёй 212 УК Белоруссии. Согласно части 1 данной статьи хищение имущества *путем изменения информации, обрабатываемой в компьютерной системе, хранящейся на машинных носителях или передаваемой по сетям передачи данных, либо путем введения в компьютерную систему ложной информации* наказывается штрафом, или лишением права занимать определенные должности или заниматься определенной деятельностью, или арестом на срок до шести месяцев, или ограничением свободы на срок до трех лет, или лишением свободы на тот же срок.

Хищение путем использования компьютерной техники также упоминается в статьях:

- хищение наркотических средств, психотропных веществ и их прекурсоров (ст. 327 УК Белоруссии);
- хищение радиоактивных материалов (ст. 323 УК Белоруссии);
- хищение огнестрельного оружия, боеприпасов или взрывчатых веществ (ст. 294 УК Белоруссии).

В статье 216 УК Белоруссии описаны возможные способы причинения имущественного ущерба без признаков хищения, к которым помимо обмана и злоупотребления доверием отнесена и модификация компьютерной информации.[2]

---

[1]Уголовный кодекс Белоруссии. [Электронный ресурс]// URL:http://etalonline.by/?type=text&regnum=hk9900275#load_text_none_1 (Дата обращения:06.01.2013).

[2] Простосердов, М.А. Преступления, совершаемые в информационном пространстве стран ЕврАзЭС // Информационное пространство Евразэс: правовые основы интеграции: монография / А.А. Арямов, И.В.

Уголовный кодекс **Дании**[1] в статье 279 «а» определяет компьютерное мошенничество (дат. - databedrageri) как «*незаконное изменение, дополнение или стирание информации либо программы, используемой для электронной обработки данных с целью получения для себя или для других лиц незаконной выгоды».*

Уголовный кодекс **Италии** сдержит сразу две статьи о компьютерном мошенничестве (ит. Frode informatica). Статья 640-ter УК Италии посвящена обычному компьютерному мошенничеству, то есть хищению, совершённому путём «вмешательства в работу компьютерных систем», в то время как статья 640-i (1) посвящена пособничеству в компьютерном мошенничестве путём выдачи сертификата электронной подписи[2].

В статье 287 Уголовного кодекса **Китайской Народной Республики** устанавливается ответственность *за использование компьютера для завладения денежными средствами путем мошенничества или иного хищения* (кит. - liyong jisuanji shishi fanzui de tishi). Данная статья является ссылочной и, в зависимости от размера и степени вреда, санкция определяется иными статьями Уголовного кодекса КНР, при этом максимальным видом наказания за совершение данного преступления является смертная казнь[3].

Пункт «а» части 3 статьи 138ab УК **Нидерландов**[4] предусматривает ответственность за «виртуальное мошенничество»**.** Согласно данному пункту «*неправомерное проникновение в компьютер, совершенное через телекоммуникационную инфраструктуру или телекоммуникационное устройство, используемое для обслуживания населения («Интернет») с целью получения для себя незаконных доходов, наказывается лишением свободы на срок*

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

[1]Уголовный кодекс Дании. [Электронный ресурс] // URL: https://www.retsinformation.dk/Forms/R0710.aspx?id=152827#Kap28 (Дата обращения: 27.01.2013).

[2]Уголовный кодекс Италии [Электронный ресурс] // URL:http://www.altalex.com/?idnot=36653 (дата обращения 25.08.2014).

[3]Уголовный кодекс Китайской Народной Республики [Электронный ресурс] // URL: http://constitutions.ru/archives/403 (Дата обращения:06.01.2013).

[4]Уголовный кодекс Нидерландов. [Электронный ресурс] // URL: http://wetten.overheid.nl/BWBR0001854/TweedeBoek/TitelV/Artikel138ab/geldigheidsdatum_29-09-2013 (Дата обращения: 27.01.2013).

до четырех лет или штрафом четвертой категории». Интересен тот факт, что данное преступление расположено в Разделе V «Преступления против общественного порядка».

В раздел XXXV «Преступления против собственности» УК **Республики Польши** включена статья 287, устанавливающая ответственность за «*хищение путём мошенничества, сопровождающегося уничтожением, изменением, модификацией компьютерной информации*»[1].

Закон **США** «О мошенничестве и злоупотреблениях с использованием компьютера» №1030 1986 года устанавливает понятие «мошенничество с использованием компьютера» (англ. – fraud with computers), под которым в пункте (A)(4) понимается «*умышленное, с целью хищения, осуществление неправомерного доступа к защищенному компьютеру или осуществление такого доступа без разрешения*»[2].

Часть 3 статьи 190 Уголовного кодекса **Украины**[3] предусматривает ответственность за мошенничество (укр. – шахрайство) «*путем незаконных операций с использованием электронно-вычислительной техники*».

Ответственность за компьютерное мошенничество предусмотрена в статье 263а УК **ФРГ** (нем. – computerbetrug). Согласно части 1 данной статьи каждый, «*кто действует с целью получения для себя или третьего лица противоправной имущественной выгоды и этим наносит вред имуществу другого лица посредством воздействия на результат обработки данных компьютера, составляя неправильные программы, использования неправильных или неполных данных, несанкционированного применения данных или влияния на такой процесс каким-либо иным неправомочным воздействием, подлежит уголовной*

[1]Лопатина Т.М. Проблемы формирования уголовно-правового способа борьбы с компьютерным мошенничеством. // Библиотека криминалиста.2013. №5(10). С.35.

[2]Свод законодательства США Раздел 18, часть 1, глава 47, §1030 Computer Fraud and Abuse Act (CFAA) [Электронный ресурс] // URL: http://www.law.cornell.edu/uscode/text/18/1030 (Дата обращения: 27.04.2012).

[3]Уголовный кодекс Украины. [Электронный ресурс] // URL: http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=2341-14&p=1214905443606898 (Дата обращения:06.01.2013).

ответственности и наказанию в виде лишения свободы на срок до 5 лет либо в виде штрафа»[1].

В Уголовном кодексе **Эстонии**[2] статья 268 «Компьютерное мошенничество» (эст. – arvutikelmus) расположена в Главе 14 «Преступления в сфере компьютерной информации и обработки данных», согласно которой «*получение чужого имущества, имущественной либо иной выгоды путем ввода компьютерных программ или информации, их модификации, уничтожения, блокирования либо иного вида вмешательства в процесс обработки информации, влияющего на результат обработки информации и обусловливающего причинение прямого имущественного или иного вреда собственности другого лица, наказывается штрафом, или арестом, или лишением свободы на срок от одного года до шести лет».*

В **Южной Корее** мошенничество с использованием компьютера (кор. – keompyuteodeung sayongsagi) предусмотрено статьёй 247-2 Уголовного кодекса. Оно может быть совершено *путем использования информации, введения ложных или ненадлежащим образом обработанных данных в технические средства, включая компьютер*[3].

В **Японии** действует Закон «О несанкционированном проникновении в компьютерные сети» 2000 года. Данный закон не выделяет компьютерное мошенничество как самостоятельный вид преступлений, но устанавливает ответственность за несанкционированное проникновение в компьютерные сети с целью хищения[4].

Как видно, законодатели разных стран пошли различными путями в определении компьютерного хищения: одни признали его в качестве самостоятельного вида хищения, другие выделили в качестве нового вида

---

[1]Уголовный кодекс Германии с изменениями от 28 декабря 2003 года. [Электронный ресурс] URL: http://lexetius.com/StGB/263a (Дата обращения: 20.01.2013).

[2]Уголовный кодекс Эстонии. [Электронный ресурс] URL: http://www.hot.ee/almanach/kriminaalseadustik.html (Дата обращения: 27.01.2012).

[3]Уголовный кодекс Республики Корея. [Электронный ресурс] // URL: http://www.crime.vl.ru/index.php?p=1324&more=1 (Дата обращения:06.01.2013).

[4]Хилюта В.В. Хищение с использованием компьютерной техники или компьютерное мошенничество? // Библиотека криминалиста.2013. №5(10). С.57.

мошенничества, третьи при построении нормы использовали хищение в качестве цели совершения неправомерного доступа к компьютерной информации. Учитывая исторический аспект каждой из стран, а также их юридические традиции, каждый из вариантов имеет право на существование, однако для Российской Федерации наиболее приемлемым, по нашему мнению, являются подходы Белоруссии, чьё уголовное законодательство является наиболее близким нашему.

Ещё одним распространённым составом экономического киберпреступления является «компьютерный коммерческий шпионаж», или получение сведений, составляющих коммерческую тайну путём неправомерного доступа к компьютерной информации.

В статье 478 УК **Испании** предусматривается ответственность за неуполномоченный доступ к компьютерным данным и информации, содержащим коммерческую тайну, совершенный при помощи компьютерных средств[1].

Пунктом (1) части 1 статьи 273 УК **Нидерландов** предусмотрена ответственность за незаконное использование и распространение сведений, содержащих коммерческую тайну, в целях материальной выгоды с помощью компьютерных устройств. Данное деяние наказывается лишением свободы на срок до шести месяцев или штрафом четвертой категории.

В пункте (1) статьи 4 главы 30 УК **Финляндии** в качестве способа совершения коммерческого шпионажа (неправомерного получения сведений, составляющих коммерческую тайну) устанавливается неправомерный доступ к компьютерным системам[2].

Статья 143 УК **Швейцарии** также устанавливает уголовную ответственность за «промышленный шпионаж, совершённый электронным способом»[3].

---

[1]Уголовный кодекс Испании [Электронный ресурс] // URL:http://noticias.juridicas.com/base_datos/Penal/lo10-1995.l2t13.html#a278 (Дата обращения 25.08.2014).

[2]Уголовный кодекс Финляндии [Электронный ресурс] // URL:http://www.finlex.fi/en/laki/kaannokset/1889/en18890039.pdf (Дата обращения 25.08.2014).

[3]Уголовный кодекс Швейцарии [Электронный ресурс] // URL:http://law.edu.ru/norm/norm.asp?normID=1241950&subID=100098712,100098714,100098872,100099140,100099172#text (Дата обращения 25.08.2014).

В Уголовном кодексе Российской Федерации такого состава нет, однако и острой необходимости в его принятии также нет. Дело в том, что в отечественной судебной практике квалификация подобного деяния осуществляется по совокупности преступлений, предусмотренных статьями 183 и 272 УК РФ, как получение или распространение сведений, составляющих коммерческую, налоговую или банковскую тайну и неправомерный доступ к компьютерной информации. При этом такое деяние образует идеальную совокупность, поскольку данные, содержащие коммерческую, налоговую или банковскую тайну, могут быть представлены в виде компьютерной информации, к которой и был осуществлён неправомерный доступ.

Следующим составом киберпреступления, о котором пойдёт речь, является «кибер-вымогательство». Интерес в данном составе вызывает характер угрозы, которым подкреплено требование о передаче денежных средств: угроза заключается в уничтожении компьютерных данных.

Компьютерное вымогательство существует в Уголовном законодательстве **Нидерландов**. Часть 2 статьи 317 УК Нидерландов выступает в качестве примечания к статье о классическом составе вымогательства (голл. – afpersing). Согласно данной статье, «*наказание, предусмотренное в части 1 статьи 317 УК Нидерландов (вымогательство), также применяется к лицу, которое высказывает требования под угрозой повреждения или уничтожения данных, хранящихся на компьютерном устройстве».*

Подобный состав закреплён в пункте (A)(7) Закона №1030 **США:** «вымогательство с использованием компьютера» (англ. – extortion with computers) – «то есть *запрос или требование денег или другого ценного предмета, под угрозой причинения ущерба защищённому компьютеру или под угрозой неправомерного доступа к информации, хранящейся в нем»*. За совершение данного деяния предусмотрено наказание в виде штрафа и/или лишения свободы на срок до 10 лет.

Стоит отметить, что в отечественном уголовном законодательстве на сегодняшний день отсутствует специальная норма о таком вымогательстве и, как

правило, данные деяния квалифицируются по совокупности статей 163 и 272 УК РФ, что создаёт множество проблем в правоприменительной практике, поскольку ни статьёй 163 УК РФ «Вымогательство», ни статьёй 272 УК РФ «Неправомерный доступ к компьютерной информации» не предусмотрен такой признак, как «*угроза повреждения или уничтожения данных, хранящихся на компьютерном устройстве*». Поэтому в данном случае квалификация по совокупности является неверной. Схожая ситуация возникает при совершении преступления, предусмотренного статьёй 179 УК РФ «Принуждение к совершению сделки или к отказу от ее совершения» под угрозой повреждения или уничтожения данных, хранящихся на компьютерном устройстве. Из этого следует вывод, что в отечественном уголовном законодательстве возникла необходимость в новом квалифицирующем признаке.

Помимо данных составов в уголовных кодексах разных стран существуют и другие, более специфические составы экономических киберпреступлений.

Так, статья 148a УК **Австрии**, предусматривает ответственность за *«имущественный вред, причиненный с целью извлечения незаконной выгоды для преступника или третьих лиц, путём влияния на процессы автоматизированной обработки данных с помощью специальных программ, ввода, изменения или уничтожения данных или иным способом, влияющим на процесс обработки данных»*[1]. По своей сути, аналогом данного преступления в Уголовном кодексе Российской Федерации является часть 2 статьи 272 УК РФ – неправомерный доступ к компьютерной информации, причинивший крупный ущерб или совершённый из корыстных побуждений.

Уголовный кодекс **Италии** содержит целый ряд специфических преступлений против собственности, таких как «Причинение вреда компьютерным данным и программам» (статья 635-bis), «Причинение вреда государственным компьютерным данным и программам» (статья 635-b(1)), а также «Повреждение компьютера» (статья 635-c). В отечественном уголовном

[1]Уголовный кодекс Австрии. [Электронный ресурс] // URL: http://www.gesetze-im-internet.de/stgb/ (Дата обращения 25.07.2015).

законодательстве данные преступления, кроме последнего, квалифицируются по части 1 статьи 272 УК РФ как неправомерный доступ к компьютерной информации, повлекший её уничтожение, блокирование или модификацию. Деяние, предусмотренное статьёй 635-с УК Италии, в России квалифицировалось по статье 167 УК РФ как умышленное уничтожение или повреждение чужого имущества.

Часть 1 статьи 216 УК **Украины** криминализирует незаконное изготовление, подделку, использование или сбыт незаконно изготовленных, полученных или поддельных аудиовизуальных произведений, фонограмм, «видеограмм», компьютерных программ. Подобные деяния наказываются штрафом или ограничением свободы на срок до четырех лет. Данное преступление содержится в Разделе VII «Преступления в сфере хозяйственной деятельности», который является аналогом Главы 22 УК РФ. В отечественном законодательстве такого состава нет.

Часть 2 статьи 314 **Южнокорейского** Уголовного кодекса регулирует ответственность за препятствия в бизнесе (кор. – eobmubanghae), то есть *за препятствие бизнесу другого лица путём повреждения или разрушения устройств, включая компьютер, либо данных, включая электромагнитные (компьютерные) данные, либо путём неправомерного доступа к информационному устройству*. На наш взгляд, в Российской Федерации данное деяние также следует квалифицировать по части 2 статьи 272 УК РФ как неправомерный доступ к компьютерной информации, причинивший крупный ущерб или совершённый из корыстных побуждений.

Помимо уголовно-правового регулирования, в качестве мер противодействия киберпреступлениям в зарубежных странах применяются и иные, зачастую более эффективные меры. Так, проблема анонимности пользователей киберпространства, являющаяся одной из причин существования киберпреступности, в некоторых странах решена на административном уровне. К примеру, после террористического акта 11 марта 2004 года в Милане итальянские власти обязали всех пользователей Интернет-кафе и общественных точек доступа

в сеть «Интернет» предъявлять паспорт или идентификационную карту[1]. Без предъявления таких документов сотрудники Интернет-кафе не имеют права предоставить пользователю доступ в сеть.

Похожим путём пошли власти **Китайской Народной Республики** в 2011 году. Каждый пользователь китайского сегмента информационного пространства при регистрации в социальных сетях и на других сайтах обязан вводить паспортные данные, иначе доступ к таким сайтам для этого пользователя будет закрыт. Такие меры были вызваны распространением клеветы, недобросовестной рекламы и мошенничества в киберпространстве КНР. Они сильно повлияли на внешний облик киберпространства Китая, фактически уничтожив свободу общения. Однако свой вклад в противодействие киберпреступности данные нововведения внесли – уровень киберпреступности в социальных сетях Китая резко снизился[2].

Представляется, что нормативное регулирование на сегодняшний день остаётся самой распространённой мерой противодействия киберпреступлениям во всех странах, в то время как другие меры (повышение финансирования правоохранительных органов, обучение их сотрудников и информирование граждан) применяются скорее как дополнительные и сопутствующие.

В целом международный и зарубежный опыт противодействия киберпреступности можно охарактеризовать как несогласованный и поэтому малоэффективный. Разные страны по-разному определяют компьютерные преступления, в одних государствах деяние криминализировано уже более 30 лет, в то время как в других оно остаётся законным. На международном уровне принимаются конвенции, носящие скорее политический, нежели правовой характер, ратифицировать которые не представляется возможным.

В то же время на национальных уровнях сложились свои направления уголовно-правовой политики противодействия киберпреступности и подходы

---

[1]Газета Белла-Италия [Электронный ресурс] // URL: http://bellaitalia.at.ua/news/svjaz_v_italii/2012-11-05-94 (Дата обращения:06.01.2013).

[2]Информационный ресурс «China Space». [Электронный ресурс] //URL: http://www.chinaspace.ru/internet-tolko-po-pasportu/ (Дата обращения: 06.01.2013).

построения уголовно-правовых норм. В одних странах принимаются новые, специальные нормы о том или ином традиционном преступлении, ставшим киберпреступлением (Дания, США, ФРГ, Эстония), в то время как в других расширяется само понятие преступления добавлением нового способа его совершения (Белоруссия, Украина).

Первый подход, на наш взгляд, является самым простым, но сомнительным, поскольку он может привести к тому, что помимо простого уголовного кодекса в каждой стране фактически появится второй закон о компьютерных преступлениях, поскольку почти каждое преступление можно совершить с использованием киберпространства. Как справедливо указывают В.Н. Черкасов, К.П. Семёнов и А.Э. Симонова, следуя такой логике в УК РФ необходимо будет ввести киберклевету, кибершпионаж, киберхалатность и так до исчерпания уголовно-правовых норм[1].

Второй подход, на наш взгляд, более оптимален для Российской Федерации. Криминализация общественно опасного деяния в самостоятельной статье необходима лишь в случае, если деяние уникально и не является разновидностью другого преступления. При появлении нового способа совершения преступления необходимо учесть, влияет ли он на общественную опасность деяния, и только в положительном случае выделить его как квалифицирующий признак или обстоятельство, отягчающее наказание.

Основываясь на вышесказанном, можно сделать следующие выводы:

1. наиболее общим направлением государственной политики разных стран является защита стратегических и правительственных информационных систем, таких как информационная система на объектах атомной энергетики, объектах бюджетной и финансовой сферы, государственных банках, в нефтепромышленном и военно-промышленном комплексе. По нашему мнению,

[1]Черкасов В.Н. Информационные технологии и организованная преступность [Электронный ресурс] // URL: http://www.crime-research.ru/library/Cherkas03.html (Дата обращения:20.01.2015); Семёнов К.П., Симонова А.Э. законодательное регулирование и уголовно-правовая защита информационных правоотношений: состояние и перспективы. // Информационная безопасность регионов. 2011. № 2(9). С 93.

данный аспект должен быть учтён в принятии Стратегии кибербезопасности Российской Федерации;

2. основной мерой противодействия в большинстве стран является правовое регулирование: совершенствование уголовного, административного и информационного законодательства, криминализация новых деяний, ужесточение ответственности за уже существующие компьютерные преступления;

3. самыми распространёнными составами экономических киберпреступлений в уголовном законодательстве разных стран являются: компьютерное мошенничество (или компьютерное хищение); получение сведений, составляющих коммерческую тайну, путём неправомерного доступа к компьютерной информации (коммерческий шпионаж); вымогательство с использованием средств компьютерной техники;

4. криминализация всё новых составов киберпреступлений является неверным решением для уголовного законодательства Российской Федерации. Более эффективным и здравым решением, на наш взгляд, было бы его совершенствование, расширяющее понятия «хищение», «вымогательство» и так далее, а также учитывающее использование средств компьютерной техники в качестве обстоятельства, отягчающего наказание.[1]

[1] 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.

ГЛАВА 2
УГОЛОВНО-ПРАВОВАЯ ХАРАКТЕРИСТИКА ЭКОНОМИЧЕСКИХ ПРЕСТУПЛЕНИЙ, СОВЕРШАЕМЫХ В КИБЕРПРОСТРАНСТВЕ

§1. Общая характеристика экономических преступлений, совершаемых в киберпространстве

Под экономическими киберпреступлениями в настоящей работе понимаются исключительно преступления, совершаемые дистанционно, путём использования средств компьютерной техники, информационно-телекоммуникационных сетей и образованного ими киберпространства, имеющие родовым объектом экономические отношения. Такие преступления, как неправомерный доступ к компьютерной информации, причинивший крупный ущерб или совершённый из корыстной заинтересованности (ч. 2 ст. 272 УК РФ), и иные компьютерные преступления, где экономические отношения выступают в качестве дополнительного объекта, не являются предметом данного диссертационного исследования. Ряд преступлений, предусмотренных разделом VIII УК РФ, также не являются предметом исследования, так как их совершение в киберпространстве невозможно. К таким преступлениям можно отнести кражу (ст. 158 УК РФ), грабёж (ст. 161 УК РФ), разбой (ст. 162 УК РФ), сбыт поддельных кредитных либо расчетных карт (ст. 187 УК РФ), незаконный оборот драгоценных металлов, природных драгоценных камней или жемчуга (ст. 191 УК РФ), сбыт поддельных денег или ценных бумаг (ст. 186 УК РФ), злоупотребление полномочиями (ст. 201 УК РФ) и другие.

В связи с этим общая характеристика оставшихся составов позволит выделить экономические киберпреступления в отдельную группу, определить специфические признаки, характерные для всех преступлений данной группы и для каждого преступления, в частности, а также провести их классификацию. Представляется, что наиболее эффективным подходом для общей характеристики

экономических преступлений, совершаемых в киберпространстве, является анализ их составов по обязательным и факультативным признакам.

Объект и предмет. Как было сказано ранее, киберпреступления могут представлять угрозу разным общественным отношениям, а не только отношениям в сфере компьютерной информации. Это связано с тем, что в киберпространстве существует возможность совершения двух видов киберпреступлений: одно- и двухобъектных. В первом случае виновный причиняет вред одной группе общественных отношений (экономическим отношениям), во втором – сразу двум (экономическим отношениям и отношениям в сфере компьютерной информации).

Представляется, что родовым объектом всех экономических преступлений, совершаемых в киберпространстве, следует признать экономические отношения, обеспечивающие материальное благосостояние личности, общества и государства, поскольку на них направлено общественно опасное деяние и именно им причиняется вред в первую очередь. Видовым объектом, в зависимости от конкретного состава, могут выступать отношения собственности (ст. 159, 159.6, 160, 163 УК РФ), отношения в сфере экономической деятельности (ст. 171, 171.2, 172, 183 УК РФ и др.). В зависимости от способа совершения преступления дополнительным объектом может выступать совокупность общественных отношений по правомерному и безопасному использованию компьютерной информации, а также общественная безопасность и общественный порядок[1].

На основании вышеизложенного можно привести следующую классификацию экономических преступлений, совершаемых в киберпространстве по видовому объекту посягательства:

[1]Подробнее см.: Желудков М.А. Новый взгляд на концепцию объекта защиты от корыстных преступлений против собственности // Вестник Воронежского института МВД России. 2011. №1. С.47-51; Краснопеев В.А. Объект преступления в российском уголовном праве: теоретико-правовой анализ: дис. ... канд. юрид. наук. Кисловодск, 2001.С. 30-37; Семченков И.П. Объект преступления: социально-философские и методологические аспекты проблемы: дис. ... канд. юрид. наук. М., 2003. С.47-53; Таций В. Я. Проблема ответственности за хозяйственные преступления: объект и система: дис… докт. юрид. наук. Харьков, 1984. С.7-18; Павлов С.Н. Объект и последствия преступления в теории уголовного права: дис. ... канд. юрид. наук. Ростов-н/Д., 2011. С. 40-42; Шульга А. В. Объект и предмет преступления против собственности в условиях рыночных отношений и информационного общества: дис... докт.юрид.наук. Волгоград, 2008. С. 49-67.; Мазуренко Е.А. Объект и предмет уголовно-правовой охраны преступлений против собственности: современные проблемы квалификации. дис. ... канд. юрид. наук. М., 2003. С.50-57.; Вишнякова Н.В. Объект и предмет преступлений против собственности: дис… канд. юрид. наук. Омск, 2003. С.90

А) киберпреступления против собственности**,** к которым можно отнести:

•хищения – мошенничество (ст. 159 УК РФ), мошенничество в сфере кредитования (ст. 159.1 УК РФ); мошенничество в сфере компьютерной информации (ст. 159.6 УК РФ), присвоение и растрата (ст. 160 УК РФ);

•иные преступления против собственности – вымогательство (ст. 163 УК РФ), причинение имущественного ущерба путём обмана и злоупотребления доверием (ст. 165 УК РФ), умышленное уничтожение или повреждение чужого имущества (с. 167 УК РФ);

Б) киберпреступления в сфере экономической деятельности**,** к которым можно отнести:

•преступления против интересов предпринимательства – незаконное предпринимательство (ст. 171 УК РФ); незаконные организация и проведение азартных игр (ст. 171.2 УК РФ); незаконная банковская деятельность (ст. 172 УК РФ); незаконное получение кредита (ст. 176 УК РФ); легализация (отмывание) денежных средств или иного имущества, полученных преступным путём (ст. 174, 174.1 УК РФ);

•преступления против свободной и добросовестной конкуренции – принуждение к совершению сделки или к отказу от ее совершения (ст. 179 УК РФ); незаконное использование средств индивидуализации товаров, работ и услуг (ст. 180 УК РФ); незаконное получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну (ст. 183 УК РФ); неправомерное использование инсайдерской информации (ст. 185.6 УК РФ);

•иные преступления в сфере экономической деятельности – фальсификация Единого государственного реестра юридических лиц, Реестра владельцев ценных бумаг или системы депозитарного учета (ст. 170.1 УК РФ); манипулирование рынком (ст. 185.3 УК РФ); совершение валютных операций по переводу денежных средств в иностранной валюте или валюте Российской Федерации на счета нерезидентов с использованием подложных документов (ст. 193.1 УК РФ); сокрытие денежных средств либо имущества организации или индивидуального предпринимателя, за счет которых должно производиться взыскание налогов и

(или) сборов (ст. 193.2 УК РФ); фиктивное банкротство (ст. 197 УК РФ); уклонение от уплаты налогов и (или) сборов с физического лица (ст. 198 УК РФ); уклонение от уплаты налогов и (или) сборов с организации (ст. 199 УК РФ).

Предмет киберпреступлений может отличаться от предмета аналогичных преступлений, совершаемых в материальном мире, и иметь свои особенности[1]. Поскольку киберпространство является сферой деятельности в информационном пространстве, т.е. некой виртуальной реальностью, то такие общественно опасные деяния, как, например, хищения (ст. 159, 159.6, 160 УК РФ), не могут быть направлены на изъятие конкретных материальных предметов (бумажник, телефон, автомобиль), поскольку они просто не могут существовать в киберпространстве. Однако данные преступления могут быть направлены на другие предметы, обладающие такой же экономической значимостью, существование которых возможно в цифровой среде (безналичные и электронные денежные средства, криптовалюта). В то же время киберпространство даёт доступ к таким материальным предметам, как компьютер, планшет или смартфон, которые при определённых навыках можно умышленно повредить или вовсе уничтожить (ст. 167 УК РФ).

В связи с этим, на наш взгляд, подробнее стоит остановиться на таких предметах экономических киберпреступлений, как электронные деньги и криптовалюта.

Электронные деньги, распространенные в цифровом мире, несмотря на используемый термин, как таковыми деньгами не являются[2]. Как указывает

---

[1]Подобнее см.: Бикмурзин М.П. Предмет преступления: теоретико-правовой анализ: дис… канд. юрид. наук. Уфа, 2005. С. 3-15; Мазуренко Е.А. Объект и предмет уголовно-правовой охраны преступлений против собственности: современные проблемы квалификации. дис. ... канд. юрид. наук. М., 2003. С. 8-12; Спиридонова О.Е. Символ как предмет преступления: дис… канд. юрид. наук. Ярославль, 2002. С 5-10; Герасимова Е.В. Предмет хищения в российском уголовном праве: дис…канд.юрид.наук. М., 2006.С. 6-8

[2]Подробнее см.: Рищенко Д.В. Рынок информационного продукта: особенности и методизмы функционирования. дис... канд. экон. наук. М., 1996. С.72-90; Егиазарян Ш. П. Электронные деньги в современной системе денежного оборота: дис... канд.экон.наук. М., 1999. С.52-60; Горюков Е. В. Электронные деньги: анализ практики использования и прогноз развития: дис... канд.экон.наук. Иваново, 2004. С.46-50.; Гарькуша М. С. Электронные деньги как феномен виртуальной экономики: функции и способы институционализации: дис... канд.экон.наук. Краснодар, 2010. С 120; Станицкий С.С. Мобильные деньги как средство осуществления расчётов в информационной экономике: дис... канд.экон.наук. М., 2003. С.90-101; Кочергин Д. А. Современные системы электронных денег: дис...докт.экон.наук. СПб., 2006. С.72-80; Малиев С. О. Электронные деньги и платёжные системы на их основе: автореф. дис... канд.экон.наук. СПб., 2008. С.10-15; Гейцан Б. В. Совершенствование рыночного механизма электронных платежей: дис... канд.экон.наук. М., 2008. С.20-37.

В.О. Рябов, с юридической и финансовой точки зрения на сегодняшний момент электронные деньги представляют собой «или чеки, или подарочные сертификаты, или другие подобные платежные средства, в зависимости от юридической модели системы и ограничений местного законодательства. Электронные деньги могут эмитироваться банками, НКО или другими организациями»[1].

С данным мнением стоит согласиться – действительно, с одной стороны, электронные деньги являются средством платежа и могут быть использованы для оплаты услуг, выходящих за пределы киберпространства: коммунальных услуг, услуг операторов мобильной и стационарной телефонной связи. Электронные деньги активно используются в игровой Интернет-индустрии («Steam», «World of Tanks», «The Elder Scrolls Online»). Электронными деньгами можно оплачивать покупки, как через сеть, так и в материальном мире (при наличии специальной платёжной карты). С другой стороны, электронные деньги нельзя увидеть или взять в руки, то есть они являются лишь абстрактным обязательственным правом требования. Другими словами, электронные деньги – это лишь денежные обязательства эмитента, которые должны быть исполнены, в конечном счете, уже в реальной валюте.

На сегодняшний момент правовой режим электронных денег регулируется Федеральным законом «О национальной платёжной системе». Согласно пункту 18 статьи 3 данного Федерального закона они признаны в России в качестве денежных средств[2]. Однако электронные деньги стоит отличать от безналичных денежных средств, так как они не являются заменителем простых денег, а представляют собой денежные средства, эмитированные какой-либо организацией, в то время как простые безналичные денежные средства эмитируются лишь Центральным банком Российской Федерации. Другими словами, электронные деньги – это лишь заменитель реальных денежных средств,

[1]Рябов В.О. Электронные деньги в России. Проблемы использования и регулирования. // Креативная экономика. 2010. № 9(45). С. 31-37.

[2]Федеральный закон от 27.06.2011 N 161-ФЗ (ред. от 25.12.2012) «О национальной платежной системе» // Собрание законодательства РФ. 2011. N 27. Ст. 3872.

в то время как безналичные деньги – это денежный субинститут и прямой взаимосвязи между ними нет.

Следовательно, электронные деньги обладают экономической и юридической значимостью, однако их нельзя потрогать, поскольку они лишены какого-либо материального выражения – это лишь денежное обязательство, запись о котором хранится в электронной форме. В связи с этим совершить кражу электронных денег нельзя, поскольку их физически невозможно изъять, однако их можно обратить. При этом причиняется реальный ущерб отношениям собственности, а значит, электронные деньги могут быть предметом хищения (основной состав мошенничества, мошенничества в сфере компьютерной информации, присвоения либо растраты).

Следовательно, такой признак предмета хищения, как материальность, в киберпространстве становится весьма условным. Киберпространство a priori не материально и любой предмет внутри него также материальным быть не может. Электронные деньги, с технической точки зрения, - это лишь совокупность нулей и единиц, однако именно они дают их обладателю имущественные права, они могут принадлежать гражданину, организации или государству и могут приниматься как средство платежа в Российской Федерации и множестве других стран. Но с развитием информационных технологий появился новый финансовый феномен – криптовалюта, который не подпадает ни под понятие безналичных денежных средств, ни под понятие электронных денег.

Криптовалюта – это денежный суррогат, эмиссия и учёт которого основаны на криптографических методах шифрования компьютерной информации. На сегодняшний день в киберпространстве существует более 80 криптовалют, самыми популярными из которых являются «Биткойн» (BTC), «Лайткойн» (LTC), «Неймкойн» (NMC), «PPCoin» (PPC), «Кварт» (QRK), «Догикойн» (Dogecoin).

В Информационном сообщении «Об использовании криптовалют» Федеральной службы по финансовому мониторингу Российской Федерации выделяется несколько основных признаков криптовалюты:

•во-первых, процесс выпуска и обращения наиболее распространенных криптовалют полностью децентрализован и отсутствует возможность его регулирования, в том числе со стороны государства;

•во-вторых, анонимность пользователей таких криптовалют;

•в-третьих, криптовалюта не требует ведения специальной отчетной документации[1].

По своей природе любая криптовалюта – это уникальное цифровое число, представленное в форме компьютерной информации. Данное число используется как денежный эквивалент в киберпространстве: на него можно что-либо купить либо обменять на настоящие деньги, поскольку у каждой криптовалюты есть собственный курс. Однако в связи с природой криптовалюты возникает серьёзная теоретическая проблема: поскольку любая криптовалюта это компьютерная информация, то может ли она являться предметом хищения?

В науке уголовного права принято считать, что предмет хищения должен обладать тремя основными признаками[2]. Первый – экономический признак: предмет хищения должен иметь определённую экономическую значимость, то есть иметь стоимость. Второй – материальный признак: предмет хищения должен быть предметом материального мира, то есть вещным имуществом либо правом на него. Третий – юридический признак: предметом хищения может быть только чужое имущество (право на имущество), то есть не принадлежащее виновному. Только при наличии всех трёх признаков можно утверждать, что данный предмет может быть предметом хищения.

---

[1]Информационное сообщение Росфинмониторинга «Об использовании криптовалют» // СПС «КонсультантПлюс».

[2]См.: Бойцов А.И. Преступления против собственности. СПб., Юридический центр ПРЕСС. 2002.С.104; Зубова М. А. Компьютерная информация как объект уголовно-правовой охраны: дис. канд. юрид. наук. Казань, 2008. С.50-59.; Шульга А. В. Объект и предмет преступления против собственности в условиях рыночных отношений и информационного общества: дис… докт.юрид.наук. Волгоград, 2008. С.40-49; Челноков В. В. Компьютерная информация как предмет преступления в отечественном уголовном праве: автореф. дис. канд. юрид. наук. Екатеринбург, 2013. С. 9-18.; Яни П.С. Посягательства на собственность. М., Библиотека российского судьи.1998. С.40-42.; Яшков С.А. Информация как предмет преступления: дис…. канд. юрид. наук. Екатеринбург, 2005. С.69.

Криптовалюта, безусловно, обладает стоимостью. Этот факт можно увидеть на примере «Биткойн» (или сокращённо BTC)[1]. «Биткойн» (от англ. «Bit» – бит, т.е. мера исчисления информации, и «coin» – монета) – это криптовалюта с открытым исходным кодом, не имеющая банка-эмитента, созданная лицом (или группой лиц) под псевдонимом «Сатоши Накамото». Известно, что она использует технологию P2P (peer-to-peer), аналогичную общеизвестным «торрентам». Чтобы заработать 1 BTC пользователи системы «Биткойн» предоставляют вычислительную мощность своего компьютера, а система взамен начисляет на электронный кошелёк пользователя определённую сумму BTC.

Изначально стоимость такой криптовалюты составляла примерно 0,3 цента США за 1 BTC, однако из-за открытого исходного кода и простоты система стала довольно популярной, и стоимость BTC резко выросла. Пиковая стоимость BTC была зафиксирована 4 декабря 2013 года и составляла 1240 долл. США за 1 BTC**.** При этом общая сумма всех криптовалют в мире (включая BTC) на 2015 год составляет примерно 5 млрд. долларов США.

BTC отличаются от электронных и безналичных денег тем, что они ничем не обеспечены и по своей природе не являются долговым обязательством, так как в мире нет банка-эмитента, который выпускает эту валюту. Трансакции BTC мгновенные, анонимные и проходят по всему миру, при этом за них не взимается комиссия. Другими словами, система «Биткоин» – это аналог финансовой пирамиды, а BTC – это «электронные фантики», купленные за реальные деньги. Стоимость им придают сами люди на торгах и биржах. Аналогичное мнение было высказано в Заявлении Банка России от 27 января 2014 года «Об использовании при совершении сделок "виртуальных валют", в частности, Биткойн»: «Операции по так называемым «Биткойнам» носят спекулятивный характер, осуществляются на так называемых "виртуальных биржах" и несут высокий риск потери стоимости. Банк России предостерегает граждан и юридических лиц … от

[1]Официальный сайт системы «Биткойн». [Электронный ресурс] // URL: http://bitcoin.org/ru/ (Дата обращения: 27.08.2013).

использования «виртуальных валют» для их обмена на товары (работы, услуги) или на денежные средства в рублях и в иностранной валюте»[1].

Однако при всём этом невозможно отрицать тот факт, что криптовалюта обладает экономической значимостью, поскольку, во-первых, её можно обменять на реальные деньги (как на рубли, так и на иностранную валюту), во-вторых, её можно обменять на разнообразные товары и использовать для оплаты различных услуг и работ.

Второй вопрос, на который необходимо ответить при анализе криптовалюты как предмета хищения, – является ли криптовалюта вещным имуществом? Для ответа на него необходимо обратиться к гражданскому законодательству.

Согласно статье 128 ГК РФ к объектам гражданских прав относятся вещи, включая наличные деньги и документарные ценные бумаги, иное имущество, в том числе безналичные денежные средства, бездокументарные ценные бумаги, имущественные права; результаты работ и оказание услуг; охраняемые результаты интеллектуальной деятельности и приравненные к ним средства индивидуализации (интеллектуальная собственность); нематериальные блага.

Представляется, что криптовалюту можно было бы отнести к деньгам (валюте). Так, 6 августа 2013 года суд Восточного округа штата Техас принял решение: «Поскольку «Биткойн» можно использовать в качестве денег для оплаты за товары или обменять на обычные валюты, то «Биткойн» является валютой или формой денег»[2]. Также 21 марта 2014 года швейцарским парламентом был принят законопроект, согласно которому «Биткойн» следует рассматривать как иностранную валюту[3].

Сегодня криптовалюту можно обменять не только на привычные деньги (рубли, доллары или евро), но и на различные товары или услуги. Так,

---

[1]Информация Банка России от 27 января 2014 «Об использовании при совершении сделок «виртуальных валют», в частности, Биткойн» // СПС «КонсультантПлюс».

[2]Официальный сайт информационного агентства «Russia Today» [Электронный ресурс] // URL: http://rt.com/usa/bitcoin-sec-shavers-texas-231/ (Дата обращения: 5.04.2015).

[3]Официальный сайт Парламента Швецарии [Электронный ресурс] // URL: http://www.parlament.ch/e/suche/Pages/geschaefte.aspx?gesch_id=20134070 (Дата обращения: 5.04.2015).

Университет Никосии в качестве оплаты обучения принимает BTC[1]; компания «Virgin Galactic» осуществляет авиаперевозки за криптовалюту; «Ламборджини» продаёт свои автомобили за «Биткойн»[2], как и американская компания «Philipp Preuss» – недвижимость[3]. Однако подавляющее большинство услуг, за которые принимается криптовалюта, осуществляются лишь в киберпространстве – это, как правило, хостинг, оплата онлайн-игр и иных услуг.

Как указывает академик РАЕН А.А. Фатьянов, криптовалюта – это «хорошо защищённый файл, признанный платёжной единицей… (аналог нынешнего наличного оборота) ... прообраз настоящих электронных денег отдалённого будущего»[4].

Проанализировав сложившуюся ситуацию, можно сделать вывод: криптовалюта однозначно является средством платежа. Однако только лишь это не делает её настоящими деньгами. Основные причины, по которым нельзя признать криптовалюту деньгами, это то, что она эмитируется децентрализовано, и не существует субъекта, обеспечивающего её платёжеспособность. Напомним, что в Российской Федерации эмиссия криптовалют запрещена, поскольку они приравнены к денежным суррогатам, т.е. самовольно введённым денежным знакам, не предусмотренным действующим законодательством[5]. При этом запрета на оборот криптовалюты как такового нет. Так, например, председатель «Сбербанка России» Г.О. Греф признался о наличии у него некоторого количества BTC, а Президент России Владимир Владимирович Путин допустил возможность использования криптовалюты в некоторых IT-сферах[6]. По нашему мнению, стоит

[1]Официальный сайт «Итар-тасс» [Электронный ресурс] // URL: http://itar-tass.com/ekonomika/ 783989 (Дата обращения: 5.04.2015) .

[2]Форум «Ламборджини » [Электронный ресурс] // URL: http://lamborghininewportbeach.blogspot.ru/2013/12/the-bitcoin-saga-continues.html (Дата обращения: 5.04.2015).

[3]Информационный ресурс «The Wall Street Journal» [Электронный ресурс] // URL: http://blogs.wsj.com/developments/2013/12/17/hamptons-seller-tries-new-pitch-buy-my-house-in-bitcoin/?mod=WSJ_3Up_RealEstate (Дата обращения: 5.04.2015).

[4]Фатьянов А.А.Правовой анализ категории «электронные денежные средства» в российском законодательстве. Гражданское общество в России и за рубежом. 2014.N 3. // СПС «КонсультантПлюс».

[5]Информация Банка России от 27 января 2014 «Об использовании при совершении сделок «виртуальных валют», в частности, Биткойн» // СПС «КонсультантПлюс».

[6] Официальный сайт «Бизнес ФМ» [Электронный ресурс] // URL:http://bfm.ru/news/303135; URL:http://bfm.ru/news/303004. (Дата обращения: 4.10.2015)

согласиться с А.А. Фатьяновым: криптовалюта – это «прообраз денег отдалённого будущего», но пока – неполноценные деньги.

Раз криптовалюту нельзя отнести к деньгам, то чем же она является? Криптовалюта имеет нечто общее с бездокументарными ценными бумагами (БЦБ), переход права собственности на которые связан не с получением ценной бумаги, а с внесением приходной записи по лицевому счёту нового владельца с помощью ЭВМ. Однако между этими понятиями существуют серьёзные отличия. По своей природе БЦБ – это лишь запись в реестре владельцев ценных бумаг, фиксирующая имущественное право, то есть предмет преступления – это не запись, а само право[1]. Следовательно, БЦБ по своей природе не могут быть признаны предметом хищения. Криптовалюта – нечто иное, это не просто запись, которая фиксирует имущественное право, а это уникальный файл, обладающий собственной стоимостью.

Наиболее верным, на наш взгляд, было бы решение считать криптовалюту «иным имуществом» в рамках статьи 128 ГК РФ.

Каждая единица криптовалюты индивидуально определена. Это уникальное, очень длинное число, содержащееся в защищённом компьютерном файле. Одновременно двух таких единиц быть не может. Следовательно, приобретая криптовалюту за реальные (настоящие) деньги, покупатель приобретает уникальную индивидуально определённую вещь, имеющую коммерческую ценность, то есть товар.

Как справедливо отметил А.И. Савельев, «вряд ли можно оспаривать тот факт, что объекты, обладающие качеством товара, т.е. коммерческой ценностью и приобретающиеся за деньги, не заслуживают того, чтобы не быть причисленными к объектам гражданских прав, хотя бы в качестве иного имущества»[2].

Соглашусь с мнением А.И. Савельева. Включение криптовалюты в объект гражданских прав в качестве иного вещного имущества «не нарушит стройности

---

[1]Ветошкина М.М. Ценные бумаги как предмет хищения: дис. … канд.юрид.наук. Екатеринбург, 2001. С.74.

[2]Савельев А.И. Правовая природа виртуальных объектов, приобретаемых за реальные деньги в многопользовательских играх. Вестник гражданского права. 2014. N 1. // СПС «КонсультантПлюс».

гражданско-правовых конструкций и связанных с ним догматических построений»[1].

Даже если этот товар (криптовалюта) представлен в форме компьютерной информации (файла), невозможно отрицать факт, что его приобрели за реальные деньги. Следовательно, причинение ущерба криптовалюте может быть выражено в средствах, за которые эта криптовалюта была приобретена. Так, при списании BTC на сумму 1 000 рублей без ведома собственника происходит не просто неправомерный доступ к компьютерной информации из корыстных побуждений, а самое настоящее хищение путём неправомерного безвозмездного обращения в пользу виновного 1 000 рублей в форме BTC, причиняющее вред собственнику. Законный собственник BTC больше не может их использовать, поскольку просто не имеет к ним доступ, в то время как злоумышленник, наоборот, может свободно осуществлять любые финансовые операции с похищенной криптовалютой.

Представляется, что в данном примере общественно опасное деяние причиняет ущерб не столько отношениям, складывающимся по поводу нормального оборота компьютерной информации, сколько отношениям собственности. Действия виновного направлены на завладение чужим имуществом – криптовалютой, а не просто каким-то компьютерным файлом.

С точки зрения гражданского права можно говорить как минимум о неосновательном обогащении (ст. 1102 ГК РФ). Следовательно, у виновного возникает обязанность возвратить неосновательное обогащение либо в натуре (ст. 1104 ГК), т.е. вернуть саму криптовалюту, либо возместить стоимость неосновательного обогащения (ст. 1105 ГК РФ).

Поскольку оборот криптовалюты в России запрещён, то наиболее верным решением, на наш взгляд, является на основании экспертного заключения определить стоимость похищенной криптовалюты и в порядке статьи 1105 ГК РФ возместить её стоимость.

Признав криптовалюту объектом вещного права в качестве «иного имущества», будет возможным защитить права её владельцев,

[1] Там же.

как в гражданском (ст. 1102, 1104, 1105 ГК РФ), так и в уголовном порядке (ст. 159, 159.6, 160 УК РФ).

Учитывая тот факт, что по смыслу статьи 128 ГК РФ криптовалюту можно отнести к категории «иное имущество», она может быть признана предметом хищения, поскольку обладает всеми признаками товара (имеет собственную экономическую стоимость и может быть обменена на реальный деньги).

С данным мнением согласно 56% (54 чел.) опрошенных судей районных и областных судов Российской Федерации, при этом 27% высказались против, а 17% затруднились ответить.[1]

В научной литературе мнение о расширении предмета хищения, включив в него экономически значимую компьютерную информацию, высказывалось уже неоднократно, однако данное положение всё ещё остаётся весьма актуальным. Так, А.В. Шульга считает, что предметом преступления следует признать не только материальные, но и другие блага, в которых проявляются общественные отношения и воздействуя на которые субъект изменяет эти отношения. По его мнению, предметом преступления против собственности (например, хищения) может быть информация имущественного характера, обладающая экономической значимостью[2]. Сходное мнение высказывает А.И. Бойцов. Он указывает, что «обладая экономической ценностью, но при этом оставаясь по своей природе информацией, информационные продукты находятся на грани между понятиями «имущество» и «неимущественное благо»[3].

Компьютерная информация сегодня пока не признана предметом хищения. Это связано как с консерватизмом существующей теории уголовного права, так и с рядом объективных причин. Не вся компьютерная информация может обладать стоимостью сама по себе, как, например, метаданные (т.е. сведения о компьютерных данных), текстовый файл или просто электронная переписка – это всего лишь простая информация, представленная в цифровой форме.

---

[1] См.: Приложение №2. Опросный лист.

[2] Шульга А. В. Объект и предмет преступления против собственности в условиях рыночных отношений и информационного общества: дис… докт. юрид. наук. Волгоград, 2008. С.118-135.

[3] Бойцов А.И. Преступления против собственности. СПб., Юридический центр ПРЕСС. 2002. С.118.

Также возникают споры с авторскими и смежными правами. Например, в случае если виновный без ведома собственника скачает компьютерную программу и будет ею пользоваться, то такое деяние нельзя квалифицировать как хищение – это неправомерный доступ к компьютерной информации и незаконное использование объектов авторского права. Ничего не изымается и не обращается – преступник просто использует компьютерную программу и не платит за это.

Представляется, что компьютерная информация сама по себе не может являться предметом хищения, пока она не преобразована в конкретный цифровой информационный продукт, обладающий всеми признаками товара. До недавнего времени такого продукта в полноценном виде просто не существовало. Были программы – объекты авторского права. Однако с развитием информационных технологий появилась криптовалюта, финансовый феномен, который по своей природе и стал тем недостающим информационным продуктом – объектом вещного права.

В связи с этим нами предлагается расширить предмет хищения, включив в него цифровой информационный продукт, то есть совокупность уникальных компьютерных данных, объединённых в материальный либо виртуальный носитель, обладающих всеми признаками товара, собственной стоимостью и принадлежащих на праве собственности другому лицу. При хищении такого продукта нарушаются не столько отношения в сфере нормального оборота компьютерной информации или авторские права, сколько отношения собственности, поскольку правомерный собственник больше не может осуществлять права пользования, владения и распоряжения данным продуктом. Примером такого продукта может служить криптовалюта.

Объективная сторона. Что касается объективной стороны экономических киберпреступлений, то её особенности проявляются не в обязательных признаках (они ничем не отличаются от аналогичных составов экономических преступлений), а скорее в факультативных признаках, таких как способ, место и средство совершения преступления.

Как было сказано выше, отличительным признаком всех киберпреступлений является дистанционный способ их совершения. Такие преступления принципиально отличаются отсутствием физического или пространственного контакта между виновным и потерпевшим. Преступник может совершить хищение из банка, расположенного в другой стране, не выходя из дома, только с использованием киберпространства.

Дистанционное совершение преступления не снижает его общественной опасности. Представляется, что такой способ, наоборот, предполагает более серьезный подход к планированию и реализации преступного умысла. Так, для того, чтобы совершить, например, мошенничество путём обмана или злоупотребления доверием, преступник может зарегистрироваться в нескольких социальных сетях под разными именами и в течение продолжительного времени вести общение с ничего не подозревающими потерпевшими, и только после того, как он полностью завладеет их доверием, попросить денег и обмануть.

Дистанционный способ совершения преступления позволяет не оставлять физических следов, что затрудняет процесс доказывания и выявления преступника. Всё что остаётся после совершения большинства киберпреступлений – это записи на компьютере потерпевшего и записи его Интернет-провайдера. Единственное, что таким образом можно выявить, – это IP-адрес (от англ. Internet Protocol Address) компьютера виновного, однако в большинстве случаев преступники используют «анонимайзеры» и иные программы, тем самым скрывая свой действительный IP-адрес.

Более того, в случае, если преступник воспользовался бесплатным и беспроводным Интернет-соединением (Wi-Fi) в каком-либо кафе, то проследить его можно только лишь до IP-адреса компьютера кафе. В этом случае единственная нить, связывающая преступника и жертву, – это MAC-адрес (от англ. Media Access Control) ноутбука, планшета или смартфона виновного и запись на компьютере кафе о том, что с этого MAC-адреса в определённое время был осуществлён доступ в сеть Интернет. Однако виновный может просто

выкинуть свой смартфон или планшет после совершения преступления, и на этом нить оборвется.

Также дистанционный способ совершения преступления позволяет преступникам оставаться анонимными и субъективно чувствовать себя защищёнными от правоохранительных органов. Потерпевшие не могут описать ни примерный возраст, ни рост, ни пол преступника.

Дистанционный способ совершения преступления оказал влияние на другие факультативные признаки состава. Так, например, в научной литературе можно встретить споры касательно места совершения киберпреступления.

Как указывает А.К. Киселёв, сеть «Интернет» используется преступными группами уже не только как средство, но и как место совершения традиционных преступлений[1]. С такой же точкой зрения выступает М.С. Дашян: по его мнению, в зависимости от конкретной проблемы, «Интернет» может признаваться и средством исполнения противоправных действий, и местом совершения деяния[2].

Представляется, что авторы использовали понятие «Интернет» достаточно широко, включив в него само киберпространство. Немного корректируя данные высказывая, можно представить основную мысль так: киберпространство может рассматриваться в качестве места совершения преступления.

Данная идея является весьма новаторской и поэтому вызывает сильный интерес. Использование киберпространства как места совершения преступления позволяет понять простоту и лёгкость совершения киберпреступлений. Представив виртуальную реальность как некое место, можно легко проиллюстрировать саму суть киберпреступлений. Однако, на наш взгляд, такой подход является слишком утрированным, поскольку при его использовании не учитывается само значение места совершения преступления.

Выявление места совершения преступления необходимо для определения уголовного закона, который будет действовать в этом месте. В случае признания киберпространства местом совершения преступления не представляется

[1]Киселёв А.К. Киберпреступность – взгляд из Европы. // Библиотека криминалиста. 2013. №5(10) С.310.

[2]Дашян М.С. Право информационных магистралей: вопрос правового регулирования в сети «Интернет». М., Волтерс Клувер, 2007. С. 81.

возможным достоверно определить, уголовный закон какого государства следует принять в той или иной ситуации, поскольку киберпространство не является территорией ни одного из существующих государств. Следовательно, к преступлениям, совершённым в таком месте, как киберпространство, невозможно применить территориальный принцип действия уголовного закона. Отсюда следует, что понимание киберпространства в качестве места совершения преступления не имеет никакого уголовно-правового значения.

Как верно указывает О.С. Гузеева, местом совершения интернет-преступления (или в нашем случае киберпреступления) является территория того государства, где было совершено общественно опасное деяние либо завершено или пресечено преступление[1].

Само киберпространство нельзя рассматривать в качестве места совершения деяния. Так, при совершении любого киберпреступления активным действием человека, на наш взгляд, следует считать его действия по вводу данных (работа за компьютером, нажатие клавиш клавиатуры). Из этого следует, что местом совершения деяния является место, где виновный совершил ввод компьютерных данных, то есть это место доступа в киберпространство (конкретная квартира или Интернет-кафе).

Представляется, что киберпространство – это основное средство совершения преступления. Киберпространство создаёт все необходимые условия для совершения преступления дистанционно. Преступник использует эту возможность, что заметно облегчает ему сам процесс совершения преступления. При этом в отсутствие доступа в киберпространство совершение экономических киберпреступлений становится невозможным. Даже если у преступника будет в наличии персональный компьютер, но доступа в киберпространство не будет, то и совершить дистанционно преступление у него не получится. Киберпространство создаёт между субъектом и потерпевшим связь, без которой доведение преступления до конца не представляется возможным.

---

[1] Гузеева О.С. Действие Уголовного кодекса России в отношении интернет-преступлений // Законы России: опят, анализ, практика. 2013. №10. С. 18.

Устройства доступа в киберпространство (смартфоны, планшеты, компьютеры) могут выступать в качестве вспомогательных средств, поскольку без доступа в киберпространство они теряют свою значимость для преступника и делают невозможным доведение киберпреступления до конца. Это положение справедливо также для вирусов и иного вредоносного программного обеспечения.

Субъективная сторона. С субъективной стороны, все исследуемые составы преступлений совершаются умышлено, при этом, как правило, с прямым умыслом, что также говорит о характере общественной опасности[1].

В 1996 году корыстный мотив уже составил две трети (66%)[2] от общего числа всех компьютерных преступлений, в 2008 году эта цифра выросла до 95,83%[3], а в 2013 году почти все киберпреступления, зафиксированные в Российской Федерации, были совершены из корыстных побуждений[4]. Исходя из прослеживаемой динамики, можно сделать вывод, что процент корыстного мотива будет стремиться к 100%.

Основываясь на полученных данных, можно сделать вывод, что тенденция к увеличению корыстных преступлений из общего числа компьютерных преступлений на сегодняшний день достигла своего апогея. Данное явление, на наш взгляд, обуславливается естественным развитием киберпреступности: поскольку в киберпространстве возник массовый оборот денежных средств, появилась возможность хранить их в виртуальных кошельках и осуществлять реальную экономическую деятельность в сети, то и хакеры обнаружили в своих навыках экономический потенциал. Возможность легкого заработка в сети

---

[1]См.: Гарботович Д.А. Квалификация уголовно-правовых деяний по субъективной стороне: дис. ... канд. юрид. наук. Челябинск, 2004. С. 106; Гребенюк А.В. Вина в российском уголовном праве: дис. ... канд. юрид. наук. Ростов-н/Д., 2004. С. 67-69; Скляров С.В. Вина и мотивы преступного поведения как основание дифференциации и индивидуализации ответственности: дис… докт.юрид.наук. М., 2004. С. 111; Черепенников Р.В. Цели преступного деяния и их уголовно-правовое значение: дис. ... канд. юрид. наук. М., 2011. С.57-70; Паньков И.В. Умышленная вина по российскому уголовному праву: теоретический и нормативный аспекты: дис. ... канд. юрид. наук. СПб., 2010. С. 47-56; Кораблёва С.Ю. Вина как уголовно-правовая категория и её влияние на квалификацию преступлений: дис. ... канд. юрид. наук. М., 2013.С. 40-42

[2]Вехов В.Б. Компьютерные преступления: способы совершения, методики расследования. М., 1996. С. 41.

[3]Дремлюга Р.И. Интернет-преступность: монография. С.140.

[4]Мошков А.Н. Информационная безопасность России: новые вызовы, угрозы, решения // Информационная безопасность России: аналитический сборник. 2014. Вып.1. С.86.

привлекла преступников, ранее осуществлявших экономические преступления в материальном мире.

Субъект экономических киберпреступлений не обладает особыми специфическими признаками, что нельзя сказать о личности преступника. Об этом подробнее будет идти речь в следующей главе.

В зависимости от конкретных составов субъект данных преступлений может быть как общим, так и специальным. При наличии общего субъекта таковым признается вменяемое физическое лицо, достигшее возраста уголовной ответственности (14 лет для преступлений, предусмотренных статьёй 163 и частью 2 статьи 167 УК РФ, или 16 лет для остальных преступлений). К специальным характеристикам субъектов некоторых киберпреступлений можно отнести наличие специального статуса: инсайдера при неправомерном использовании инсайдерской информации (ст. 185.6 УК РФ) или налогоплательщика при совершении ряда налоговых преступлений (ст. 198, 199, 193.2 УК РФ) и так далее.

Основываясь на вышесказанном, в качестве выводов по общей характеристике составов экономических киберпреступлений можно привести следующие положения:

1. родовым объектом всех экономических преступлений, совершаемых в киберпространстве, являются экономические отношения, обеспечивающие материальное благосостояние личности, общества и государства. В зависимости от способа совершения киберпреступления в качестве дополнительного объекта могут выступать отношения в сфере компьютерной информации;

2. 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.

3. отличительными признаками объективной стороны киберпреступлений являются дистанционный способ их совершения; отдалённость друг от друга места совершения общественно опасного деяния и места наступления последствий; использование киберпространства в качестве основного средства совершения преступления;

4. корыстные мотивы и цели являются преобладающими во всех экономических преступлениях, совершаемых в киберпространстве;

5. для более полного анализа экономических преступлений, совершаемых в киберпространстве, необходимо подробно рассмотреть каждый их состав в отдельности.

§2. Преступления против собственности, совершаемые в киберпространстве

«Мошенничество» (хищение) в сфере компьютерной информации. Хищение, совершаемое с помощью средств компьютерной техники, называемое «компьютерным мошенничеством» или «мошенничеством в сфере компьютерной информации», является самым обсуждаемым видом киберпреступлений в отечественном и зарубежном научном сообществе, а также одним из самых распространённых киберпреступлений[1]. Как неоднократно отмечал начальник Бюро специальных технических мероприятий МВД РФ А.Н.Мошков, подавляющее большинство всех киберпреступлений, совершаемых в России, – это мошенничества[2]. По нашим данным, 74% всех киберпреступлений являются мошенничествами (39% – основной состав мошенничества, 35% – мошенничество в сфере компьютерной информации). [3]

[1]См.: Медведев С. С. Мошенничество в сфере высоких технологий: дис... канд. юрид. наук. Краснодар, 2008. С. 62-67; Зыков Д.А. Виктимологические аспекты предупреждения компьютерного мошенничества: дис. … канд. юрид. наук. Владимир, 2002. С. 44-47; Окружко В. Ю. Современное мошенничество: криминологическая характеристика и предупреждение: дис.... канд. юрид. наук. Ростов-н/Д. 2009.. С. 27-33; Дремлюга Р.И., Интернет-преступность. дис. ... канд. юрид. наук. Владивосток, 2007. С.40; Тропина Т.Л. Киберпреступность: понятие, состояние, уголовно-правовые меры борьбы: дис. …канд. юрид. наук. Владивосток, 2005. С.152.

[2]Материалы «Инфофорум-2013», «Инфофорум-2014», «Инфофорум-2015». Архив автора.

[3] См. Приложение №3. Таблица работы с судебными документами.

Однако в связи с тематикой исследования и недавними дополнениями уголовного законодательства анализ компьютерного мошенничества, на наш взгляд, следует начать не с основного состава (ст. 159 УК РФ), а с нового – мошенничества в сфере компьютерной информации (ст. 159.6 УК РФ).

Представляется, что такое «мошенничество» – это следующая ступень развития таких преступлений, как неправомерный доступ к компьютерной информации (ст. 272 УК РФ) и создание, использование и распространение вредоносных компьютерных программ (ст. 273 УК РФ). Потеряв интерес во взломе компьютерных систем защиты ради развлечения, хакеры решили извлечь из такой деятельности материальную выгоду. Так, если всего десять-двадцать лет назад вредоносные программы меняли местами раскладку клавиатуры, то сегодня вирусы создаются для взлома виртуальных кошельков, получения персональных данных с целью хищения денежных средств.[1]

Криминализация такого деяния, как «мошенничество», или хищение в сфере компьютерной информации, в России была вопросом времени, так как данный состав был широко распространён за рубежом и возникала необходимость в создании новых, специальных норм[2]. С такими предложениями выступали Л.В. Григорьева в 1996 году[3], В.С. Карпов[4] в 2002 году, Т.Л Тропина в 2005 году и многие другие ученые. В итоге 29 ноября 2012 года в Уголовный кодекс Российской Федерации была введена статья 159.6 «Мошенничество в сфере компьютерной информации»[5].

---

[1] 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 / Под ред. А.В. Бриллиантова и Ю.Е. Пудовочкина. − М.: РГУП, 2015. – С. 334-351.

[2]Козаев Н.Ш. Некоторые новеллы уголовного законодательства, направленные на обеспечение экономической безопасности в условиях научно-технического прогресса.// Библиотека криминалиста. 2013. №5(10). С.19.

[3]Григорьева Л.В. Уголовная ответственность за мошенничество в условиях становления новых экономических отношений: дис... канд. юрид. Наук. Саратов, 1996. С.12 .

[4]Карпов В.С. Уголовная ответственность за преступления в сфере компьютерной информации. автореферат. дис. ... канд. юрид. наук Красноярск. 2002. С. 11.

[5]Федеральный закон от 29.11.2012 N 207-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации»// Собрание законодательства РФ. 2012. N49. Ст. 6752.

Согласно действующей редакции Уголовного кодекса Российской Федерации, мошенничеством в сфере компьютерной информации (ст. 159.6 УК РФ) признаётся хищение чужого имущества или приобретение права на него путём ввода, удаления, блокирования, модификации компьютерной информации, либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей.

В данном определении используются такие известные понятия, как «блокирование компьютерной информации» и «модификация компьютерной информации». Эти понятия были заимствованы из диспозиции статьи 272 УК РФ и понимаются в том же смысле. Однако при построении нормы законодатель использовал и новые понятия, такие как «ввод компьютерной информации» и «иное вмешательство в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей», легального определения которым нет.

Из смысла статьи 159.6 УК РФ следует, что ввод компьютерной информации – это один из способов вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей, то есть вмешательство в функционирование компьютера или сети компьютеров («Интернета»). Следовательно, вводом компьютерной информации, по смыслу данной статьи, не будет считаться электронная переписка между виновным и потерпевшим (ввод текста сообщения).

Однако из анализа судебной практики следует, что «вводом компьютерной информации» также будет считаться введение украденного или подложного пароля. При этом возникает следующее противоречие: такой ввод не нарушает функционирование средств хранения, обработки или передачи компьютерной информации с технической стороны вопроса, поскольку компьютерная система воспринимает данный пароль как действительный и разрешает доступ. С другой

стороны, такой ввод является неправомерным, следовательно, система фактически разрешает доступ не владельцу счета, а преступнику.[1]

Из этого следует, что под вводом компьютерной информации, на наш взгляд, следует считать внедрение 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.

В качестве примера можно привести дело из судебной практики.

Д., получив информацию о счетах граждан и действуя по договоренности с группой лиц, изготовил поддельные доверенности, получал дубликаты сим-карт и незаконно получил информацию о паролях к девяти аккаунтам системы Интернет-банка «-Онлайн». В ходе ввода информации о логинах и паролях Д. получил доступ к банковским счетам потерпевших. Затем, путем перечисления на разные счета и банковские карты, он завладел денежными средствами девяти потерпевших на общую сумму 2 740 000 рублей. Д. был признан виновным в совершении преступления, предусмотренного частью 2 статьи 159.6 УК РФ*[2].

Иное вмешательство в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей – достаточно широкое понятие, которое, на наш взгляд, включает в себя все действия с компьютерной информацией за исключением ввода, удаления, блокирования и модификации такой информации. Как указывает С.М. Кочои, таким вмешательством будет, например, нарушение правил эксплуатации данных средств хранения, обработки или передачи

---

[1] Простосердов М.А. Экономические преступления, совершаемые в киберпространстве и меры противодействия им // Судебные известия. Информационный бюллетень управления судебного департамента в Тамбовской области. 2014. №15(2). С. 49-53.

[2] Апелляционное определение Московского городского суда №10-2076 от 06.05.2013 // СПС «КонсультантПлюс».

охраняемой компьютерной информации либо нарушение правил эксплуатации данных информационно-телекоммуникационных сетей[1].

Примером может послужить дело из судебной практики.

Л., Б. и неустановленные следствием лица из корыстных побуждений вступили в организованную преступную группу. В период с 28 сентября 2010 г. по 16 марта 2011 г. Л., Б. и неустановленные следствием соучастники, получив через Б. оформленную на имя Л. дебетовую банковскую карту ОАО «Р», используя компьютерную технику и программы, технические познания в сфере работы с компьютерной информацией, удаленно, находясь в неустановленном следствием месте, с неустановленного следствием компьютера, неправомерно, через сеть «Интернет», осуществили вмешательство в функционирование компьютера ООО «Б». Вследствие данных действий Л., Б. и неустановленные следствием лица получили полный доступ к управлению расчетным счетом ООО «Б», после чего похитили с расчетного счета ООО «Б» денежные средства на общую сумму 438 000 руб. Л. и Б. признаны виновными в совершении преступления, предусмотренного частью 4 статьи 159.6 УК РФ[2].

Ещё одним спорным моментом в диспозиции статьи 159.6 УК РФ является отсутствие таких понятий, как «обман» и «злоупотребление доверием». Это связано с тем, что фактически обманывается не пользователь, а сам компьютер путем вмешательства в функционирование его средств хранения, обработки или передачи данных или информационно-телекоммуникационных сетей.

Однако, по нашему мнению, такое вмешательство не может считаться обманом в классическом его понимании. Невозможно обмануть компьютер, вводя в него вирус или иную вредоносную программу, как, например, невозможно обмануть дверной замок, вставив отмычку, а можно лишь обойти его систему защиты. Обман – это психологическое понятие, и воспринять обман может только существо, обладающее интеллектом и разумом. Компьютер же – лишь машина, не

[1]Кочои С.М. Новые нормы о мошенничестве в УК РФ: особенности и отличия. // Криминологический журнал Байкальского государственного университета экономики и права. 2013. № 4. С. 109.

[2]Апелляционное определение Московского городского суда №10-8391 от 23.09.2013 // СПС «КонсультантПлюс».

обладающая ни тем, ни другим. Значит, применение термина «обман» к компьютеру как минимум некорректно.

С подобной точкой зрения соглашается В.В. Хилюта: «хищение путём использования компьютерной техники возможно только посредством компьютерных манипуляций… следовательно, невозможно говорить о том, что при злоупотреблении с автоматизированными системами обработки данных присутствует обман. Обман компьютера – это эфемерное понятие, потому что компьютер – это всего лишь механизм и обмануть его в принципе невозможно»[1].

Схожая точка зрения была высказана также в пункте 13 Постановления Пленума Верховного Суда Российской Федерации от 27 декабря 2007 г. N 51, но применительно к банкоматам. Согласно данному Постановлению, «не образует состава мошенничества хищение чужих денежных средств путем использования заранее похищенной или поддельной кредитной (расчетной) карты, если выдача наличных денежных средств осуществляется посредством банкомата без участия уполномоченного работника кредитной организации»[2]. Такое деяние до введения статья 159.6 УК РФ необходимо было квалифицировать по статье 158 УК РФ как кражу.

Применительно к статье 159.6 УК РФ, говорится в другом Постановлении Пленума Верховного Суда Российской Федерации N 6 от 05 апреля 2012 года. Согласно Постановлению «подобные преступления совершаются не путем обмана или злоупотребления доверием конкретного субъекта, а путем получения доступа к компьютерной системе и совершения вышеуказанных действий, которые в результате приводят к хищению чужого имущества или приобретению права на чужое имущество»[3].

---

[1]Хилюта В.В. Хищение с использованием компьютерной техники или компьютерное мошенничество? // Библиотека криминалиста. 2013. №5(10). С.62.

[2]Постановление Пленума Верховного Суда РФ от 27.12.2007 N 51 «О судебной практике по делам о мошенничестве, присвоении и растрате»// Бюллетень Верховного Суда РФ. 2008. N 2.

[3]Постановление Пленума Верховного Суда РФ от 05.04.2012 N 6 «О внесении в Государственную Думу Федерального Собрания Российской Федерации проекта Федерального закона «О внесении изменений в Уголовный кодекс Российской Федерации и иные законодательные акты Российской Федерации»// СПС «КонсультантПлюс».

Из этого следует, что диспозицией статьи 159.6 УК РФ предусмотрена новая, самостоятельная форма хищения со специальным способом (путём ввода, удаления, блокирования, модификации компьютерной информации и т.д.), а термин «мошенничество» применён некорректно, так как данное хищение совершается без обмана или злоупотребления доверием. С данной точкой зрения соглашается 62,5% (60 чел.) опрошенных судей, при этом 25% (24 чел.) высказались против, а 12,5% (10 чел.) затруднились ответить.[1]

По нашему мнению, данную статью необходимо изложить в следующей редакции:

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.[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

[1] См.: Приложение №2. Опросный лист.

[2] Простосердов М.А. Мошенничество, совершаемое в киберпространстве и его виды // Актуальные проблемы теории и практики применения уголовного закона: сборник материалов научно-практической конференции. Под ред. А.В. Бриллиантова и Ю.Е. Пудовочкина. М., РГУП. 2015. С. 334-351.

[3] Мутасова М.А. Мошенничество в информационной сфере. // 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.185.

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

[1]Информационный ресурс компании «CERT-GIB». Анализ обращений в CERT-GIB за 2013 год... - Group-IB Расследование компьютерных преступлений. [Электронный ресурс] //URL: https://www.facebook.com/GroupIB/posts/640006572733415 (Дата обращения: 27.01.2014).

совершается хищение вверенного имущества[1]. 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 рубля*[2].

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.

---

[1]См.: Шульга А.В. Присвоение или растрата в условиях становления рыночных отношений: дис... канд. юрид. наук. Краснодар, 2000. С.52-62; Селиванов И.О. Присвоение или растрата: Уголовно-правовые и криминологические аспекты: дис... канд. юрид. наук. Калининград, 2002. С.62-78; Бакрадзе А.А. Присвоение и растрата как формы хищения в уголовном праве России: дис... канд. юрид. наук. М., 2004. С.40; Скрипников Д. Ю. Присвоение и растрата как способы изъятия и обращения чужого имущества, вверенного виновному: дис... канд. юрид. наук. М., 2009. С.147.

[2]Приговор Курского районного суда Ставропольского края от 08.08.2013 по делу N 1-132/2013 ст.160 ч. 2 УК РФ // СПС «КонсультантПлюс».

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 рублей[1].

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;

4. получение логина и пароля к аккаунту виртуального кошелька или банковского счета путём обмана (фишинг, вишинг, фарминг) само по себе не формирует ни состав мошенничества в сфере компьютерной информации (ст. 159.6 УК РФ), ни основной состав мошенничества (ст. 159 УК РФ), поскольку предметом посягательства является не чужое имущество, а информация. Данное

[1]Приговор Октябрьского районного суда города Пензы от 14.06.2012 по делу N 1-166/2012. // СПС «КонсультантПлюс».

деяние необходимо 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 уже необходимо будет квалифицировать только по статье 159.6 УК РФ;

5. мошенничество в сфере компьютерной информации (ст. 159.6 УК РФ) стоит отличать от присвоения и растраты (ст. 160 УК РФ), которые также могут быть совершены путём ввода компьютерной информации, поскольку в последнем случае происходит хищение вверенного имущества;

6. в связи со сложившимися терминологическими трудностями и проблемами в квалификации деяния, указанного в статье 159.6 УК РФ, возникла объективная необходимость в принятии соответствующего Постановления Пленума Верховного Суда Российской Федерации.[1]

Мошенничество. Несмотря на появление статьи 159.6 УК РФ (мошенничество в сфере компьютерной информации), в киберпространстве всё же осталась возможность совершить мошенничество путём обмана или злоупотребления доверием. С данной точкой зрения согласно 52% (50 чел.) опрошенных судей, 29,2 % (28 чел.) высказались против, а 18,8% (18 чел.) затруднились ответить.[2]

Основное отличие такого мошенничества (ст. 159 УК РФ) от «мошенничества» в сфере компьютерной информации (ст. 159.6 УК РФ), по нашему мнению, заключается в способе его совершения. В науке сложилась устойчивая точка зрения, что классическим признаком мошенничества является

[1] Простосердов М.А. Мошенничество, совершаемое в киберпространстве и его виды // Актуальные проблемы теории и практики применения уголовного закона: сборник материалов научно-практической конференции. Под ред. А.В. Бриллиантова и Ю.Е. Пудовочкина. М., РГУП. 2015. С. 334-351.

[2] См.: Приложение №2. Опросный лист.

добровольная передача потерпевшим имущества или права на имущество виновному под влиянием обмана или злоупотребления доверием[1].

При «мошенничестве» в сфере компьютерной информации имущество добровольно не передаётся, а напрямую обращается путём ввода, удаления, блокирования компьютерной информации и т.д. Следовательно, мошенничество (в рамках статьи 159 УК РФ) в киберпространстве можно совершить только путём обмана или злоупотребления доверием.

Обман и злоупотребление доверием в киберпространстве возможны путём личного общения виновного с потерпевшим, через чат, форумы, видео- и аудио-звонки, опубликованием объявлений о продаже заведомо несуществующих предметов и множеством других способов, что породило разные виды такого мошенничества. К примеру, Т.М. Лопатина, даёт следующую классификацию «Интернет-мошенничества»:

•традиционное «Интернет-мошенничество» (мошенничество с предоплатой в электронной почте, мошенничество при оплате страховки, финансовые пирамиды в сети «Интернет», «Нигерийская афера»[2] и так далее);

•новое «Интернет-мошенничество» (игровое мошенничество, то есть мошенничество в Онлайн-играх, мошенничество в сфере Интернет-услуг, Онлайн-аукционы, создание фальшивых Интернет-магазинов)[3].

---

[1]См.: Качурин Д.В. Уголовная ответственность за обман и злоупотребление доверием (мошенничество) в отношении предприятий, организаций и коммерческих структур с различными формами собственности в период рыночных отношений: дис... канд. юрид. наук. М., 1996. С.38-50; Григорьева Л.В. Уголовная ответственность за мошенничество в условиях становления новых экономических отношений: дис... канд. юрид. наук. Саратов, 1996. С. 47-53; Лесняк В.И. Мошенничество: Уголовно-правовой и криминологический аспекты: дис... канд. юрид. наук. Екатеринбург, 2000. С.72-88; Оленев Р.Г. Мошенничество как вид девиантного экономического поведения: дис... канд.экон.наук. СПб., 2000. С.8-10; Семина Л.В. Уголовно-правовые и криминологические аспекты мошенничеств, совершаемых в сфере экономической деятельности: дис... канд. юрид. наук. Краснодар, 2003. С.40; Сунчалиева Л.Э. Мошенничество: Уголовно-правовой и криминологический аспект: дис... канд. юрид. наук. Ставрополь, 2004. С. 80-81; Алиева Д.Н. Мошенничество: уголовно-правовой и криминологический анализ: По материалам Республики Дагестан: дис... канд. юрид. наук. Махачкала, 2005. С.10-12; Лунин Н.Н. Мошенничество по уголовному законодательству России: уголовно-правовая характеристика и квалификация: дис... канд. юрид. наук. Орел, 2006. С.30-49; Беляк О. С. Ответственность за мошенничество по уголовному праву России: дис... канд. юрид. наук. М., 2006. С. 48; Суслина Е. В. Ответственность за мошенничество по Уголовному кодексу Российской Федерации: дис... канд. юрид. наук. Екатеринбург, 2007. С. 49; Яни П.С. Мошенничество и иные преступления против собственности: уголовная ответственность. Книга третья. М., Библиотека журнала «Уголовное право». 2007. С. 64-68.

[2]«Нигерийская афера», или «афера 419», названа по статье 419 УК Нигерии «мошенничество с предварительным уведомлением» была распространена в 2002-2003 годах на сайтах знакомств.

[3]Лопатина Т.М. Проблемы формирования уголовно-правового способа борьбы с компьютерным мошенничеством. // Библиотека криминалиста. 2013. №5(10). С.36-37.

С.С. Медведев выделяет похожие виды простого мошенничества, совершаемого в сети «Интернет»:

- мошенничество в сфере азартных игр;
- мошенничество в сфере онлайн-аукционов;
- мошенничество с использованием электронных денег и электронных платёжных систем;
- мошенничество в сфере предоставления товаров и услуг;
- мошенничество в сфере знакомств;
- «Нигерийская афера»[1].

О.С. Гузеева выделяет следующие виды мошенничества в сети Интернет:

- схема «увеличить и сбросить» – вид рыночной манипуляции, заключающийся в извлечении прибыли за счёт продаж ценных бумаг, сброс на которые был искусственно сформирован;
- схема финансовой пирамиды;
- схема «надёжного» вложения капитала – распространение через сеть Интернет ложных инвестиционных предложений с низким уровнем риска и высоким уровнем прибыли;
- экзотические предложения – распространение через сеть Интернет предложений о покупке акций Коста-Риканской кокосовой компании на условиях получения сверхприбыли;
- мошенничество с использованием банков;
- фишинг;
- интернет-попрошайничество;
- аукционы и розничная торговля в режиме онлайн[2].

Также отдельно выделяют такой вид кибермошенничества, как «кремминг» – выставление счетов за неоказанные услуги или товар в сети «Интернет». [1] К

[1]Медведев С.С. Мошенничество в сфере высоких технологий: дис...канд.юрид.наук. Краснодар, 2008. С.100-145.

[2] Гузеева О.С. Квалификация мошенничества в российском сегменте сети Интернет. // Законность. 2013. №3(941). С. 21-24.

примеру, при покупке в Интернет-магазине продавец высылает письмо-подтверждение на электронную почту покупателя и добавляет к его покупке ряд новых позиций, которые покупатель не намеревался приобретать. Покупатель соглашается с покупкой автоматически, не вглядываясь в содержание письма и не подозревая, что его обманом заставили приобрести ненужные ему предметы.

Такое разнообразие видов кибермошенничества А.Э. Побегайло объясняет анонимностью, как самого киберпространства, так и его пользователей. Она поясняет, что «Интернет» позволяет с лёгкостью выдавать себя за другого человека, изменяя данные о возрасте, социальном статусе и другие идентифицирующие признаки, что даёт большое преимущество преступникам при совершении мошенничества[2].

По нашему мнению, такое многообразие видов кибермошенничества объясняется тем, что:

- во-первых, обман или злоупотребление являются относительно простыми в исполнении способами совершения преступления и не требуют каких-либо специальных знаний и навыков;
- во-вторых, само киберпространство проникло почти во все сферы жизни общества, тем самым создав все условия для существования разных способов обмана пользователей компьютерных сетей.

В настоящее время самыми распространенными сферами общественной жизни в киберпространстве являются: финансовая сфера (Интернет-банки и виртуальные кошельки); сфера предоставление товаров и услуг (Интернет-магазины, объявления, покупка-продажа билетов); социальная сфера (социальные сети и сайты знакомств); развлекательная сфера (Интернет-игры и Интернет-казино). Как показывает практика, именно в этих сферах совершается наибольшее количество преступлений путём обмана или злоупотребления доверием.

---

[1]Официальный отзыв Правительства РФ от 02.08.2012 N 3904п-П4 «На проект Федерального закона «О внесении изменений в Уголовный кодекс Российской Федерации и иные законодательные акты Российской Федерации»// СПС «КонсультантПлюс».

[2]Побегайло А.Э. Киберпреступность: лекция. С.31.

К примеру, *в 2011 году сотрудниками МВД Санкт-Петербурга и Йошкар-Олы была пресечена деятельность брачных аферистов. Девушки в составе организованной группы создавали поддельные аккаунты в социальной сети и вели переписку с потерпевшими, ищущими молодых жен. Через некоторое время они писали о личной встрече и просили переслать определённую сумму денег на счет Интернет-кошелька, якобы на дорогу. После того как деньги были зачислены на счёт мошенника, они удаляли старые аккаунты, создавали под другим именем новый и повторяли всю схему с другим потерпевшим. Ежемесячный преступный доход организованной группы составлял более 10 млн. рублей. После их обнаружения было возбуждено уголовное дело по факту мошенничества (ст. 159 УК РФ)*[1].

Ещё одним примером основного состава мошенничества в киберпространстве может служить уголовное дело в отношении сотрудников компании «Эвитерра Трэвел»[2].

Как сообщает Следственный Комитет Российской Федерации, в течение 2013 года сотрудники компании ООО «Эвитерра Трэвел» осуществляли продажу билетов на рейсы различных авиакомпаний от имени ООО «АВИА ЦЕНТР» через сеть «Интернет». Однако полученные от граждан денежные средства в размере свыше 1 млн. рублей во исполнение имеющихся обязательств по субагентскому договору с ООО «АВИА ЦЕНТР» не перечислили, а распорядились по своему усмотрению. В связи с этим проданные билеты были аннулированы ООО «АВИА ЦЕНТР» без возмещения денежных средств владельцам билетов. 9 января 2014 года было возбуждено уголовное дело по факту мошенничества в особо крупном размере (ч. 4 ст. 159 УК РФ).

Согласно статистическим данным компании «Group-IB» в 2013 году было зафиксировано более 4000 обращений, связанных с мошенническими сайтами[3].

---

[1]Информационный ресурс «Mari Uver». [Электронный ресурс]// URL: http://mariuver.wordpress.com/2011/09/13/brach-aferist/ (Дата обращения: 27.01.2014).

[2]Официальный сайт Следственного Комитета Российской Федерации [Электронный ресурс] URL: http://www.sledcom.ru/actual/372197/ (Дата обращения: 27.02.2014).

[3]Анализ обращений в CERT-GIB за 2013 год... - Group-IB Расследование компьютерных преступлений. [Электронный ресурс]// URL: https://www.facebook.com/GroupIB/posts/640006572733415 (Дата обращения: 27.01.2014).

Ещё одним способом совершения мошенничества путём обмана в киберпространстве является мошенничество с «мини-кредитами». В сети «Интернет» многие банки оказывают услугу выдачи «мини-кредита» или «микро-займа» (как правило, от 1 до 30 тысяч рублей) только посредством предоставления паспортных данных. Деньги начисляются на банковский счет клиента или на электронный кошелёк. Такая услуга стала весьма популярной за рубежом, ею пользуются, если для оплаты какого-либо товара не хватает незначительной суммы денег, а весь товар в кредит брать не хочется. В России данная услуга только набирает популярность.

Преступник может взять множество кредитов на чужое имя, предоставляя банку через Интернет чужие паспортные данные. В связи с особенностью способа совершения преступления содеянное необходимо квалифицировать по статье 159.1 УК РФ как мошенничество в сфере кредитования.

Такое мошенничество совершается в киберпространстве без специальных программ и без вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей. В случае если виновный осуществляет неправомерный ввод, удаление, блокирование, модификацию компьютерной информации, то своими действиями он совершает преступление, предусмотренное статьёй 159.6 УК РФ.

В связи с тем, что подобное мошенничество совершается, хотя и с использованием телекоммуникационных технологий, дополнительной квалификации по статьям главы 28 УК РФ не требуется, так как нарушаются лишь отношения собственности, а не отношения, обеспечивающие правомерный доступ, создание, обработку, преобразование и использование компьютерной информации, которым вред не причиняется.

Основываясь на вышесказанном можно сделать следующие предварительные выводы:

1. способы совершения основного состава мошенничества в киберпространстве ограничиваются лишь возможностями самого киберпространства и также разнообразны;

2. в настоящее время самыми распространенными сферами общественной жизни в киберпространстве являются: финансовая сфера (Интернет-банки и виртуальные кошельки); сфера предоставление товаров и услуг (Интернет-магазины, объявления, покупка-продажа билетов); социальная сфера (социальные сети и сайты знакомств); развлекательная сфера (Интернет-игры и Интернет-казино). Как показывает практика, именно в этих сферах совершается наибольшее количество преступлений путём обмана или злоупотребления доверием;

3. мошенничество, совершаемое путём обмана или злоупотребления доверием в киберпространстве, необходимо квалифицировать только по статье 159 УК РФ, квалификация по совокупности со статьями главы 28 УК РФ не требуется, поскольку вред причиняется только отношениям собственности, а отношения в сфере компьютерной информации остаются незатронутыми.

Вымогательство. При квалификации вымогательства, совершенного в киберпространстве, возникают вопросы о характере угрозы. Принято считать, что вымогательство может совершаться путём угрозы применения насилия; путём угрозы распространения сведений; путём угрозы уничтожения или повреждения чужого имущества[1].

[1]Подробнее см.: Лукьянова И. В. Угроза как преступление в уголовном праве России: дис. ... канд. юрид. наук. М., 2004. С. 10-12; Фомичева М.А. Угроза как способ совершения преступления: дис. ... канд. юрид. наук. М., 2008. С.8-10; Ивахненко А. М. Квалификация бандитизма, разбоя, вымогательства: проблемы соотношения составов: дис... канд. юрид. наук. М., 1996. С. 12; Щербина В. В. Ответственность за вымогательство: социально-правовые аспекты: дис... канд. юрид. наук. Ростов-н/Д., - 1999; Рассказов М. Ю. Уголовная ответственность за вымогательство: дис... канд. юрид. наук: 12.00.08 / Рассказов Михаил Юрьевич - Ростов-н/Д., 2002. С.4-15; Абдулгазиев Р. З. Вымогательство по российскому уголовному праву: дис... канд. юрид. наук. Махачкала, 2003. С 93-100.; Жариков Р. А. Детерминанты вымогательства и особенности его предупреждения в сверхкрупном городе: дис... канд. юрид. наук. Челябинск, 2004. С 10-15.; Жданухин Д.Ю. Уголовно-правовая характеристика шантажа: дис... канд. юрид. наук. Екатеринбург, 2005. С. 20-20; Богомолов А.А. Вымогательство в системе преступлений против собственности: криминологический анализ и предупреждение: дис... канд. юрид. наук. М., 2005. С. 3-18; Рыжкова И.Д. Вымогательство: теоретико-правовой анализ и криминологическая характеристика: дис... канд. юрид. наук. М., 2008. С.5-15.; Буранова А.Г. Вымогательство и меры его предупреждения: дис... канд. юрид. наук. Ростов-н/Д.,2011. С. 10-12; Тагиев Т.Р. Вымогательство по уголовному праву России: дис... канд. юрид. наук. Томск, 2011. С. 15-20; Чхвимиани Э. Ж. Уголовно-правовые и криминологические аспекты противодействия вымогательству: по материалам Краснодарского края: автореферат дис.... канд. юрид. наук. Ростов-н/Д., 2011.С. 10.

Такое вымогательство принципиально отличается отсутствием физического (пространственного) контакта между виновным и потерпевшим, что не снижает общественной опасности такого деяния, а предполагает более серьезный подход к планированию и реализации преступного умысла. Последнее обстоятельство определенным образом повышает степень общественной опасности «бесконтактного» вымогательства.

Угрозы в киберпространстве могут быть выражены через «Skype» или аудио-чат, через личные сообщения или электронную почту. При этом на практике наиболее распространены вымогательства, совершенные 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[1], а также под угрозой DDoS-атаки.

В качестве примера можно привести судебную практику. *Потерпевшая К., воспользовавшаяся услугами Интернет-кафе «Ультра», забыла закрыть аккаунт личной электронной почты. Виновный В. являлся работником Интернет-кафе, получив доступ к электронному ящику К., обнаружил фотографии, где К. была в обнаженном виде. Связавшись с К. по электронной почте, В. потребовал передать ему денежную сумму в размере 5000 рублей под угрозой распространения данных фотографий. В. был признан виновным в совершении преступлений, предусмотренных ч. 1 ст. 272, ч. 1 ст. 138, ч. 1 ст. 137, ч. 1 ст. 163 УК РФ. Наказание было назначено в виде 2 лет лишения свободы условно со штрафом в размере 5000 рублей*[2].

Другим примером может служить вымогательство под угрозой DDoS-атаки (англ. Distributed Denial of Service – отказ в обслуживании), технология которой достаточно проста. Хакер отправляет в киберпространство специальную, вредоносную программу, которую ничего не подозревающие пользователи устанавливают на персональный компьютер. Цель этой программы, на первый

[1] Простосердов М.А. Вымогательство, совершенное в сети Интернет // Библиотека криминалиста. 2013. №6. С.150-152.

[2] Приговор Октябрьского районного суда города Тамбова №1-324/09 от 29 мая 2009 года. // Архив Октябрьского районного суда города Тамбова.

взгляд, безвредна – зайти с компьютера, на котором она установлена, на выбранный хакером сайт по его команде или послать на данный сайт запрос. До команды хакера программа не проявляет никакой активности, но как только программа будет установлена на достаточное количество компьютеров (как правило, несколько сотен тысяч), хакер сможет создать из зараженных компьютеров «Бот-сеть» (сеть автономных компьютеров, управляемых с одного «главного компьютера»). По воле хакера каждый из тысячи зараженных компьютеров может одновременно посетить один сайт или послать на него какой-либо запрос.

Если на один сайт одновременно зайдет слишком много компьютеров или будет принято слишком много сообщений, то возможны два варианта развития событий:

- либо сеть (выделенная телекоммуникационная линия) не справится с потоком данных и переполнится;
- либо процессор компьютера, на котором расположен сайт, не успеет обработать информацию и сервер будет заблокирован (зависнет).

В любом случае добросовестные пользователи сайта не смогут его посетить, так как он будет недоступен, то есть заблокирован. DDoS-атака может продолжаться неопределённое время, и если данный сайт является коммерческим (Интернет-магазин), то добросовестные пользователи не смогут приобрести в нем товар, что приведёт к убыткам собственника сайта, а в дальнейшем к его разорению.

Следовательно, реализация DDoS-атаки может причинить значительный вред экономическим отношениям, в частности, отношениям собственности и отношениям, складывающимся в сфере компьютерной информации. Согласно «CERT-GIB» в 2013 году в центр круглосуточного реагирования на инциденты информационной безопасности поступило более 1500 обращений, связанных с

«ботнет-контроллерами» и вредоносным кодом[1]. При этом в сутки совершается приблизительно 150 DDoS-атак на территории России[2].

Так, Ф., имея умысел на вымогательство денежных средств, принадлежащих ЗАО «Тинькофф Банк», находясь у себя дома, используя компьютер, подключенный к сети «Интернет», при помощи приобретенного доступа к вредоносной компьютерной программе, осуществил ряд DDoS-атак на компьютерную информацию, содержащуюся на информационных ресурсах сайта, принадлежащего ЗАО «Тинькофф Банк». В результате осуществленных DDoS-атак работа информационных компьютерных систем ЗАО «Тинькофф Банк», объединенных в единую есть, была блокирована, в связи с чем ее пользователям было отказано в возможности оказания электронных услуг. После чего, действуя из корыстных побуждений, через социальную сеть «Twitter», Ф. потребовал от владельца ЗАО «Тинькофф Банк» передачи денежных средств в сумме 1000 долларов США за прекращение DDoS-атаки. Таким образом, Ф. использовал вредоносную компьютерную программу и под угрозой уничтожения и повреждения компьютерных систем ЗАО «Тинькофф Банк» выдвинул требование о передаче ему денежных средств. Ф. был признан виновным в совершении преступлений, предусмотренных статьям 163 и 273 УК РФ[3].

Поскольку в данном примере DDoS-атака была реализована, суд верно квалифицировал вымогательство по совокупности со статьёй 273 УК РФ. Однако в случае только лишь угрозы реализации DDoS-атаки такая квалификация, на наш взгляд, невозможна. При этом такая угроза, расцениваемая как реальная, способна причинить существенный вред правам и законным интересам потерпевшего.

Уголовная ответственность за подобное «компьютерное вымогательство», то есть за требование о передаче денежных средств или иного имущества,

---

[1]Анализ обращений в CERT-GIB за 2013 год... - Group-IB Расследование компьютерных преступлений. [Электронный ресурс]// URL: https://www.facebook.com/GroupIB/posts/640006572733415 (Дата обращения: 27.01.2014).

[2]Доклад компании Group-IB «Threat Intelligence Report 2012 – 2013 H1» [Электронный ресурс] // URL: http://report2013.group-ib.ru/ (Дата обращения: 26.04.2012).

[3]Приговор Хорошевского районного суда города Москвы от 01.12.2014 по делу N 1-587/2014. ст.163 ч. 1; ст. 273 ч. 1; ст. 273 ч. 2; ст. 273 ч. 2; ст. 273 ч. 2 УК РФ.// СПС «КонсультантПлюс».

совершенное под угрозой причинения ущерба компьютерной информации (её блокирование, модификацию, удаление или уничтожение), уже существует в США, Нидерландах и ряде других стран.

Следовательно, угроза удалением, блокированием либо модификацией компьютерной информации, а равно угроза иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации всё же может рассматриваться как новый характер угрозы при совершении вымогательства. С данной точкой зрения соглашается большинство опрошенных судей районных и областных судов Российской Федерации – 65,6% (63 чел.), против высказалось 18,75% (18 чел.), а 15,65% (15 чел.) затруднились ответить.[1]

Однако угроза совершения таких действий, по нашему мнению, выходит за пределы диспозиции статьи 163 УК РФ, поскольку её нельзя расценивать ни как уничтожение, ни как повреждение чужого имущества. С подобной точкой зрения выступал С.А. Филимонов, который указывал, что к организаторам DDoS-атак применить положения норм статьи 163 УК РФ нельзя, т.к. их действия находятся за рамками действий статьи и, следовательно, необходима квалификация по совокупности с соответствующими статьями главы 28 УК РФ[2].

Стоит согласиться с С.А. Филимоновым в части, что угроза удаления, блокирования либо модификации компьютерной информации находится за рамками действий вымогательства по смыслу статьи 163 УК РФ, однако квалификация данного деяния по совокупности со статьями 272, 273 или 274 УК РФ не решит проблему, поскольку собственно посягательство на эти отношения здесь фактически отсутствует, а виновный лишь создает угрозу такого посягательства, используя ее в качестве способа воздействия на потерпевшую сторону.

Поэтому, на наш взгляд, отсутствует необходимость выделения данного состава преступления в качестве квалифицирующего признака вымогательства. В

[1] См.: Приложение №2. Опросный лист.

[2] Филимонов С.А. Ошибки и затруднения, возникающие при квалификации киберпреступлений. // Библиотека криминалиста. 2013. №5(10). С.49, 50.

связи с чем, в целях корректной квалификации содеянного без формирования искусственной совокупности преступлений, часть 1 статьи 163 УК РФ необходимо изложить в следующей редакции:

«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»

Такая точка зрения является непопулярной среди опрошенных судей – с ней согласились лишь 5,6% (4 чел.)[1], однако, на наш взгляд, именно такое нововведение позволит в полной мере оценить общественную опасность деяния и избавит правоприменителя от трудностей квалификации, поскольку в данном случае дополнительная квалификация с соответствующими статьями главы 28 УК РФ будет необходима, только если злоумышленник действительно совершит уничтожение, блокирование либо модификацию компьютерной информации, или иное вмешательство в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей.

Основываясь на вышесказанном, можно сделать следующие выводы по данному составу преступления:

[1] См.: Приложение №2. Опросный лист.

1. наиболее распространёнными характерами угрозы при вымогательстве в киберпространстве являются:

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

б) угроза удаления, блокирования либо модификации компьютерной информации, угроза иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей;

2. 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, следовательно, необходимо провести редакцию действующего уголовного законодательства.

Причинение имущественного ущерба путем обмана или злоупотребления доверием. Так же как и в случае с мошенничеством, обман в диспозиции статьи 165 УК РФ может быть выражен в действиях, которые вводят в заблуждение потерпевшего, а не его компьютер. Однако ранее обман трактовался весьма широко, в том числе и как ввод в телефонную либо иную информационно-телекоммуникационную сеть технических изменений, позволяющих её «бесплатное» использование. При этом не имело значения, причинялся ли ущерб непосредственно провайдеру (оператору связи) либо клиенту.

На наш взгляд, когда виновный путем подобного неправомерного доступа «обманывает» компьютер, что причиняет имущественный ущерб, то данное деяние выходит за пределы статьи 165 УК РФ, если непосредственного контакта с потерпевшим не было, а само подключение было автоматизированным. Примером такого преступления может служить следующее дело из судебной практики.

В 2004 году Мичуринским городским судом Тамбовской области был осужден безработный «А.», который, обладая достаточными знаниями в области пользования компьютерной техникой и опытом работы в сети «Интернет», имея в личном пользовании персональный компьютер, через провайдера ОАО «Тамбовская электросвязь» неправомерно подключился к сети «Интернет». Незаконно скопировал на жесткий диск своего персонального компьютера, с целью дальнейшего использования, логин и пароль, принадлежащий ОАО «Волжский Ювелир». Используя данные реквизиты, А. неправомерно подключался к глобальной сети «Интернет», что привело к блокированию доступа к сети «Интернет» законного пользователя. В результате преступной деятельности ОАО «Волжский Ювелир» был причинён имущественный ущерб на общую сумму 4 500 рублей. А. был признан виновным в совершении преступления, предусмотренного частью 1 статьи 165 и частью 1 статьи 272 УК РФ[1].

На наш взгляд, квалификация данного деяния по совокупности преступлений является неверной, поскольку отсутствуют такие обязательные элементы объективной стороны преступления, предусмотренного статьёй 165 УК РФ, как обман и злоупотребление доверием. «А.» причинил имущественный ущерб только лишь путём неправомерного доступа к компьютерной информации, а именно к логину и паролю ОАО «Волжский Ювелир». Получив логин и пароль, система автоматически идентифицировала «А.» как законного пользователя и предоставила ему доступ в сеть «Интернет».

Представляется, что сегодня данное деяние следует квалифицировать по части 2 статьи 272 УК РФ, как «неправомерный доступ к компьютерной информации, причинивший крупный ущерб или совершенный из корыстной заинтересованности». Однако, на наш взгляд, расположение данной нормы в главе 28 Уголовного кодекса России является сомнительным. Чему причиняется

[1]Уголовное дело № 1-563/2004 год архив Мичуринского городского суда Тамбовской области из материалов монографии / Дворецкий М.Ю., Копырюлин А.Н. Оптимизация уголовной ответственности и проблемы квалификации преступлений в сфере компьютерной информации. С.178.

вред в первую очередь: отношениям, складывающимся в сфере компьютерной информации, либо экономическим отношениям?

Виновный использует чужой логин и пароль не для того, чтобы скопировать, уничтожить, блокировать либо модифицировать компьютерную информацию, а для того, чтобы избежать затрат по оплате доступа в сеть «Интернет». Да, виновный совершил неправомерный ввод охраняемой законом компьютерной информации, но первоначальной целью его была всё же корыстная выгода. Первоначально вред направлен на отношения собственности (в форме упущенной выгоды).

Представляется, что непосредственный состав, предусмотренный частью 2 статьи 272 УК РФ, необходимо переместить в главу 21 «Преступления против собственности». Виновный вводит компьютерную информацию и тем самым причиняет имущественный ущерб собственнику. Непосредственным объектом такого деяния, на наш взгляд, следует признать отношения собственности. При этом способ совершения такого преступления причиняет вред ещё одному объекту – отношениям, складывающимся в сфере компьютерной информации. Такие отношения выступают лишь в качестве дополнительного объекта.

Деяние не содержит в себе всех признаков хищения, следовательно, его не возможно квалифицировать по статье 159.6 УК РФ. В то же время оно совершается без обмана и злоупотребления доверием, поскольку фактически «обманывается» не человек, а компьютер, значит, квалификация деяния по статье 165 УК РФ также будет не верна.

Более того, аналогичная ситуация возникает в случае использования вредоносных программ (вирусов или иного вредоносного программного обеспечения), так как часть 2 статьи 273 УК РФ содержит смежный состав.

На наш взгляд, возникла необходимость в появлении нового состава преступления – «Причинения имущественного ущерба в сфере компьютерной информации».

Нами предлагается ввести в главу 21 Уголовного кодекса Российской Федерации следующую статью:

Статья 165.1. Причинение 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 необходимо будет признать утратившими силу части 2 статей 272 и 273 УК РФ. Это позволит избежать проблем квалификации таких деяний и положительно повлияет на систему отечественного уголовного законодательства.

При всём этом в киберпространстве остаётся возможность причинения имущественного ущерба именно путём обмана или злоупотребления доверием человека, а не компьютера. С данным мнением согласно 44,7% (44 чел.) опрошенных судей, 31,3% (30 чел.) высказались против него, а 24% (23 чел.) затруднились ответить.[1]

Так, исходя из смысла пункта 16 Постановления Пленума Верховного Суда Российской Федерации от 27 декабря 2007 г. N 51 обман или злоупотребление доверием при совершения преступления, предусмотренного статьёй 165 УК РФ, может выражаться, например, в представлении лицом поддельных документов,

[1] См.: Приложение №2. Опросный лист.

освобождающих от уплаты установленных законодательством платежей или от платы за коммунальные услуги, или иных услуг[1]. Представляется, что в киберпространстве также можно предоставить поддельные документы, закреплённые электронной подписью (через электронную почту, социальную сеть или иным способом).

В случае если своими действиями виновный причинит имущественный ущерб в крупном (250 тыс. руб.) или особо крупном (1 млн. руб.) размере, то он совершит преступление, предусмотренное статьёй 165 УК РФ. Поскольку для совершения преступления виновный использовал уже существующую инфраструктуру в киберпространстве (сайты, система электронной почты) и не представлял угрозы для отношений в сфере компьютерной информации, то дополнительной квалификации со статьёй 272 УК РФ не требуется. По той же причине, на наш взгляд, нет необходимости выносить данный состав преступления в самостоятельную норму либо в качестве квалифицирующего признака статьи 165 УК РФ.

Из анализа данного состава киберпреступления следует, что:

1. причинение имущественного ущерба путём вмешательства в информационно-телекоммуникационную сеть сегодня следует квалифицировать по части 2 статьи 272 УК РФ, а в случае использования вирусов и иных вредоносных программ – по части 2 статьи 273 УК РФ;

2. в киберпространстве существует возможность причинения имущественного вреда путём обмана или злоупотребления доверием без признаков хищения, однако при этом размер причиняемого виновным вреда должен составлять минимум 250 000 рублей. Такое деяние необходимо квалифицировать только по статье 165 УК РФ, без совокупности с соответствующими статьями главы 28 УК РФ.

[1]Постановление Пленума Верховного Суда РФ от 27.12.2007 N 51 «О судебной практике по делам о мошенничестве, присвоении и растрате»// СПС «КонсультантПлюс».

Умышленное уничтожение или повреждение имущества. Умышленное уничтожение или повреждение имущества с использованием киберпространства – это пример того, что киберпреступления причиняют реальный вред. Предметом данного киберпреступления может являться чужой компьютер, планшет, мобильный телефон и иное высокотехнологичное электронное устройство.

Поскольку состав данного преступления материальный, то деяние считается оконченным с момента причинения ущерба (ч. 1 ст. 167 УК РФ – значительного ущерба от 2 500 рублей). Учитывая, что стоимость современной электронной техники весьма высока (стоимость настольного персонального компьютера в России варьируется от 11 000 до 550 000 рублей)[1], то преступник может с лёгкостью совершить данное преступление, причинив ущерб всего одному потерпевшему. При этом с возможностями киберпространства количество потерпевших от одного преступника может достичь нескольких десятков.

Совершение данного преступления под силу только опытным программистам и хакерам, поскольку простым вирусом повредить или уничтожить оборудование нельзя. Вирус может повлиять на «софт», то есть программное обеспечение компьютера, что можно квалифицировать по статье 273 УК РФ.

Однако повреждение оборудования с использованием вредоносных программ все же возможно. Так, в настоящее время прослеживается тенденция к переходу с жестких дисков («винчестеров») на твердотельные накопители SSD. Их использование в разы ускоряет работу компьютера, но имеет два существенных минуса: во-первых, высокая стоимость (до 200 000 рублей); во-вторых, предел циклов перезаписи, по достижению которых он перестаёт работать, то есть все SSD-накопители имеют свой срок годности. Хакер может написать вредоносную программу, целью которой будет бесконечное копирование и удаление самой себя (перезапись). В случае если такая программа продолжительное время будет сама себя перезаписывать, это приведёт к

[1]Информационный ресурс «Яндекс.Маркет». Компьютеры // [Электронный ресурс] URL:http://market.yandex.ru/search.xml?&hid=91011&track=menuleaf&how=dprice&np=1 (Дата посещения 21.01.2015).

уничтожению SSD-накопителя, поскольку его невозможно будет ни использовать по целевому назначению, ни починить.

Представляется, что, действуя умышленно (например, по найму), хакер может совершить подобную кибер-атаку в отношении какой-либо коммерческой компании или в отношении частного лица. По нашему мнению, такое деяние выходит за пределы статьи 273 УК РФ и его необходимо квалифицировать по совокупности со статьёй 167 УК РФ. Это является лишь малым примером уничтожения реального имущества с использованием вредоносного программного обеспечения.

Более серьёзным примером может послужить дело о крушении рейса №5022.

20 августа 2008 года из-за троянской программы потерпел крушение самолёт McDonnell Douglas MD-82, выполнявший рейс из Мадрида в Лас-Пальмас. Троянская программа блокировала пилоту оповещение о том, что были убраны закрылки – это привело к катастрофе. Погибли 154 человека[1].

Содеянное, разумеется, невозможно квалифицировать по статье 167 УК РФ, однако этот пример наглядно демонстрирует возможности причинения реального физического ущерба с использованием вредоносного программного обеспечения и киберпространства.

В связи с вышесказанным, интерес вызывают квалифицирующие признаки, предусмотренные частью 2 статьи 167 УК РФ, а именно причинение иных тяжких последствий или смерть человека по неосторожности.

Согласно пункту 10 Постановления Пленума Верховного Суда РФ от 05.06.2002 N 14, к тяжким последствиям, причиненным по неосторожности в результате умышленного уничтожения или повреждения имущества, относятся, в частности, причинение по неосторожности тяжкого вреда здоровью хотя бы одному человеку либо причинение средней тяжести вреда здоровью двум и более лицам; оставление потерпевших без жилья или средств к существованию;

[1]Информационный ресурс «Хабрахабр» [Электронный ресурс] URL:http://habrahabr.ru/post/102427/ (Дата посещения 21.01.2015).

длительная приостановка или дезорганизация работы предприятия, учреждения или организации; длительное отключение потребителей от источников жизнеобеспечения – электроэнергии, газа, тепла, водоснабжения и т.п.[1]

Смерть, тяжкий вред здоровью или вред здоровью средней тяжести рассматриваемым деянием можно причинить, к примеру, в случае кибер-атаки на больницы, поликлиники или госпитали, где жизнь и здоровье людей зависят от аппаратов жизнеобеспечения либо где проводятся хирургические операции с применением средств компьютерной техники. Данное обстоятельство также подтверждает повышенную общественную опасность киберпреступлений.

Уничтожение или повреждение такого имущества, как криптовалюта, на наш взгляд, также следует квалифицировать по статье 167 УК РФ. Однако в случае если была уничтожена простая компьютерная информация (метаданные, аудио–, видео– или текстовой файл и т.д.), то такое деяние необходимо квалифицировать по статье 272 УК РФ как неправомерный доступ к компьютерной информации, повлекший её уничтожение.

Подводя итог анализу преступлений против собственности, совершаемых в киберпространстве в целом, можно сделать следующие выводы:

1. в киберпространстве можно совершить следующие преступления против собственности:

- мошенничество (ст. 159 УК РФ);
- мошенничество в сфере кредитования (ст. 159.1 УК РФ);
- мошенничество в сфере компьютерной информации (ст. 159.6 УК РФ);
- присвоение и растрату (ст. 160 УК РФ);
- вымогательство (ст. 163 УК РФ);
- причинение имущественного ущерба путём обмана и злоупотребления доверием (ст. 165 УК РФ);

[1]Постановление Пленума Верховного Суда РФ от 05.06.2002 N 14 (ред. от 18.10.2012) «О судебной практике по делам о нарушении правил пожарной безопасности, уничтожении или повреждении имущества путем поджога либо в результате неосторожного обращения с огнем»// Бюллетень Верховного Суда РФ. 2002. N 8.

•умышленное уничтожение или повреждение чужого имущества (ст. 167 УК РФ);

2. необходимо внести редакцию в название и диспозицию статьи 159.6 УК РФ («мошенничество» в сфере компьютерной информации), поскольку термин «мошенничество» к данному составу преступления применён некорректно;

3. диспозицию статьи 163 УК РФ (вымогательство) также необходимо изменить, дополнив новый характер угрозы: путём угрозы удаления, блокирования, модификации компьютерной информации, а также угрозы 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.

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

Киберпреступления в сфере предпринимательской, банковской деятельности и сфере азартных игр. Составы незаконного предпринимательства (ст. 171 УК РФ), организации и проведения азартных игр (ст. 171.2 УК РФ), а также незаконной банковской деятельности (ст. 172 УК РФ) имеют схожую конструкцию и объект посягательства, поэтому, для более точного и полного анализа, данные киберпреступления, на наш взгляд, следует рассмотреть в комплексе.

Современные технологии сильно упростили и удешевили процесс создания собственного дела благодаря сети «Интернет». Для открытия магазина, салона или фирмы в киберпространстве не требуется арендовать торговую площадь и ездить на работу – сегодня достаточно открыть собственный сайт и заниматься предпринимательской деятельностью «он-лайн». Благодаря избавлению от подобных издержек, занятие Интернет-предпринимательством получило широкое распространение. Так, по данным исследовательского агентства «Data Insight», в

2010 году объем рынка электронной коммерции на территории Российской Федерации составил 240 млрд. рублей[1]. В связи с такой популярностью в сети «Интернет» появился новый вид предпринимателей – т.н. «фрилансеры»[2].

Однако мало кто из «фрилансеров» осознаёт, что для предпринимательской деятельности необходимо как минимум зарегистрироваться в качестве индивидуального предпринимателя. Как следствие, с появлением возможности резко сократить расходы на осуществление предпринимательской деятельности, перенеся её в киберпространство, многие предприниматели просто стали игнорировать требования отечественного законодательства и осуществлять свою предпринимательскую деятельность без регистрации и лицензии. Помимо этого, как правильно указывала А.Э. Побегайло, данную проблему усугубляет полное отсутствие правового контроля в сфере Интернет-торговли[3].

В киберпространстве распространены следующие виды предпринимательской деятельности:

- электронная коммерция;
- банковская деятельность;
- предоставление услуг связи, передачи и хранения компьютерных данных, хостинг; [4]
- рекламная деятельность;
- оказание иных услуг (оформление сайтов, вёрстка электронных файлов и т.д.).

Стоит внести ясность: подобная экономическая деятельность направлена исключительно на систематическое получение прибыли. Перенос её в киберпространство для того, чтобы избежать лишних затрат и регистрации,

[1]Информационный ресурс «Бизнес ФМ». Электронная торговля отправится в регионы. [Электронный ресурс] // URL: http://www.bfm.ru/news/101235 (Дата обращения: 15.04.2014).
[2]От англ. freelancer — свободный наёмник.
[3]Побегайло А.Э. Киберпреступность: лекция. С.32.
[4]Предоставление вычислительной мощности оборудования в сети.

создаёт все условия для существования теневой экономики, а также «чёрного рынка» товаров и услуг в сети «Интернет»[1].

Представляется, что осуществление подобного вида экономической деятельности в отсутствие регистрации или лицензии, с причинением крупного ущерба гражданам, организациям или государству либо сопряженное с извлечением дохода в крупном размере, образует состав преступления, предусмотренного статьёй 171 УК РФ «Незаконное предпринимательство».

Несмотря на использование средств компьютерной техники, при совершении данного киберпреступления (ст. 171 УК РФ) виновный использовал уже существующую инфраструктуру в киберпространстве, а, следовательно, им не был причинён ущерб отношениям в сфере компьютерной информации. Поэтому дополнительная квалификация со статьями главы 28 УК РФ является излишней.

Однако данное деяние необходимо квалифицировать по совокупности со статьями 272 и 273 УК РФ, в случае если виновный при осуществлении незаконной предпринимательской деятельности совершит неправомерный доступ к компьютерной информации либо будет использовать вредоносные программы. Например, если предприниматель разошлёт по электронной почте вредоносные программы, которые будут принудительно перенаправлять пользователей на сайт его компании.

Другим видом предпринимательской деятельности, осуществляемым в киберпространстве, является банковская деятельность. Интернет-банкинг – не новое понятие для Российской Федерации. Изначально банки давали возможность

[1]Подробнее см.: Мусаев Ф.А. Преступления против общего порядка осуществления экономической деятельности (ст. 171, 172-174.1 УК РФ): вопросы законодательной техники и дифференциации ответственности: дис... канд. юрид. наук. Ярославль, 2005. С. 59-60.; Плотников С.А. Уголовная ответственность за незаконное предпринимательство: дис... канд. юрид. наук. М., 2003. С.72-80; Лубешко В.Н. Незаконное предпринимательство как вид преступного посягательства против установленного порядка экономической деятельности: Уголовно-правовой и криминологический аспекты: дис.... канд. юрид. наук. Ростов-н/Д., 2004. С.69-70.; Иванова Я. Е. Незаконное предпринимательство: вопросы теории и проблемы правоприменения: автореферат дис.... канд. юрид. наук. М., 2010. С.7-12; Урда М. Н. Проблемы применения нормы, устанавливающей ответственность за незаконное предпринимательство. Курск, 2010. С.30; Виноградов С.П. Противодействие незаконному предпринимательству: криминологический и уголовно-правовой аспекты: дис... канд. юрид. наук. М., 2006. С. 92-100; Авдеева О.А. Незаконное предпринимательство: уголовно-правовая характеристика и ответственность: дис... канд. юрид. наук. Иркутск, 2009.С.57-60.

лишь проверять состояние счета или осуществлять безналичный расчет в киберпространстве, однако с развитием телекоммуникационных технологий появилась возможность открывать счета, вклады и оформлять кредиты через сеть «Интернет». Данные операции являются банковскими и, в соответствии со статьёй 13 Федерального закона «О банках и банковской деятельности»[1], осуществление таких операций производится только на основании лицензии, выдаваемой Банком России. Осуществление подобной деятельности без таковой может образовать состав преступления 172 УК РФ «Незаконная банковская деятельность»[2].

Так, благодаря появлению в киберпространстве таких систем оборота денежных средств, как PyaPal (США), WebMoney (СНГ) и других, стало возможным осуществлять банковские операции вовсе без регистрации и лицензии[3].

На наш взгляд, не имеет уголовно-правового значения, где и каким способом была осуществлена банковская услуга (в материальном или виртуальном мире, посредством привычных банковских операций или с помощью цифровых сервисов в киберпространстве), если по своей природе такая деятельность является банковской. В случае причинения такой деятельностью крупного ущерба гражданам, организациям или государству, либо при извлечении дохода в крупном размере и осуществлении её без регистрации либо лицензии, образует состав преступления «незаконная банковская деятельность». Как в случае с незаконной предпринимательской деятельностью, данное деяние, совершенное в киберпространстве, необходимо квалифицировать только по статье 172 УК РФ, без совокупности со статьями главы 28 УК РФ.

---

[1]Федеральный закон от 2 декабря 1990 N 395-1 (ред. от 30 сентября 2013) «О банках и банковской деятельности»// Собрание законодательства РФ. 1996. N 6. Ст. 492.

[2]См.: Мильчехина Е.В. Уголовно-правовой и криминологический анализ незаконной банковской деятельности: автореф. дис.... канд. юрид. наук. Екатеринбург, 2010. С. 10-12.; Саркисян А.Ж. Незаконная банковская деятельность: уголовно-правовые аспекты: дис... канд. юрид. наук. Ростов-н/Д., 2007. С. 79-83.; Зотов П.В. Уголовно-правовая и криминологическая характеристика незаконной банковской деятельности: автореферат дис.... канд. юрид. наук. М., 2007. С.10-12.

[3]Побегайло А.Э. Киберпреступность: лекция. С. 35

При этом, поскольку в киберпространстве появилась возможность получить кредит, то появился и новый способ совершения преступления, предусмотренного статьёй 176 УК РФ «Незаконное получение кредита».

На наш взгляд, предоставление банку заведомо ложных сведений о хозяйственном положении либо финансовом состоянии индивидуального предпринимателя или организации в киберпространстве может сформировать состав преступления, предусмотренного статьёй 176 УК РФ.

В случае если заведомо ложные сведения о своём финансовом положении банку предоставит не индивидуальный предприниматель или организация, а физическое лицо, то такое деяние необходимо квалифицировать по статье 159.1 УК РФ как «Мошенничество в сфере кредитования».

Отдельно стоит упомянуть об организации и проведении азартных игр, поскольку данная деятельность в киберпространстве является более распространённой по сравнению с незаконной предпринимательской либо банковской деятельностью.

Более того, в диспозиции части 1 статьи 171.2 УК РФ прямо указано, что организация и (или) проведение азартных игр с использованием информационно-телекоммуникационных сетей, в том числе сети «Интернет», а также средств связи, в том числе подвижной связи (через мобильный телефон или SMS), сопряженное с извлечением дохода в крупном размере, подлежит уголовной ответственности.

Представляется, что азартные игры следует отграничить от развлекательных компьютерных игр в сети «Интернет», поскольку последние могут быть основаны на азарте.

Согласно пункту 1 статьи 4 Федерального закона №244-ФЗ[1] от 29 декабря 2006 года, под азартной игрой понимается основанное на риске соглашение о выигрыше, заключенное двумя или несколькими участниками такого соглашения между собой либо с организатором азартной игры по правилам, установленным

[1]Федеральный закон от 29.12.2006 N 244-ФЗ (ред. от 23.07.2013) «О государственном регулировании деятельности по организации и проведению азартных игр и о внесении изменений в некоторые законодательные акты Российской Федерации»// Собрание законодательства РФ. 2007. N 1(1ч.). Ст. 7.

организатором азартной игры. При этом, если выигрыш (п. 3) в азартной игре может быть выражен как в форме денежных средств, так и другого имущества или права на него, то ставки, согласно п. 4 данного Закона, должны быть выражены исключительно в виде денежных средств.

В киберпространстве распространены Интернет-казино, покерные турниры, виртуальные рулетки, а также эмуляторы игровых автоматов, которые не могут быть признаны азартными играми, так как ставки в подобных играх осуществляются без денежных средств. Игровая валюта, используемая в таких играх, предназначена для развлечения и удобства пользователей, но не для получения реального выигрыша, так как данный выигрыш невозможно вывести из игры и тем более из киберпространства в материальный мир. Более того, во многих из них отсутствует возможность даже вносить денежные средства.

Однако в погоне за прибылью организаторы Интернет-казино в качестве игровой валюты нередко используют реальные денежные средства, то есть принимают ставки и выплачивают выигрыши электронными либо безналичными денежными средствами, BTC или иной криптовалютой. В таком случае подобная деятельность уже является незаконной, и в случае извлечения дохода в размере 1,5 миллиона рублей данное деяние образует состав преступления, указанного в статье 171.2 УК РФ.

За последние годы на территории Российской Федерации было закрыто несколько десятков незаконных Интернет-казино, самыми громкими из которых стало закрытие сайта «White Club» [1] и «Goldfishka»[2]. Данные Интернет-казино осуществляли преступную деятельность около 10 лет и предлагали около 500 видов азартных игр, их жертвами стало несколько тысяч пользователей. Примерный доход каждого Интернет-казино составлял десятки миллионов рублей в год, а размер одной ставки мог достигать 20 тысяч рублей. Примером из

[1]Информационный ресурс «Over Betting». Закрыто Интернет казино White Club [Электронный ресурс] // URL: http://www.overbetting.ru/news/casino/zakryto-internet-kazino-white-club.html (Дата обращения: 24.06.2013).

[2]Информационный ресурс «Казино 367». Закрыта Голдфишка. [Электронный ресурс] URL: http://casino367.com/news/close-golfishka-2/ (Дата обращения: 24.06.2013).

судебной практики может служить уголовное дело об «Омском Интернет-Казино».

М., являясь фактическим руководителем ряда компьютерных клубов, организовал и проводил азартные игры с использованием игрового оборудования и информационно-телекоммуникационных сетей, в том числе сети «Интернет» вне игорной зоны.

В соответствии с установленными М. правилами проведения азартных игр, посетители клубов (игроки), имеющие ограниченный доступ в помещение игрового зала, с целью участия в азартных играх, заключали основанное на риске соглашение лично с М. либо с администраторами игрового зала, действовавшими в интересах М., передавая им денежные средства. После этого выбирали для игр один из персональных компьютеров, расположенных в указанных помещениях. Получив от игрока денежные средства, администраторы, используя определенную комбинацию клавиш на компьютерной клавиатуре, начисляли игроку кредиты – условные денежные средства в сумме, эквивалентной денежным средствам, полученным от игрока, из расчета 1 рубль Российской Федерации за 1 кредит. Затем игроки самостоятельно, используя компьютерную клавиатуру, осуществляли запуск случайной смены символов, выведенных на экран. В зависимости от произвольно выпавшей комбинации символов посетитель мог выиграть или проиграть в азартной игре. При наличии выигрышной комбинации на мониторе компьютера происходило увеличение имеющихся в распоряжении игрока кредитов, а в случае проигрыша – их уменьшение. В результате выигрыша игрока в азартной игре администраторы выплачивали ему денежные средства с учетом внесенных игроком денежных средств в сумме, эквивалентной количеству выигранных кредитов, из расчета 1 рубль Российской Федерации за 1 кредит.

При проигрыше денежные средства, переданные игроком администраторам и начисленные на компьютеры в виде

кредитов, обращались в доход М. В результате преступных действий М. извлёк доход в сумме 1 820 000 рублей[1].

Основываясь на вышесказанном, можно сделать следующие выводы о данных составах киберпреступлений, совершаемых в сфере экономической деятельности:

1. в киберпространстве сложились все условия для осуществления незаконной предпринимательской и банковской деятельности, а также для организации и проведении азартных игр;

2. поскольку для осуществления данных киберпреступлений виновный использует уже существующую инфраструктуру и не причиняет вреда отношениям, складывающимся в сфере компьютерной информации, то дополнительной квалификации по статьям главы 28 УК РФ, как правило, не требуется;

3. осуществление данных киберпреступлений создаёт условия для образования в нём теневой экономики и «черного рынка» товаров и услуг, что без должного правового регулирования может причинить существенный ущерб всему обществу.

Легализация (отмывание) денежных средств. Легализация денежных средств и иного имущества, приобретённого преступным путём, является преступлением международного уровня, для противодействия которому было принято множество международных соглашений и конвенций (Конвенция Совета Европы об отмывании, выявлении, изъятии и конфискации доходов от преступной деятельности (Страсбург, 8 ноября 1990 г.), Конвенция ООН против транснациональной организованной преступности (Нью-Йорк, 15 ноября 2000 г.) и многие другие).

Международный характер данного преступления обосновывается, в том числе, и способом его совершения, так как многие фиктивные финансовые

[1]Приговор Куйбышевского районного суда города Омска от 05.02.2014 по делу N 1-53/2014(1-476/2013;) ст.171.2 ч. 1; ст. 291 ч. 3 УК РФ.// СПС «КонсультантПлюс».

операции являются международными трансакциями. Однако если 10-20 лет назад такие операции осуществлялись исключительно банками, то сегодня международный перевод денежных средств можно совершить в киберпространстве.

Благодаря своей анонимности и трансграничности киберпространство даёт почти неограниченные возможности по приданию легальной формы преступному доходу. Так, по мнению Е.Л. Логинова, поскольку «Интернет» становится местом осуществления мировой торговли, возникают возможности отмывания денег по счетам-фактурам или в обход их, что открывает новые способы легализации[1]. Данное обстоятельство создаёт множество трудностей в вопросах квалификации деяний, поиска и привлечения к ответственности виновных лиц, доказывании, а также создаёт условия для укрепления организованной киберпреступности.

Совершение данного киберпреступления создаёт сложности и в правоприменительной практике, поскольку способ его совершения носит сильно завуалированный характер.

Все способы легализации денежных средств в киберпространстве можно условно разделить на следующие группы:

- легализация денежных средств с использованием существующих сайтов (сайты-аукционы, сайты-объявления, социальные сети);
- легализация денежных средств с помощью открытия новых сайтов (Интернет-казино, Интернет-магазин);
- легализация денежных средств с использованием Интернет-банкинга;
- легализация денежных средств с использованием криптовалют.[2]

Одним из самых простых и распространённых способов легализации денежных средств является продажа несуществующего имущества через сайты-объявления (Avito.ru, irr.ru, board.sakh.com либо мобильные приложения). Злоумышленник создаёт несколько аккаунтов на сайте, регистрируясь под

[1]Логинов Е.Л. Отмывание денег через Интернет-технологии: Методы использования электронных финансовых технологий для легализации криминальных доходов и уклонения от уплаты налогов. М., ЮНИТИ-ДАНА. 2012. С.5.

[2] Простосердов М.А. Легализация (отмывание) денежных средств в киберпространстве // Российское правосудие. 2014. № 9(101) С. 75 – 80.

разными именами с разных IP-адресов. Часть ложных аккаунтов используется как «Продавцы», вторая – «Покупатели». В качестве «Продавца» преступник выставляет на сайте разнообразные предметы, не требующие специальных документов и регистрации права собственности (компьютеры, телевизоры, драгоценности, картины). Данных предметов у злоумышленника нет, то есть объявления фиктивны. В качестве «Покупателя» виновный использует денежные средства, полученные преступным путём. На первом этапе он переводит их в электронную валюту через терминалы оплаты (Яндекс.деньги, Webmoney, Киви) на заранее созданные ложные аккаунты самих электронных денежных систем, на следующем этапе происходит ряд мелких переводов с этих аккаунтов на электронные кошельки ложных аккаунтов «Покупателей» на сайте объявлений. Далее преступник от имени каждого из «Покупателей» приобретает несуществующие предметы, которые он же и выставил на продажу в качестве «Продавца». Полученный доход переводится на действительный банковский счет и может быть снят в любом банкомате. В качестве подтверждения дохода виновный может предоставить выписки из истории покупок сайта или иные документы, свидетельствующие о теперь уже легальном характере дохода.

Осуществив данные финансовые операции, виновный придаёт «грязным» денежным средствам правомерный вид, тем самым совершает преступление, предусмотренное статьёй 174 УК РФ («легализация (отмывание) денежных средств, полученных преступным путём»)[1].

Схожая ситуация на сайтах-аукционах. Преступник создаёт множество ложных аккаунтов на сайте Интернет-аукциона. С одного выставляет предмет на

[1]Подробнее см.: Шебунов А. А. Легализация денежных средств и иного имущества, приобретенных незаконным путем: дис... канд. юрид. наук. М., 1998. С. 12-13; Рыбаков Д. В. Легализация денежных средств или иного имущества в российском уголовном праве: дис... канд. юрид. наук. М., 2002. С. 15-25; Гусейнова С.М. Проблемы уголовно-правовой регламентации легализации (отмывания) денежных средств или иного имущества, приобретенных преступным путем: дис... канд. юрид. наук. Ростов-н/Д., 2003. С. 60-72.; Педун О. Л. Легализация денежных средств или иного имущества, приобретенных преступным путем: дис... канд. юрид. наук. М., 2004. С. 51-72; Тер-Аванесов И.Г.Легализация денежных средств или иного имущества, приобретенных преступным путем: дис... канд. юрид. наук. Ставрополь, 2005. С. 30-33; Радзевановская Ю. В. Легализация (отмывание) денежных средств или иного имущества, приобретенных преступным путем: Уголовно-правовая и криминологическая характеристика: дис... канд. юрид. наук. Уфа, 2005. С.37-52; Кузахметов Д. Р. Легализация (отмывание) денежных средств или иного имущества, приобретенных преступным путем: Вопросы теории, законодательного регулирования и практики: дис... канд. юрид. наук. Казань, 2006. С.47-50; Мусаев Ф.А. Преступления против общего порядка осуществления экономической деятельности (ст. 171, 172-174.1 УК РФ): вопросы законодательной техники и дифференциации ответственности. Ярославль, 2005. С. 30-45

аукцион, а с остальных создаёт ложный спрос, искусственно повышая цену. Виновный в одном лице является как продавцом, так и покупателем, а для оплаты использует оговорённую выше схему.

Особенностью данных способов является то, что их может осуществить всего один человек, при этом не обладающий специальными техническими знаниями, так как он будет использовать уже существующую инфраструктуру. Также при должном знании в области программирования преступник может автоматизировать процесс. Написав вредоносную программу, которая будет за него регистрироваться под разными именами и осуществлять простые финансовые операции, либо создав «бот-сеть», заразив множество компьютеров вирусом, преступнику достаточно будет лишь вовремя вносить «грязные» денежные средства в терминалы оплаты и получать «чистый» доход на банковский счет.

В случае если для совершения преступления виновный осуществит неправомерный доступ к чужой компьютерной информации или использует вредоносные программы, повлекшие уничтожение, блокирование, модификацию, копирование или нейтрализацию средств защиты компьютерной информации, то данное деяние следует квалифицировать по совокупности статей 174, 272 и 273 УК РФ соответственно.

Система легализации денежных средств, полученных преступным путём с использованием Интернет-магазина, немного сложнее, чем с использованием сайтов-объявлений или сайтов-аукционов, однако принцип тот же. Для отмывания денежных средств преступник не регистрируется на существующем сайте, а создаёт и регистрирует свой. Процесс создания и регистрации сайта-магазина во многом сложнее, чем простая регистрация на уже готовом сайте. Нередко владельцы подобных сайтов регистрируются в качестве индивидуальных предпринимателей, по всем правилам, предусмотренным законодательством, чтобы избежать внимания правоохранительных органов. Однако в таких магазинах, как правило, отсутствуют как покупатели, так и товары, а финансовые

операции происходят исключительно с «грязными» денежными средствами по разнообразным схемам.

Ещё более сложной системой легализации денежных средств является система с использованием Интернет-казино. Сложность заключается в том, что подобные казино, как правило, открываются на серверах, за пределами России, а доступ к ним может быть осуществлён с любой точки планеты, где есть доступ к сети «Интернет». Как правильно отмечает Л.Е. Логинов, для отмывания денег с помощью «онлайновых азартных игр» злоумышленники используют оборудование, расположенное в офшоре, к примеру, на Карибских островах[1]. В остальном система легализации денежных средств через Интернет-казино ничем не отличается от легализации денег через простые казино и игорные дома в материальном мире: электронные деньги, полученные преступным путём выдаются за выручку Интернет-казино, а вместо посетителей выступают «Бот-программы». Тем самым винновые лица придают «грязным» деньгам легальный вид, а в качестве подтверждения используют всевозможные записи о якобы существующих посетителях.

Интернет-магазины или Интернет-казино, как правило, используются для отмывания денежных средств, полученных преступным путём в особо крупном размере. При этом для поддержания нормального функционирования таких сайтов необходим постоянный контроль за оборудованием и финансовыми операциями. Подобная система может существовать на постоянной основе во многих преступных сообществах (организациях) либо являться самостоятельной устойчивой преступной структурой уровня организованной группы. Следовательно, данное деяние необходимо квалифицировать по части 4 статьи 174 УК РФ. В случае осуществления неправомерного доступа к компьютерной информации либо использования «Бот-программ» возникает необходимость в квалификации по совокупности со статьями 272 и 273 УК РФ соответственно.

[1]Логинов Е.Л. Отмывание денег через Интернет-технологии: Методы использования электронных финансовых технологий для легализации криминальных доходов и уклонения от уплаты налогов. С.5.

Использование Интернет-банков или иных кредитных организаций, имеющих систему обслуживания клиентов через «Интернет», для отмывания денег – не редкость. Для перевода денег в киберпространстве Интернет-банками создаются специальные системы обслуживания: пластиковые карты («CyberPlat», «Instant») или предоставление доступа к счетам напрямую через «Интернет», выпуск собственной Интернет-валюты (т.н. цифровые жетоны) и т.д. При этом многие банки не контролируют поток такой Интернет-валюты и даже не взимают комиссию за перевод, что создаёт условия для легализации «грязных» денежных средств с помощью данной системы.

К примеру, в 1994 году международная платёжная система «MasterCard» выпустила карты «Mondex», предназначенные для платежей в киберпространстве или через платёжные POS-терминалы. Сами карты содержат микрочип, который, по сути, и является электронным кошельком. Преимущество карт Mondex перед простыми дебетовыми и кредитными банковскими картами заключается в том, что они дают возможность переводить деньги с карты на карту, минуя банковский счет лишь посредством сети «Интернет». Такая система лишает эмитента возможности контролировать платежи и создаёт условия для легализации преступного дохода[1].

В России схожая система используется в картах «QIWI Wallet» от «Visa», для приобретения которых не требуются ни паспортные данные, ни какие-либо другие документы, а только номер телефона. Эти особенности делают держателей данных карт анонимными и создают все условия для отмывания денег.

В случае осуществления финансовых операций с «грязными» денежными средствами с помощью Интернет-банкинга возникает серьёзная опасность придания краденным денежным средствам правомерного вида, что усложняет процесс доказывания и привлечения виновных к уголовной ответственности. К примеру, если виновное лицо с использованием подобной банковской карты осуществит перевод краденых денег через «Интернет» на другую карту, то данную операцию будет невозможно проследить, однако запись о пополнении

[1]Там же.

карты останется. Данное деяние также необходимо квалифицировать как легализацию (отмывание) денежных средств в соответствии со статьёй 174 УК РФ.

Ещё одним способом легализации посредством использования киберпространства могут являться финансовые операции с криптовалютой, а именно с системой «Биткоин» (BTC).

Трансакции BTC мгновенные, анонимные и проходят по всему миру, при этом за них не взимается комиссия, что также создаёт условия для легализации преступного дохода. К примеру, 22 ноября 2013 года был зарегистрирован рекордный анонимный перевод BTC с одного счета на другой в размере 194 993 BTC, что на то время составило примерно 4,5 миллиарда рублей без какой-либо комиссии, при этом не было известно происхождение данной суммы[1].

Согласно Информационному сообщению «Об использовании криптовалют» Федеральной службы по финансовому мониторингу Российской Федерации использование криптовалют (включая BTC) при совершении сделок является основанием для рассмотрения вопроса об отнесении таких сделок (операций) к сделкам (операциям), направленным на легализацию (отмывание) доходов, полученных преступным путем, и финансирование терроризма[2].

Виновный может приобрести некоторое количество криптовалюты на «грязные» деньги и, осуществив несколько анонимных финансовых операций в сети «Интернет» или сети «TOP», придать им правомерный вид, продав криптовалюту на стороннем сайте-аукционе либо обменяв её на настоящие деньги в иностранных банках, тем самым совершив их легализацию.

На сегодняшний день использование криптовалюты для отмывания денег представляет наибольшую опасность, поскольку данный феномен объективно не изучен ни законодателем, ни судом. Анонимность пользователей систем

[1]Среднесрочный прогноз «Биткойн» от сайта «Matbea», Форум «Биткойн» [Электронный ресурс] // URL: http://blog.matbea.com/194993btc/(Дата обращения: 24.04.2014).

[2]Информационное сообщение Росфинмониторинга «Об использовании криптовалют» // СПС «КонсультантПлюс».

«Биткойн», анонимность самих финансовых операций и их международный характер значительно усугубляют сложившуюся обстановку.

Основываясь на вышесказанном, можно с определённой уверенностью утверждать, что:

1. сеть «Интернет» и образованное ею киберпространство создали уникальную среду и уникальные условия для осуществления преступной деятельности, в частности, для легализации денежных средств, полученных преступным путём;

2. совершение легализации денежных средств в киберпространстве создаёт трудности в правоприменительной практике, что приводит к необходимости совершенствования отечественного уголовного законодательства и принятия новой редакции Постановления Пленума Верховного Суда РФ «О судебной практике по делам о незаконном предпринимательстве и легализации (отмывании) денежных средств или иного имущества, приобретенных преступным путем»[1].

Принуждение к совершению сделки или к отказу. Состав принуждения к совершению сделки или к отказу от её совершения (ст. 179 УК РФ) по своей конструкции схож с составом вымогательства (ст. 163 УК РФ), однако данные преступления отличаются объектом посягательства. Данное преступление направлено уже не на отношения собственности, а на отношения в сфере экономической деятельности, поскольку общественно опасное деяние направлено на совершение сделки либо на отказ от неё[2].

С объективной стороны, как и при вымогательстве, виновный может высказать требование о совершении сделки в киберпространстве (в чате или по электронной почте), подкрепив её угрозой применения насилия, уничтожения или

---

[1] Простосердов М.А. Легализация (отмывание) денежных средств в киберпространстве // Российское правосудие. 2014. № 9(101). С. 75 – 80.

[2] См.: Субботина И. В.Уголовная ответственность за принуждение к совершению сделки или отказу от ее совершения: дис... канд. юрид. наук. Пятигорск, 2006. С.56-59; Нафиков И.И. Принуждение к совершению сделки или отказу от ее совершения: криминологические и уголовно-правовые аспекты: автореф. дис.... канд. юрид. наук. М., 2012.С. 10-13.

повреждения чужого имущества, или угрозой распространения сведений, которые могут причинить существенный вред правам и законным интересам потерпевшего или его близких. В данном случае виновный своими деяниями совершит преступление, предусмотренное статьёй 179 УК РФ.

Представляется, что для квалификации данного преступления не имеет особого значения, каким способом потерпевшему было доведено требование и соответствующая угроза (лично или через электронную почту), если потерпевший воспринял данную угрозу как реальную. В связи с этим, по нашему мнению, наиболее исполнимым из способов принуждения к совершению сделки в киберпространстве может быть угроза распространения сведений. Так, например, возможна следующая ситуация.

В. и П., являясь конкурентами, вступили в конфликт, поскольку П. заключил контракт с некой коммерческой организацией, которой ранее интересовался В. Через электронную почту В. наставал на том, чтобы П. отказался от контракта, однако тот стоял на своём. В итоге В., совершив неправомерный доступ к компьютерной информации потерпевшего П., взломал его электронную почту и получил конфиденциальную информацию о нём (фото), распространение которой может причинить существенный вред правам и законным интересам П. Затем виновный повторил требование об отказе от контракта, подкрепив угрозой распространения данных сведений, прикрепив к письму фотографию. П., удостоверившись, что виновный действительно обладает данными сведениями, расценил угрозу как реальную и обратился в полицию.

В данной теоретической ситуации виновный совершил два преступления: неправомерный доступ к компьютерной информации (ст. 272 УК РФ) и принуждение к отказу от совершения сделки (ст. 179 УК РФ), поскольку состав данного преступления носит формальный характер и не имеет особого значения, был ли осуществлён отказ от сделки либо нет.

При этом аналогично статье 163 УК РФ помимо перечисленных выше способов принуждения к совершению сделки или к отказу от ее совершения сформировался новый – угроза уничтожения, блокирования либо модификации

компьютерной информации, и угроза иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей (угроза DDoS-атаки).

Как и в случае с вымогательством, данный способ выходит за пределы объективной стороны преступления, указанного в статье 179 УК РФ, а дополнительная квалификация по совокупности со статьями 272 или 273 УК РФ не решает проблему квалификации. В то же время, поскольку реализация данной угрозы может также причинить существенный вред правам и законным интересам потерпевшего или его близких (заблокировав сайт, попросту довести Интернет-магазин до банкротства), то, по нашему мнению, часть 1 статьи 179 УК РФ необходимо изложить в следующей редакции:

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.

Данное нововведение внесёт ясность в процесс квалификации деяния и уменьшит возможность судебной ошибки. Примечательно, что большинство опрошенных судей районных и областных судов (61%, 39 чел.) считают данное обстоятельство фактором, повышающим общественную опасность деяния, и указывают, что совершение данного преступления под угрозой DDoS-атаки

необходимо выделить в качестве квалифицирующего признака, а 39% (25 чел.) предлагают выделить данное преступление в самостоятельный состав.[1]

Однако, на наш взгляд, данное обстоятельство является лишь новым характером угрозы при совершении преступления, предусмотренного статьёй 179 УК РФ. Аналогично случаю с вымогательством такая угроза не наносит вреда дополнительному объекту и не повышает ни характер, ни степень общественной опасности деяния. Следовательно, такое преступление можно квалифицировать только по статье 179 УК РФ, без совокупности со статьёй 272 УК РФ. При решении вопроса о редакции уголовного законодательства такое обстоятельство должно быть выражено лишь в качестве нового характера угрозы в рамках основного состава статьи 179 УК РФ, но никак не в качестве квалифицирующего признака либо нового состава. Представляется, что данное деяние необходимо квалифицировать по совокупности со статьями 272 и 273 УК РФ только в случае реализации DDoS-атаки.

Основываясь на вышесказанном, можно сделать следующие выводы о данном киберпреступлении:

1. принуждение к совершению сделки, а также отказу от её совершения может быть реализовано путём угрозы применения насилия, уничтожения или повреждения чужого имущества, распространения сведений, которые могут причинить существенный вред правам и законным интересам потерпевшего или его близких, а также угрозы 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;

2. поскольку такое деяние выходит за пределы статей 179 и 272 УК РФ, возникла необходимость в редакции уголовного законодательства.

[1] См.: Приложение №2. Опросный лист.

Незаконное использование средств индивидуализации товаров (работ, услуг). Большинство коммерческих сайтов, осуществляющих предпринимательскую деятельность в киберпространстве, для собственной индивидуализации используют запоминающиеся эмблемы, логотипы и названия. Нередко они регистрируют их как товарный знак, в качестве которого в сети «Интернет» может выступать и само доменное имя сайта (google.com, yandex.ru, raj.ru и др.)[1]. В то же время по данным «CERT-GIB» в 2013 году было зафиксировано более 500 обращений о защите брендов и товарных знаков в киберпространстве[2].

Один из первых примеров незаконного использования товарного знака с использованием компьютерных технологий в России был зафиксирован ещё в 1998 году.

Г. и Б., действуя по предварительному сговору, в период с ноября 1998 по октябрь 1999 года, без разрешения правообладателя рекламировали продукцию агентства «Р» (программы – информационные терминалы), используя зарегистрированный товарный знак агентства, и незаконно продавали её. Установив на компьютеры различных фирм информационные терминалы агентства «Р», также содержащие её товарный знак, Г. и Б. причинили правообладателю крупный ущерб. Г.и Б. были признаны виновными в совершении преступления, предусмотренного частью 1 статьи 180 УК РФ[3].

Сегодня такие товарные знаки могут быть использованы на сайтах-клонах, которые внешне ничем не отличаются от оригинальных сайтов, за исключением

---

[1]Подробнее см.: Постановление Пленума Верховного Суда РФ от 26.04.2007 N 14 «О практике рассмотрения судами уголовных дел о нарушении авторских, смежных, изобретательских и патентных прав, а также о незаконном использовании товарного знака»// СПС «КонсультантПлюс»; Склярук С.А.Уголовная ответственность за незаконное использование товарного знака: дис... канд. юрид. наук. М., 1999. С.10-12; Демьяненко Е. В. Уголовная ответственность за незаконное использование товарного знака: дис... канд. юрид. наук. Ростов-н/Д., 2003. С.13-15.; Кондрашина В. А. Уголовная ответственность за незаконное использование товарного знака по законодательству России и зарубежных стран: дис... канд. юрид. наук. Казань, 2004. С.10-13; Головизнина И. А. Незаконное использование товарного знака: проблемы квалификации и правоприменения: дис... канд. юрид. наук. М., 2008. С 15-19.; Жайворонок А. В. Незаконное использование товарного знака: криминологическое и уголовно-правовое исследование: дис... канд. юрид. наук. Омск, 2010. С.6-16; Трейгер С.М. Уголовная ответственность за незаконное использование товарного знака: дис... канд. юрид. наук. М., 2011. С.5-16;

[2]Анализ обращений в CERT-GIB за 2013 год... - Group-IB Расследование компьютерных преступлений. [Электронный ресурс] // URL: https://www.facebook.com/GroupIB/posts/640006572733415 (Дата обращения: 27.01.2014).

[3]Кесареева Т.П. Криминалистическая характеристика и проблемы предупреждения преступности в российском сегменте сети Интернет: дис…. канд.юрид.наук. М., 2002. С. 96.

одного-двух символов в доменном имени (www.sam**s**ung.com и www.sam**c**ung.com). Как правило, данные сайты создаются для совершения мошеннических действий, однако возможна ситуация, когда сайт-клон создаётся в целях предпринимательства. Также в связи с анонимностью киберпространства и его пользователей возможна ситуация, в которой преступники на Интернет-торгах представляются авторитетной организацией, используя её товарный знак.

*Так, С. и К. распространяли товар (сухие смеси) на электронной площадке «****» в сети "Интернет" под видом товара ООО «М» и ООО «Д», при этом используя зарегистрированные товарные знаки ООО «М» (свидетельство на товарный знак №*****) и ООО «Д» (свидетельство на товарный знак №*****). Виновные заключили несколько договоров с ИП «ФИО41» и ГУП «Таттехмедфарм». Само ООО «М» никогда никаких взаимоотношений с ИП «ФИО41» и ГУП «Таттехмедфарм» не поддерживало, соответственно, руководством ООО «М» было установлено, что некие лица самовольно занимаются поставками смесей, используя их имя и товарный знак.*

Своими неоднократными преступными действиями в результате незаконного использования чужого товарного знака С. и К. причинили крупный ущерб ООО «Д» на сумму 2 827 318 рублей 40 копеек и крупный ущерб ООО «М» на сумму 3 059 304 рублей 50 копеек[1].

С. и К. были признаны виновными в совершении преступления предусмотренного статьёй 180 УК РФ. Им было назначено наказание в виде лишения свободы на срок 3 и 2 года условно.

Чаще всего ущерб правообладателю товарного знака выражается в упущенной выгоде из-за безвозмездного использования его виновным лицом, а также из-за потери рынка сбыта товара или оказания услуг. Ущерб может выражаться также в утрате имиджа компании, если выдаваемая продукция была низкого качества и от услуг компании попросту стали отказываться.

[1]Приговор Приволжского районного суда города Казани от 28.02.2014 по делу N 1-13 2013;1-86 2012 ст.180 ч. 3 УК РФ// СПС «КонсультантПлюс».

В случае если виновный использовал вредоносные программы для привлечения пользователей и потенциальных покупателей (вирусы, СПАМ-программы), то такое деяние необходимо квалифицировать по совокупности со статьёй 273 УК РФ.

Однако само незаконное использование товарного знака в киберпространстве возможно и без подобных средств. В этом случае виновный для достижения своих преступных целей использовал ресурсы и возможности самого киберпространства и не причинил вреда отношениям в сфере компьютерной информации, следовательно, квалификация такого деяния должна осуществляться только по статье 180 УК РФ.

Дополнительная квалификация по совокупности со статьёй 272 УК РФ «Неправомерный доступ к компьютерной информации», на наш взгляд, потребуется только в случае, если для получения товарного знака виновный взломал почту или сервер потерпевшего, где хранился файл с товарным знаком.

Основываясь на вышесказанном, можно сделать следующие выводы по данному составу киберпреступления:

1. незаконное использование средств индивидуализации товаров в киберпространстве может прочинить такой же ущерб правам и законным интересам правообладателя, что и их незаконное использование в материальном мире;

2. использование вредоносных компьютерных программ и незаконный доступ к компьютерной информации при незаконном использовании средств индивидуализации товаров, работ и услуг (ст. 180 УК РФ) необходимо квалифицировать по совокупности преступлений со статьями 272 и 273 УК РФ.

Незаконное получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну. Деяние, предусмотренное статьёй 183 УК РФ (незаконное получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну), является самым распространённым киберпреступлением, совершаемым в сфере экономической

деятельности (83% от киберпреступлений в сфере экономической деятельности, что составляет 10% от общего числа экономических киберпреступлений).[1]

«Электронный коммерческий шпионаж», то есть незаконное получение сведений, составляющих коммерческую, налоговую, банковскую тайну, посредством компьютерной техники, выведен в отдельную статью во многих странах мира, таких как Испания, Нидерланды, Финляндия, Швейцария. Однако в отечественном законодательстве такой нормы нет. Это связано с тем, что на практике такое деяние квалифицируется по совокупности со статьями 272 либо 273 УК РФ, что отражает повышенную общественную опасность, поскольку при совершении данного преступления виновный нарушает сразу две группы общественных отношений – в сфере экономической деятельности и компьютерной информации.

Как указывает М.М. Лапутин, собирание сведений, составляющих коммерческую, налоговую, банковскую тайну, путём неправомерного доступа к компьютерной информации следует квалифицировать по совокупности преступлений, предусмотренных статьями 183 и 272 УК РФ, так как объективная сторона преступления выходит за пределы предусмотренных статьёй 183 УК РФ.[2]

Однако, по нашему мнению, такая квалификация не точна, что может быть связано с двойственной природой сведений, составляющих коммерческую, налоговую или банковскую тайну, поскольку такие сведения могут быть представлены, в том числе, в форме компьютерной информации (файла). Представляется, что такие деяния следует квалифицировать по совокупности только тогда, когда помимо копирования сведений виновное лицо совершит их модификацию, уничтожение или блокирование, поскольку само по себе копирование является разновидностью собирания сведений, то есть частью объективной стороны преступления, предусмотренного статьёй 183 УК РФ, и полностью охватывается ею. С данной квалификацией согласно 48% (46 чел.)

[1] См. Приложение №3. Таблица работы с судебными документами

[2] Лапутин М.М. Уголовная ответственность за неправомерный доступ к компьютерной информации: общая характеристика и некоторые проблемы квалификации.// Библиотека криминалиста. 2013. №5(10) С.31.

опрошенных судей, при этом лишь 34,4% (33 чел.) настаивает на квалификации по совокупности, а 17,6 % (17 чел.) затруднились ответить.[1] Другими словами, возможна лишь реальная совокупность преступлений, что подтверждается следующим примером из судебной практики.

«Г», являясь работником ЗАО «1», используя электронную почту, незаконно собрал и распространил сведения, составляющие коммерческую тайну, без согласия ЗАО «1». Меры, принятые акционерным обществом по охране конфиденциальности информации, в целом соответствуют ст. 10 ФЗ «О коммерческой тайне», в обществе действовала экспертная комиссия.

«Г» был ознакомлен с правилами использования ресурсов сети Интернет под роспись, предупрежден об ответственности за несанкционированную отправку в Интернет информации, составляющей коммерческую тайну, и о недопустимости отправки через электронную почту такой информации. Правомерный доступ к незаконно собранным и впоследствии разглашенным сведениям коммерческой тайны осужденный не имел – он их «похитил». С учетом образования (высшее экономическое и юридическое), опыта работы, способа совершения преступления, характера незаконно собранных и разглашенных сведений осужденный понимал, какие конкретно сведения он собирал и разгласил. «Г» был признан виновным в совершении преступлений, предусмотренных частями 1 и 2 статьи 183 УК РФ[2].

Иная ситуация с использованием вредоносных компьютерных программ (ст. 273 УК РФ) в целях получения доступа к коммерческой тайне. В случае собирания сведений посредством таких программ квалификация по совокупности необходима.

Автозаводским районным судом города Тольятти Самарской области был осужден сотрудник ОАО «Авто ВАЗ» З., который с помощью вредоносной программы, позволяющей копировать из сети «Интернет» файлы, содержащие

[1] См.: Приложение №2. Опросный лист.
[2] Постановление Московского городского суда №4у/2-9352 от 05.12.2013 // СПС «КонсультантПлюс».

пароли, и «взламывать» их, получил служебные реквизиты доступа в сеть «Интернет», принадлежащие потерпевшему Г.

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 человеку[2]. 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

[1]Уголовное дело № 1-828/2004 год, архив Автозаводского районного суда г. Тольятти, Самарской области из материалов монографии / Дворецкий М.Ю., Копырюлин А.Н. Оптимизация уголовной ответственности и проблемы квалификации преступлений в сфере компьютерной информации. С.182.

[2] Волженкин Б.В. Преступления в сфере экономической деятельности по уголовному праву России / СПб., Юридический центр Пресс. 2007. С.462.

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 подписью[1]. Следовательно, с появлением нового способа предоставления документов появился и новый способ совершения

[1]Подробнее см.: официальный сайт ФНС РФ. [Электронный ресурс] // URL: http://www.nalog.ru/rn68/related_activities/registration_ip_yl/reg_yl/changes/3796283/ (Дата обращения: 26.04.2014).

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.

К примеру, злоумышленник может взломать компьютер, на котором содержится реестр и, внеся определённые изменения в реестр, он может незаконно стать акционером данного общества.

---

[1] Желудков М.А. Криминологический анализ содержания угрозы в виде рейдерства для общественных отношений собственности // Вестник Тамбовского университета. Серия: Гуманитарные науки. 2009. № 3 (71). С. 268-271.

Если целью виновного является только модификация данных, то неправомерный доступ, по нашему мнению, следует признать способом совершения такого преступления и данное деяние должно охватываться лишь частью 2 статьи 170.1 УК РФ. С данной квалификацией соглашается 67,1% (53 чел.) опрошенных судей.[1] Но если виновный помимо модификации скопирует или уничтожит какие-либо данные, то данное деяние всё же необходимо квалифицировать по совокупности преступлений, предусмотренных частью 2 статьи 170.1 и статьёй 272 УК РФ, то есть возможна лишь реальная совокупность.

Следующим видом киберпреступлений в сфере экономической деятельности являются преступления, связанные с использованием инсайдерской информации[2], которая, в свою очередь, может оказать существенное влияние на цены финансовых инструментов, иностранной валюты и (или) товаров, если она появится в СМИ или в киберпространстве. Нарушая установленный порядок обращения такой информации в киберпространстве, виновное лицо может совершить два различных преступления, предусмотренных Уголовным кодексом Российской Федерации: манипулирование рынком (ст. 185.3 УК РФ) и неправомерное использование инсайдерской информации (ст. 185.6 УК РФ).

Примером первого может служить уголовное дело, возбужденное по факту манипулирования ценой обыкновенных акций ОАО «ТАТБЕНТО» на торгах ЗАО «Фондовая биржа ММВБ».

*Организатором преступления являлся один из учредителей ОАО «ТАТБЕНТО», 35-летний ранее судимый за экономическое преступление гражданин Т. На сайте ОАО «ТАТБЕНТО» размещалась не соответствующая действительности информация о том, что предприятие занимается деятельностью по добыче ****, но в реальности данное юридическое лицо не осуществляло эту деятельность, и более того, вовсе не имело собственного*

[1] См.: Приложение №2. Опросный лист.

[2] Согласно статье 2 Федерального закона от 27.07.2012 №224-ФЗ «О противодействии неправомерному использованию инсайдерской информации и манипулированию рынком и о внесении изменений в отдельные законодательные акты Российской Федерации», под инсайдерской информацией понимается точная и конкретная информация, распространение или предоставление которой может оказать существенное влияние на цены финансовых инструментов, иностранной валюты и (или) товаров.

имущества. Данная ложная информация является инсайдерской, так как прямо влияет на цену акций компании. Преступная деятельность велась с сентября по декабрь 2010 года, цена на обычные акции ОАО «ТАТБЕНТО» выросла в 1,5 раза. В результате преступной деятельности злоумышленники получили необоснованный доход в размере 16 миллионов рублей[1].

В данном примере объектом преступления являются только экономические отношения, складывающиеся в сфере оборота инсайдерской информации и отношения в сфере экономической деятельности[2]. Отношения в сфере компьютерной информации не будут затронуты, так как сама информация не блокируется, не модифицируется и не удаляется – она имеет лишь ложный характер. Следовательно, данное деяние подлежит квалификации по статье 185.1 УК РФ, как манипулирование рынком, без совокупности со статьёй 272 УК РФ.

Представляется, что квалификация по совокупности с данной статьёй возможна лишь в случае, когда виновный помимо распространения заведомо ложной инсайдерской информации совершит неправомерный доступ к чужому компьютеру, сайту или аккаунту. Например, для манипулирования ценами на рынке и в целях собственной конспирации виновный взламывает сайт информационной службы и от имени авторитетного журналиста распространяет ложную инсайдерскую информацию. В данном случае действия виновного выходят за пределы статьи 185.3 УК РФ и, на наш взгляд, подлежат квалификации по совокупности со статьёй 272 УК РФ.

Распространение ложной инсайдерской информации в киберпространстве возможно разными способами: опубликование на сайте, на форуме, в социальной сети, при массовой рассылке по электронной почте и т.д. Поскольку распространение считается оконченным с момента, когда ложная инсайдерская информация была передана хотя бы одному человеку, то, следовательно, информация может быть распространена и при личной переписке через

[1]Козаев Н.Ш. Некоторые новеллы уголовного законодательства, направленные на обеспечение экономической безопасности в условиях научно-технического прогресса.// Библиотека криминалиста. 2013. №5(10). С.16.

[2]См.: Емельянова Е. А. Правовые последствия манипулирования информацией на рынках: автореф. дис.... канд. юрид. наук. СПб., 2013. С.7-10.

мгновенные сообщения в социальной сети или через частные письма по электронной почте.

Другое преступление, которое можно совершить в киберпространстве с использованием инсайдерской информации, – это её неправомерное использование (ст. 185.6 УК РФ).

В отличие от манипулирования рынком посредством распространения ложной инсайдерской информации, незаконное использование возможно только с действительной инсайдерской информацией. Следовательно, если лицо заблуждается в действительности такой информации, то, на наш взгляд, можно говорить о фактической ошибке.

Способы неправомерного использования инсайдерской информации в киберпространстве те же, что и в статье 185.3 УК РФ. Действительную инсайдерскую информацию можно распространить на сайтах, форумах, социальных сетях, опубликовать в Интернет-газете или «живом журнале».

Как и в случае с манипулированием рынком, при неправомерном использовании инсайдерской информации напрямую не нарушаются отношения, складывающиеся в сфере нормального оборота компьютерной информации, а объектом преступления являются лишь отношения в сфере экономической деятельности и отношения в сфере оборота инсайдерской информации. Компьютерная информация в данных случаях выступает лишь в качестве внешней формы выражения инсайдерской информации. Следовательно, такие деяния подлежат квалификации только по статье 185.6 УК РФ, без совокупности со статьёй 272 УК РФ.

В киберпространстве, на наш взгляд, также существует объективная возможность совершения ряда валютных и налоговых преступлений. К ним можно отнести совершение валютных операций по переводу денежных средств в иностранной валюте или валюте Российской Федерации на счета нерезидентов с использованием подложных документов (ст. 193.1 УК РФ), уклонение от уплаты налогов и (или) сборов с физических (ст. 198 УК РФ) и юридических лиц (ст. 199

УК РФ), а также сокрытие денежных средств, за счет которых должно производиться взыскание налогов и сборов (ст. 199.2 УК РФ).

При совершении преступления, предусмотренного статьёй 193.1 УК РФ, валютная операция совершается с предоставлением заведомо недостоверных сведений об основаниях, целях и назначении перевода лицом, обладающим правомочиями агента валютного контроля, на счета нерезидентов. Заведомо недостоверные или ложные сведения могут быть переданы в киберпространстве, к примеру, через систему электронного документооборота любого иностранного банка, предоставляющего данную услугу.

Используя возможности киберпространства и его популярность, многие банки не ограничивают максимальный размер валютных операций. Это значит, что всего одна валютная операция может причинить существенный ущерб экономическим интересам Российской Федерации и составить крупный (6 млн. руб.) или особо крупный размер (30 млн. руб.).

Следующим киберпреступлением в сфере экономической деятельности, которое можно совершить в киберпространстве, является фиктивное банкротство (ст. 197 УК РФ). Объективная сторона данного преступления заключается в публичном объявлении руководителем или учредителем (участником) юридического лица о несостоятельности его юридического лица, а равно индивидуальным предпринимателем о своей несостоятельности.

Признак публичности заключается в том, что деяние должно быть доведено до неопределённого круга лиц – если руководитель юридического лица в личной электронной переписке сообщит ложные сведения о несостоятельности своей компании только одному лицу, то такое деяния не сформирует состав преступления, предусмотренного статьёй 197 УК РФ.

Публичным объявлением в киберпространстве можно считать сообщение о несостоятельности организации на её официальном сайте, либо на публичной странице (т.н. «паблике») в социальной сети и т.д. В случае если ложное сообщение причинит крупный ущерб, то такое деяние необходимо квалифицировать по статье 197 УК РФ.

Примером налоговых киберпреступлений может служить уклонение от уплаты налогов, совершённое путём предоставления в налоговый орган заведомо недостоверных сведений в налоговой декларации через сеть «Интернет»[1]. Так, согласно части 4 статьи 80 НК РФ, налоговая декларация может быть предоставлена в налоговый орган в электронной форме по телекоммуникационным каналам связи с применением усиленной квалифицированной электронной подписи налогоплательщика[2].

Виновный при заполнении налоговой декларации в «личном кабинете» может умышленно указать ложные или недостоверные сведения об объектах налогообложения, о полученных доходах и произведенных расходах, об источниках доходов, о налоговой базе, налоговых льготах, об исчисленной сумме налога и (или) о других данных, служащих основанием для исчисления и уплаты налога.

Другое налоговое киберпреступление – это сокрытие денежных средств либо имущества организации или индивидуального предпринимателя, за счет которых должно производиться взыскание налогов и (или) сборов (ст. 199.2 УК РФ).

Представляется, что объективная сторона киберпреступления может заключаться в активном действии лица по сокрытию денежных средств путем безналичных расчетов через новые открытые расчетные счета или счета третьих лиц с помощью системы Интернет-банкинга[3]. Сокрытие денежных средств также может происходить посредством перевода безналичных денежных средств через электронные платёжные системы, такие как «Яндекс.Деньги» или «WebMoney», либо путём купли-продажи криптовалюты, к примеру, через систему «Биткойн». Как и в случае с манипулированием ценами на рынке, все выше оговорённые

[1]Информационный ресурс «Налог.ру» [Электронный ресурс] // URL: http://www.nalog.ru/rn77/news/activities_fts/4460907/ (Дата обращения: 08.01.2014).

[2]Налоговый кодекс Российской Федерации (часть первая) от 31 июля 1998 N 146-ФЗ (ред. от 28 декабря 2013) // Собрание законодательства РФ. 1998. №31. Ст. 3824.

[3]Постановление Пленума Верховного Суда РФ от 28.12.2006 N 64 «О практике применения судами уголовного законодательства об ответственности за налоговые преступления»// Бюллетень Верховного Суда РФ. 2007. N 3.

валютные и налоговые преступления, совершённые в киберпространстве, причиняют вред отношениям, складывающимся в сфере нормального оборота компьютерной информации, и, следовательно, не требуют дополнительной квалификации по статьям главы 28 УК РФ.

Основываясь на вышесказанном, можно с полной уверенностью утверждать, что развитие информационных технологий способствовало появлению в киберпространстве целого ряда экономических киберпреступлений, о совершении которых ещё 10-15 лет назад никто не мог и предположить. С появлением возможности дистанционно зарегистрировать юридическое лицо появилась возможность дистанционно фальсифицировать реестр данных лиц. С появлением возможности дистанционной оплаты налогов появился новый способ уклонения от их уплаты. Развитие электронных торгов и бирж открыло новую возможность манипулирования ценами на рынке.

В целом об экономических преступлениях, совершаемых в киберпространстве России, можно сделать следующие выводы:

1. самыми распространёнными преступлениями против собственности являются мошенничество (основной состав) и мошенничество в сфере компьютерной информации;

2. самыми распространёнными преступлениями в сфере экономической деятельности в Российской Федерации следует признать получение (разглашение) сведений, составляющих коммерческую, налоговую либо банковскую тайну, легализацию (отмывание) денежных средств, манипулирование рынком, незаконное использование средств индивидуализации товаров (работ, услуг), а также незаконную организацию и проведение азартных игр. Остальные преступления в судебной практике встречаются весьма редко, однако их совершение в киберпространстве всё же остаётся возможным;

3. отечественное уголовное законодательство нуждается в совершенствовании, как в отношении ряда преступлений против собственности, так и в отношении некоторых преступлений в сфере экономической деятельности;

4. предмет хищения необходимо расширить, включив в него цифровой информационный продукт, обладающий экономической и юридической значимостью;

5. возникла необходимость в принятии Постановления Пленума Верховного Суда Российской Федерации по вопросам квалификации компьютерных преступлений, а также преступлений, совершаемых в киберпространстве;

6. в целях разработки наиболее эффективных мер противодействия экономическим преступлениям, совершаемым в киберпространстве России, необходимо провести анализ причин и условий существования экономической киберпреступности, личности киберпреступника и личность его жертвы, а также провести анализ действующей уголовной политики по данному вопросу.

ГЛАВА 3
КРИМИНОЛОГИЧЕСКАЯ ХАРАКТЕРИСТИКА ЭКОНОМИЧЕСКИХ ПРЕСТУПЛЕНИЙ, СОВЕРШАЕМЫХ В КИБЕРПРОСТРАНСТВЕ

§ 1. Причины и условия экономической киберпреступности

В настоящем параграфе будут рассмотрены основные причины и условия в целом всей экономической киберпреступности, а не отдельных экономических киберпреступлений. Исходя из этого, под причинами преступности следует понимать такой вид детерминации, который неизбежно порождает преступность как своё следствие[1]; под условиями преступности следует понимать такой вид детерминации, который создаёт благоприятные возможности для формирования причин преступности либо для реализации последних[2].

Для более точного анализа все детерминанты экономической киберпреступности следует классифицировать по уровню субординации на:

•общие детерминанты экономической преступности – это совокупность причин и условий, характерных как для экономической киберпреступности, так и для всей экономической преступности в целом;

•специальные детерминанты экономической киберпреступности – это совокупность причин и условий, характерных лишь для экономической киберпреступности.

Общими детерминантами для всех экономических преступлений являются: экономический кризис, резкое снижение курса рубля, резкое повышение розничных цен на предметы первой необходимости (еду, одежду, коммунальные услуги), снижение уровня жизни, повышение уровня безработицы и т.д. Детерминанты экономической киберпреступности, на наш взгляд, обусловлены, в первую очередь, особенностями киберпространства и информационно-телекоммуникационных технологий. Потеряв работу в материальном мире и

[1]См.: Жариков Р.А. Детерминанты вымогательства и особенности его предупреждения в сверхкрупном городе: дис... канд. юрид. наук. Челябинск, 2004. С. 50-63; Корепанова И. А. Социальная специфика экономической преступности в современной России: дис... канд.соц.наук. Новочеркасск, 2011.С.47-50.

[2]Прозументов Л.М., Шеслер А.В. Криминология (общая часть). Томск, Томский филиал Академии ФСИН России. 2007. С. 135.

обладая специальными техническими знаниями в области программирования, зачастую легче найти стабильный источник заработка в виртуальной среде. Использование возможностей киберпространства облегчает процесс совершения преступления на каждом этапе, позволяет оставаться анонимным и не привлекать к себе лишнее внимание со стороны правоохранительных органов, снижает риск быть пойманным. Поэтому в связи с тематикой исследования особое внимание, на наш взгляд, следует уделить специальным детерминантам именно экономических киберпреступлений.

В ходе исследования был проведён опрос федеральных судей районных и областных судов Российской Федерации, участие в котором приняло 96 человек.[1] На вопрос «Каковы основные причины и условия существования экономической киберпреступности?» были получены данные, отражённые в Таблице №1.

Таблица №1

№	Кол-во ответов	Процент	Причины и условия
1.	**60**	**62,5%**	Анонимность
2.	**43**	**44,8%**	Несовершенство законодательства
3.	**39**	**40,6%**	Экстерриториальность киберпространства
4.	**33**	**34,4%**	Возможность получения сверхприбыли при минимальных затратах в киберпространстве
5.	**30**	**31,2%**	Техническое несовершенство киберпространства
6.	**26**	**27,1%**	Отсутствие единых и четких правил поведения в киберпространстве (отсутствие цифровой культуры)
7.	**23**	**24%**	Наличие субкультуры хакеров
8.	**19**	**19,7%**	Бездействие правоохранительных органов

Анонимность киберпространства, информационно-телекоммуникационных сетей и самих пользователей киберпространства, на наш взгляд, является одним

[1] См.: Приложение №2. Опросный лист.

из основных детерминантов возникновения киберпреступности. Если в материальном мире вор должен скрывать своё лицо и прикладывать определённые усилия, чтобы не оставлять следов совершения преступления, то в киберпространстве это уже сделано за него.

Анонимность киберпространства – это основной принцип его существования. Все пользователи сайтов, форумов или социальных сетей в киберпространстве изначально не имеют ни имён, ни внешнего вида – они эфемерны, и нередко информационные ресурсы сами присваивают таким пользователям имя «anonymous», то есть аноним. Выбрать имя и внешний вид сайты предлагают каждому своему пользователю самостоятельно и в подавляющем большинстве случаев пользователи злоупотребляют такой возможностью, представляясь чужими именами и используя чужие фотографии.

Следующий уровень анонимности – это сокрытие своих технических данных (IP-адрес, номер порта компьютера, потока данных и др.). Таким образом, создаются целые анонимные информационно-телекоммуникационные сети («TOP», «ANts P2P», «Freenet»).

Зарегистрировавшись под чужим именем, любой может безнаказанно обманывать, совершать анонимные платежи и переводы денежных средств, совершать хищения, вымогательства и иные экономические киберпреступления. Действующие способы вычисления виновных способны установить точное место, откуда виновный совершил вход в киберпространство, с точностью до квартиры, и приблизительную личность виновного, включая его национальную принадлежность[1], однако в самом киберпространстве существуют тысячи способов скрыть свою личность. Это подтверждают материалы судебной практики, где всё чаще используются такие формулировки как «неустановленное лицо», «в неустановленное время», «в неустановленном месте», «с неустановленного компьютера» и т.д.

Анонимно могут совершаться такие экономические киберпреступления, как мошенничество (основной состав), мошенничество в сфере компьютерной

[1]Материалы «Инфофорум-2014» Архив автора.

информации, вымогательство, получение сведений, составляющих коммерческую, налоговую или банковскую тайну, что составляет основную массу из общего количества экономических киберпреступлений.

На наш взгляд, анонимность в киберпространстве является основным детерминантом киберпреступлений и фактором высокого уровня латентности преступности в киберпространстве. Представляется, что наиболее эффективной мерой противодействия данной проблеме является персонализация доступа в киберпространство путём развития и внедрения биометрических технологий (сканера отпечатка пальцев, сканера лица пользователя).

Несовершенство законодательства создаёт условия для существования киберпреступности**.** Отечественный законодатель часто не успевает ответить на новые вызовы киберпреступников. Скорость развития киберпространства и скорость, с которой появляются новые способы совершения преступлений, превышает скорость реагирования на них со стороны государства. При этом, учитывая существующие сегодня и возможные в будущем технические уязвимости самого киберпространства, складывается мнение о неэффективности правового регулирования. Как было показано ранее, действующий Уголовный кодекс Российской Федерации вызывает ряд вопросов, поскольку его положения не были ориентированы на появление новых технологичных видов преступлений и новых способов их совершения.

На наш взгляд, разумное и строгое совершенствование уголовного законодательства должно стать неотъемлемой составляющей противодействия киберпреступности. Необходимо выделить использование киберпространства в целях совершения преступления, в качестве обстоятельства, отягчающего наказание; внести ясность в формулировку статьи 159.6 УК РФ в части используемого термина «мошенничество»; дополнить составы вымогательства и принуждения к совершению сделки новым характером угрозы (угроза уничтожения информации); дополнить статьи 170.1 и 183 УК РФ новым квалифицирующим признаком – «деяние, сопряженное с неправомерным доступом к компьютерной информации».

Пробелы отечественного уголовного законодательства в области противодействия киберпреступности создают условия для ухода виновных от ответственности, формируя тем самым чувство безнаказанности за содеянное, которое и побуждает хакеров на совершение всё новых преступлений.

Экстерриториальность киберпространства является важным детерминантом существования экономических киберпреступлений. Преступления, совершаемые с использованием сети «Интернет», нередко подпадают под несколько юрисдикций благодаря её глобальной и межгосударственной природе[1]. А.В. Суслопаров указывает, что специфическим признаком компьютерных преступлений является именно их интернациональный характер. Они могут совершаться на территории всего земного шара, где есть «Интернет». При этом для преступника будет неважно, в какой стране находится объект преступного посягательства[2].

По нашему мнению, следует согласиться с А.В. Суслопаровым. Действительно, преступника и потерпевшего могут разделять от нескольких метров до нескольких тысяч километров, хотя в киберпространстве они могут быть постоянными посетителями одного и того же сайта или социальной сети. В то же время потерпевшие от одного киберпреступления могут исчисляться десятками или сотнями, при этом они так же могут проживать в разных странах мира, как и сами преступники, если они действовали в соучастии. Субъективно виновный считает общественно незначимым такое деяние, как хищение электронных или безналичных денег у иностранца, или обман гражданина другой страны. Тот факт, что лицо совершает преступление против интересов иностранных граждан или организаций, субъективно снимает с него ответственность и развязывает руки. Киберпространство само по себе

[1]Дремлюга Р.И., Интернет-преступность. дис. ... канд. юрид. наук. Владивосток, 2007. С.49.

[2]Суслопаров А.В. Некоторые направления совершенствования законодательства об ответственности за компьютерные преступления с учетом международного опыта. // 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.105.

экстерриториально – в нём нет границ, нет государств, но есть сайты, форумы и их пользователи иностранцы, которых можно обмануть или обокрасть.

Данная проблема сильно усложняет работу следствия, доказывание, процесс экстрадиции и порождает проблему криминализации деяния. 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.

Единственным путём решения данной проблемы нам видится в международное сотрудничество, итогом которого должно стать принятие Конвенции о киберпреступлениях под эгидой ООН.

Возможность получения сверхприбыли при минимальных затратах в киберпространстве – одна из основных социально-экономических причин экономической киберпреступности.

При сложившейся экономической ситуации в стране замедлено создание новых предприятий и новых рабочих мест, а поток кадров, окончивших учебные заведения и получивших специальное техническое или высшее профессиональное образование, растёт с каждым годом. Следовательно, создаётся достаточно большая группа невостребованных специалистов, которые вынуждены использовать полученные знания самостоятельно, используя подручные средства, в том числе сеть «Интернет». Однако если одни занимаются законной деятельностью в киберпространстве (фрилансеры), то другие ищут лёгкий путь – преступный (организовывают сайты-казино, занимаются мошенничеством, вымогательством, взломом аккаунтов пользователей, хищениями либо торговлей вредоносными программами).

Многие хакеры за несколько дней становятся миллионерами (греческий хакер под псевдонимом «Астра» совершил хищения на общую сумму

245 млн долларов[1], хакер Ким Шмитц – 1,1 млн евро[2], хакер Максим Глотов – 10 млн рублей[3]). При этом огромные финансовые потоки в нелегальных видах Интернет-бизнеса скрыты от государства, это приводит к тому, что все они остаются «в тени» без правового и социального контроля[4], тем самым снижая риски быть пойманными.

На наш взгляд, данное обстоятельство формирует в киберпространстве условия, при которых появляется возможность получения преступным путём сверхприбыли при минимальных затратах и рисках. Учитывая анонимность и трансграничность киберпространства, а также множество технических уязвимостей последнего, данное обстоятельство может являться катализатором, побуждающим к преступной деятельности отдельные группы населения. Возможность получения сверхприбыли при минимальных затратах и минимальном риске является объективным детерминантом экономической киберпреступности, поскольку побуждает виновных совершать экономические киберпреступления.

Данную проблему, на наш взгляд, можно решить профилактикой киберпреступности среди населения и популяризацией легальных способов получения крупных доходов в киберпространстве, например, «краудфандинг» (с англ. «народное финансирование»).

Техническое несовершенство киберпространства. Несмотря на то, что данное обстоятельство было признано детерминантом экономической киберпреступности лишь 31,2% опрошенных судей (30 чел.)[5], на наш взгляд, именно техническое несовершенство киберпространства и наличие в нём технических уязвимостей, лазеек и просто ошибок сводит на нет почти все меры противодействия киберпреступности.

---

[1]Информационный ресурс «Барфик». Самые известные хакеры. [Электронный ресурс] // URL:http:// barfik.com/people/samyie-luchshie-hakeryi-v-mire.html (Дата обращения: 26.04.2014).

[2]Информационный ресурс «Хакер.ру» [Электронный ресурс] // URL: https://xakep.ru/2002/05/30/ 15400/ (Дата обращения: 26.04.2014).

[3]Информационный ресурс «Вести.ру» [Электронный ресурс] // URL: http://www.vesti.ru/videos/ show/vid/379888/# (Дата обращения: 26.04.2014).

[4]Дремлюга Р.И. Интернет-преступность: монография. С. 196.

[5] См.: Приложение №2. Опросный лист.

В качестве таких лазеек можно привести следующий пример: при обнаружении на сайте материалов экстремистского характера, Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций Российской Федерации помещает данный сайт в список запрещенных на территории России, и простой доступ закрывается. Однако любой пользователь, в том числе и российского сегмента сети «Интернет» может воспользоваться «анонимайзером», таким как «cameleo.ru», который маскирует данного пользователя и в обход РОСКОМНАДЗОРА разрешает ему доступ к данному сайту.

Что же до уязвимостей, то их можно условно разделить на программные и физические. Программными уязвимостями в киберпространстве являются ошибки в исходном коде программного обеспечения, дающие возможность в обход системы безопасности и приватности получить неправомерный доступ к компьютерным данным пользователей, как персональных компьютеров, так и крупных корпораций и даже государственных органов. Программные уязвимости, как правило, оставляют по неосторожности, однако в некоторых случаях – умышленно. Речь идёт о так называемых «backdoor» (от англ. «задняя дверь») – это случаи когда разработчики программного обеспечения на этапе его создания оставляют возможность быстро и безопасно обойти систему защиты. Достаточно часто разработчики оставляют «заднюю дверь» открытой даже после того, как программный продукт был выпущен на рынок.

Программные уязвимости позволяют получить неправомерный доступ к компьютерной информации потерпевшего и тем самым открывают возможность совершить, например, хищения из систем онлайн-банка, незаконное получение сведений, составляющих коммерческую тайну, и множество других преступлений.

Как правило, программные уязвимости решаются выпуском обновления или «патча», который исправляет данную проблему.

К физическим уязвимостям и несовершенствам киберпространства следует отнести совокупность материальных ограничений сети «Интернет», компьютеров и иных устройств.

Так, председатель Комитета Государственной Думы РФ по информационной политике, информационным технологиям и связи Л.Л.Левин на национальном форуме информационной безопасности «Инфофорум-2015» отметил, что серьёзной уязвимостью является тот факт, что персональные Интернет-данные граждан России (сведения об их адресе, паспортные данные, номера счетов и так далее) хранятся на серверах, расположенных за пределами России[1]. Поскольку киберпространство экстерриториально, то сайт (его сервер) с доменным именем «.RU» физически может быть расположен где угодно, но не в России. Это создаёт возможность манипулирования и давления, как на государство, так и на население. Миллионы пользователей, зарегистрированные в отечественной социальной сети, могут быть просто отключены от данного ресурса. При этом на таком ресурсе могут проходить сделки и осуществляться предпринимательская деятельность. В качестве мер противодействия Л.Л.Левин предложил внести в Федеральный закон «О персональных данных» норму, обязывающую отечественные IT-компании хранить персональные данные на серверах, расположенных на территории РФ.

На наш взгляд, данное решение является единственным разумным выходом из сложившейся проблемы, но оно имеет и обратную сторону. Многие IT-компании хранят персональные данные своих пользователей на иностранных серверах по ряду причин: во-первых, таким образом они избегают дополнительных затрат; во-вторых, на зарубежных серверах зачастую лучше система безопасности (антивирусы и фаерволы). Следовательно, обязывание хранить персональные данные на отечественных серверах может повлечь как дополнительные финансовые проблемы IT-компаний, так и снижение уровня защищенности ресурсов от иных кибер-угроз.

[1]Материалы Инфофорум-2015. Архив автора.

Данное предложение было услышано, и статья 18 Федерального закона «О персональных данных» была дополнена новой частью: «5*) при сборе персональных данных, в том числе посредством информационно-телекоммуникационной сети «Интернет», оператор обязан обеспечить запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан Российской Федерации с использованием баз данных, находящихся на территории Российской Федерации, за исключением случаев, указанных в пунктах 2, 3, 4, 8 части 1 статьи 6 настоящего Федерального закона».* Соответствующие изменения были также внесены в статью 16 «Защита информации» Федерального закона «Об информации, информационных технологиях и о защите информации»[1].

Ещё одной технической проблемой, по нашему мнению, является массовая «привязка» аккаунтов к одной лишь электронной почте. Киберпространство так или иначе построено на системе электронной почты, для того, чтобы зарегистрироваться на каком-либо сайте, требуется ввести свой адрес электронной почты, логин (псевдоним) и пароль. В случае если пользователь забыл пароль от сайта, то он может его восстановить через систему восстановления пароля, предусмотренную самим сайтом, в этом случае новый пароль высылается на указанный адрес электронной почты. Следовательно, если злоумышленник получит доступ к электронной почте жертвы, то он получит доступ ко всем сайтам, на которых она была зарегистрирована, а это могут быть сайты электронных платежных систем, Интернет-кошельки и т.д.

Преступнику не нужно выискивать логины пользователя, которые он использовал для регистрации на разных сайтах платёжных систем, взламывать сложную систему защиты каждого из таких сайтов, а всего лишь подобрать пароль от почтового ящика пользователя и получить доступ ко всем его электронным накоплениям разом. В связи с этим в последние годы все

[1]Федеральный закон от 21 июля 2014 N 242-ФЗ (ред. от 31 декабря 2014) «О внесении изменений в отдельные законодательные акты Российской Федерации в части уточнения порядка обработки персональных данных в информационно-телекоммуникационных сетях»// Собрание законодательства РФ. 2014. N 30. Ст. 4243.

популярнее становится система привязки аккаунта к номеру мобильного телефона или мобильному приложению.

Другой технической уязвимостью является разнообразие средств доступа в киберпространство. Сегодня в «Интернет» можно выйти не только с помощью стационарного компьютера, но и посредством мобильных устройств (планшетов, смартфонов, мобильных телефонов), а также посредством «умной» техники (от телевизоров до холодильников). С одной стороны – это благо, поскольку такое разнообразие даёт новые невиданные возможности. К примеру, сегодня уже реально по пути с работы домой через мобильный телефон включить мультиварку, что бы та сама приготовила ужин. Подобная функция уже есть в WiFi-мультиварке фирмы «POLARIS»[1].

Проблема заключается в том, что большинство подобных устройств работают на собственных операционных системах либо на сильно упрощенных мобильных операционных системах (Android, IOS и др.), и для каждой из них нужен собственный антивирус. Если владельцы стационарных компьютеров в большинстве случаев всё же устанавливают защитные программы, то владельцы мобильных устройств и «умной» техники эту необходимость игнорируют, легкомысленно рассчитывая, что их гаджеты в безопасности.

Так, на «Инфофоруме-2015» начальник Бюро специальных технических мероприятий МВД РФ А.Н.Мошков отметил, что мобильные устройства – это основное направление киберпреступников в наше время. С помощью мобильных устройств, как правило, происходят хищения из систем Онлайн-банков[2].

Преступники разрабатывают вирусы уже не только для персональных компьютеров, но и для телефонов, смартфоном и планшетов. Так, например, вирус «Android.SmsSend» предназначен для того, чтобы перенаправлять преступнику СМС сообщения с паролем доступа из системы Онлайн-банка с телефона потерпевшего. Он массово распространён на смартфонах с операционной системой «Android», пользователи которых не используют

[1]Информационный ресурс «Hi-Tech.Mail.Ru». [Электронный ресурс] // URL: http://hi-tech.mail.ru/bytovaya/polaris-wi-fi.html (Дата обращения: 08.03.2014).

[2]Материалы «Инфофорум-2015». Архив автора.

мобильный антивирус, а их свободная продажа в анонимных сетях, таких как «TOP», по мнению заместителя начальника научно-технической службы ФСБ России Н.Н. Мурашова, является ещё одной причиной киберпреступности[1]. На наш взгляд, эффективной мерой противодействия данной причине может стать отдельная криминализация сбыта вредоносного программного обеспечения путём выведения данного состава преступления как квалифицированного признака статьи 273 УК РФ.

Помимо этого, как отмечает В.Н. Мыткин, из-за того, что в обществе заметно повысился уровень информатизации, массово появились «умные» бытовые приборы, которые стали новым объектом хакерских атак. К примеру, в 2013 году в России был зафиксирован случай, когда «умный холодильник» распространял СПАМ[2].

На наш взгляд, проблеме технического несовершенства киберпространства уделяется слишком мало внимания, как законодателем, так и в научном сообществе. Как показывает история, неэффективность правовых мер регулирования заключалась в том, что они были применены поспешно, без учёта того, что в виртуальной среде их с лёгкостью можно обойти. Многие сервисы, такие как Интернет-торговля и Интернет-банкинг, преподносились как благо, однако вопросу их безопасности внимания не уделялось.

Отсутствие цифровой культуры и грамотности. В киберпространстве отсутствуют как таковые правила поведения, поэтому многие администраторы сайтов или форумов вынуждены придумывать свои, при этом санкции, которые может наложить администрация, ограничены предупреждениями, ограничением доступа и блокированием доступа к ресурсу («бан»). Такие санкции являются малоэффективными, поскольку количество сходных сайтов в киберпространстве достаточно велико, и если на одном сайте нарушителя заблокируют, то он может свободно зарегистрироваться на другом, либо может заново зарегистрироваться на заблокированном сайте под другим именем. В этом плане более эффективна

[1]Там же.
[2]Материалы «Инфофорум-2014». Архив автора.

блокировка не пользователя, а его IP-адреса, однако и этот запрет можно обойти посредством специальных программ либо осуществив доступ с другого устройства.

Как справедливо отмечает заместитель председателя комитета Совета Федерации ФС РФ по конституционному законодательству и государственному строительству Л.Н. Бокова: «Отсутствие минимального уровня цифровой грамотности и культуры – одна из основных причин киберпреступности»[1]. С ней соглашается Н.Н. Мурашов: «Цифровая неграмотность населения – основная причина киберпреступности»[2].

Привычка проходить проверку на компьютерные вирусы, не посещать подозрительные сайты должна быть выработана у граждан России на том же уровне, что и привычка мыть руки перед едой и не заводить разговоры с незнакомыми людьми – это элементарные правила предосторожности, о которых в киберпространстве забывают.

Единственным эффективным решением данной проблемы, на наш взгляд, является профилактика информационной безопасности среди населения. Необходимо прививать основные правила поведения в киберпространстве с малых лет, например, проводя специальные занятия в средней школе.

Отсутствие единых и четких правил поведения в киберпространстве привело к появлению новых субкультур, таких как **субкультура хакеров**, киберпиратов и многих других.

Свободный доступ к информации в киберпространстве является основной причиной, по которой данная технология стала так популярна, однако такой доступ возможен лишь с разрешения автора. Сейчас в киберпространстве существует множество сайтов, с которых в общий доступ выложены фильмы, музыка, книги и программы без разрешения автора.

Многие пользователи таких ресурсов и не подозревали, что нарушают чьи-то авторские права, считая, что если фильм выложен в сеть, то никакого вреда в

[1]Материалы «Инфофорум-2015». Архив автора.
[2]Там же.

его просмотре нет. Такое мнение укрепилось в сознании рядового пользователя киберпространства и породило субкультуру киберпиратов.

Субкультура хакеров (взломщиков) также имеет значительное влияние на всю киберпреступность – это своеобразное продвижение образа жизни и ценностей компьютерного преступника в широкие массы, реклама, делающая преступный путь привлекательным[1].

Общество не видит угрозы со стороны хакеров, считая их деятельность интересной и увлекательной. Данное мнение складывается у рядового пользователя киберпространства до тех пор, пока он не станет жертвой такого хакера. При этом занятие хакерством уже перестало быть неким развлечением, а является серьезным источником дохода.

Бездействие правоохранительных органов в качестве условия киберпреступности заняло последнее место по результатам опроса судей районных и областных судов Российской Федерации – 19,7% (19 человек).[2] Данный факт говорит о том, что многие сотрудники правоохранительных органов, впервые столкнувшиеся с киберпреступлением, не обладают необходимыми знаниями, как по их квалификации, так и по поиску и привлечению к ответственности виновных, что приводит к высокому уровню латентности киберпреступности**.**

Наибольшая часть киберпреступности остаётся неизвестной, а в официальную статистику попадает лишь 10%, в лучшем случае 20% совершённых деяний[3]. А.К. Киселёв указывает, что некоторые киберпреступления даже превзошли их количественный эквивалент в материальном мире: около 90% киберпреступлений остаются не зарегистрированными, то есть носят латентный характер[4]. По другим источникам уровень латентности таких преступлений колеблется от 80%[5] до 90%[1].

---

[1]Дремлюга Р.И. Интернет-преступность: монография. С.198.

[2] См.: Приложение №2. Опросный лист.

[3]Номоконов В.А., Тропина Т.Л. Киберпреступность: прогнозы и проблемы борьбы. // Библиотека криминалиста.2013. №5(10). С.153.

[4]Киселёв А.К. Киберпреступность – взгляд из Европы. // Библиотека криминалиста. 2013. №5(10). С.310.

[5]Сухаренко А.Н. Современные криминальные вызовы и угрозы информационной безопасности России [Электронный ресурс] // URL: http://sartraccc.ru/Press/special/contr_terror_1_12.pdf (Дата обращения: 5.08.2015).

По мнению М.В. Старичкова[2], в 2006 году уровень латентности преступлений в сфере компьютерной информации и иных компьютерных преступлений, в которых «Интернет» является средством их совершения, составлял 99,7-99,8%.

В наше время с развитием средств защиты от неправомерного доступа, способов выявления и изобличения преступников уровень латентности всё же снизился, но не значительно. Для выявления уровня латентности экономической киберпреступности в Российской Федерации предлагается выявить уровень латентности самых распространённых экономических киберпреступлений в России – хищений, поскольку их более 90% от общего числа всех киберпреступлений. Так, согласно официальной статистике, которую огласил начальник Бюро специальных технических мероприятий МВД России А.Н.Мошков на «ИНФОФОРУМЕ», в 2011 году зарегистрировано 2123 факта мошенничества и иного хищения с использованием сети «Интернет» (2645 факта в 2012 г.)[3]. По данным «Group-IB» за 2012 год, только в системах Интернет-банкинга ежедневно в России совершаются 44 факта хищения (примерно 10 956 в год)[4].

Если сравнить данные цифры, то уровень латентности киберпреступности в 2012 году можно вычислить по формуле №1.

$$100\% - \left(\frac{2645}{44*366} \right)*100\% = 100\% - \left(\frac{2645}{16104} \right)*100\% =$$

$$100\% - 0{,}1642*100\% = 100\% - 16{,}42\% = \mathbf{83{,}58\%}.$$

[1]Рассолов И.М. Право и «Интернет»: теоретические проблемы. С.133.

[2]Старичков М. В. Умышленные преступления в сфере компьютерной информации: уголовно-правовая и криминологическая характеристика: дис...канд. юрид. наук. Иркутск, 2006. С.109-112

[3]Материалы «Инфофорум-2013». Архив автора.

[4]Официальный сайт Российская газета [Электронный ресурс] // URL: http://www.rg.ru/2013/09/10/internet-moshenniki-site-anons.html (Дата обращения 08.03.2014).

Формула №1, где: 2645 – официальная статистика МВД РФ за 2012 год, 44 – статистика преступлений в день «Group-IB» за 2012 год, 366 – дней в 2012 году, 100% – общий процент всех киберпреступлений в 2012 году.

По другой статистике, Банка России за 2012 год, в системах Интернет-банкинга совершается 28 хищений в день (примерно 10 248 в год)[1]. При сравнении данных цифр с официальной статистикой МВД РФ уровень латентности за 2012 год немного меньше, что видно из формулы №2.

$$100\% - \left(\frac{2645}{28*366}\right)*100\% = 100\% - \left(\frac{2645}{10248}\right)*100\% =$$

$$100\% - 0{,}258*100\% = 100\% - 25{,}8\% = \mathbf{74{,}2\%}.$$

Формула №2, где: 2645 – официальная статистика МВД РФ за 2012 год, 28 – статистика Банка России за 2012 год, 366 – дней в 2012 году, 100% – общий процент всех киберпреступлений в 2012 году.

Если учесть, что в последнем случае были использованы данные о хищениях только в системе Интернет-банкинга, то реальные показатели латентности должны быть много выше.

Объединив результаты, можно сделать вывод, что уровень латентности экономических киберпреступлений России в 2012 году по разным данным варьируется от 74,2% до 83,58%.

Стоит также учесть, что высокий уровень латентности киберпреступлений является мировой проблемой. По мнению разных учёных, уровень латентности киберпреступлений в США составляет около 80%, в Великобритании — до 85%, в ФРГ — 75%[2].

---

[1]Доклад компании Group-IB «Threat Intelligence Report 2012 – 2013 H1» [Электронный ресурс] // URL: http://report2013.group-ib.ru/ (Дата обращения: 26.04.2012).

[2]Сабадаш В. Проблемы латентности компьютерной преступности. Crime-research.ru [Электронный ресурс] // URL:http://www.crime-research.ru/library/Sabodash0304.html (Дата обращения: 08.03.2014); Рассолов И.М. Право и Интернет. Теоретические проблемы. С.133.

Таким образом, реальное положение дел в этой области в разы хуже, чем это указывается в уголовной статистике. Однако, при отсутствии достоверных официальных статистических данных о киберпреступлениях, точность подобных показателей сомнительна. На данную проблему указывают многие авторитетные учёные (В.А. Номоконов, Т.Л. Тропина[1]).

Такой высокий уровень латентности связан с множеством причин**.** Как правильно отмечает И.М. Рассолов[2], основная из них – это иллюзия незначительности ущерба для потерпевшего, по сравнению с проблемами, которые могут возникнуть при расследовании. Похожая причина существует и в том случае, если потерпевшим будет являться кредитная организация: расследование большинства видов кибермошенничеств затрудняется отсутствием необходимой информации о фактах совершения таких преступлений от кредитных организаций, так как многие банки, опасаясь за свою деловую репутацию, крайне неохотно обращаются за помощью в правоохранительные органы[3]. Н.Н. Мурашов отмечает, что основная причина латентности киберпреступлений заключается в том, что представители бизнеса утаивают факты хищений и кибер-атак, опасаясь причинения вреда своей репутации[4].

Делая предварительный вывод, можно выделить следующие основные положения.

9. 1. Определяются 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;

---

[1]Номоконов В.А., Тропина Т.Л. Киберпреступность: прогнозы и проблемы борьбы. // Библиотека криминалиста. 2013. №5(10). С.153.

[2]Рассолов И.М. Там же. С. 251-254.

[3]Сухаренко А.Н. Современные криминальные вызовы и угрозы информационной безопасности России [Электронный ресурс] // URL: http://sartraccc.ru/Press/special/contr_terror_1_12.pdf (Дата обращения: 5.08.2015).

[4]Материалы «Инфофорум-2015». Архив автора.

- 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.

2. Уровень латентности экономических киберпреступлений невероятно высок. Правоохранительным органам становится известна лишь одна пятая, в лучшем случае, одна четвёртая часть из всех совершаемых экономических киберпреступлений.

§2. Личность киберпреступника и его жертвы

Анализ личности преступника. Характеристика личности преступника, способного совершить экономическое киберпреступление, является важной частью понимания самого явления киберпреступности. Полученные данные помогут выделить примерный круг лиц, нуждающихся в дополнительном контроле со стороны государственных правоохранительных органов, что облегчит поиск виновных и предупреждение новых преступлений.

Данное исследование представляет особый интерес, если учесть, что 19 марта 2013 года Европол опубликовал отчет «Оценка угрозы организованной преступности в ЕС в 2013 году», в котором «русскоговорящие»

киберпреступники занимают первое место в Европе по количеству исходящих компьютерных атак[1].

Построить примерный портрет компьютерного преступника пробовали многие отечественные ученые (М.Ю. Дворецкий, Р.И. Дремлюга, В.Б. Вехов, Т.П. Кесареева, А.Н. Копырюлин, Т.М. Лопатина, А.Э. Побегайло и др.)[2], но единой точки зрения нет, что связано с разнородностью киберпреступности. Поскольку в киберпространстве существует возможность совершения разных преступлений, требующих наличия разных навыков и знаний, то и киберпреступников делят на разные группы, потому что они обладают различными личностными характеристиками.

Так, М.Ю. Батурин выделяет:

- корыстных преступников;
- лиц совершивших компьютерные преступления по небрежности;
- шпионов;
- хакеров (взломщиков);
- кракеров (компьютерных хулиганов)[3].

В.Б. Вехов, Т.М. Лопатина и А.Э. Побегайло делят лиц, совершивших компьютерные преступления, на три группы:

- «фанатики» – лица, отличительной особенностью которых является устойчивое сочетание профессионализма в области компьютерной техники и программирования с элементами фанатизма (хакеры);

[1]Официальный сайт «Европола». Socta 2013. EU Serious and Organised Crime Threat Assessment. [Электронный ресурс] URL: https://www.europol.europa.eu/sites/default/files/publications/socta2013.pdf (Дата обращения: 18.04.2014).

[2]См.: Дворецкий М.Ю., Копырюлин А.Н. Оптимизация уголовной ответственности и проблемы квалификации преступлений в сфере компьютерной информации. С. 107-109; Дремлюга Р.И., Интернет-преступность. дис. ... канд. юрид. наук. Владивосток, 2007. С. 100-119; Побегайло А.Э. Киберпреступность: лекция. М., 2013. С.43; Кесареева Т.П. Криминалистическая характеристика и проблемы предупреждения преступности в российском сегменте сети Интернет: дис…. канд.юрид.наук. М., 2002. С. 103; Лейкина Н. С. Личность преступника и уголовная ответственность: дис... докт.юрид.наук. Ленинград, 1969. С.39-51; Флоря Е.К. Личность преступника: Криминологическое и уголовно-правовое исследование: дис... канд. юрид. наук. Кишинев, 2002. С.80; Марданов А. Б. Личность современного экономического преступника: дис... канд. юрид. наук. Сургут, 2010. С.72-89; Винокурова Н.С. Личность преступника и жертвы в механизме вымогательства и предупреждение этих преступлений: дис... канд. юрид. наук. М., 2003. С.37-42.

[3]Батурин Ю.М. Право и политика в компьютерном круге. М., 1987. С.27-34.

- «психически больные» – лица, страдающие такими психическими заболеваниями, как информационная болезнь или компьютерная фобия;
- «профи» – профессиональные компьютерные преступники с ярко выраженными корыстными целями[1].

По мнению М.Ю. Дворецкого и А.Н. Копырюлина, компьютерных преступников можно разделить на следующие группы:

- нарушители правил пользования ЭВМ;
- «белые воротнички» (или респектабельные преступники);
- компьютерные шпионы;
- хакеры[2].

Р.И. Дремлюга даёт следующую классификацию:

- «Интернет-мошенник»;
- «Интернет-взломщик» (хакер);
- создатель Интернет-вирусов[3].

Анализируя такое разнообразие видов киберпреступников, можно обнаружить одну особенность: почти все ученые так или иначе отдельно выделяют две самостоятельные группы киберпреступников: хакеров и корыстных преступников. Если учесть, что эти две группы друг друга не исключают, то среди корыстных киберпреступников можно встретить как хакеров, так и обычных мошенников. Также среди хакеров можно встретить как корыстных хакеров, так и наоборот, некорыстных (например, движимых хулиганскими побуждениями). В данной работе будет детально проанализирована личность именно корыстного киберпреступника, поскольку подавляющее большинство экономических киберпреступлений – корыстной направленности.

Как указывает Р.И. Дремлюга, 95,83% всех Интернет-преступлений совершаются из корыстной заинтересованности[1]. Такое же мнение высказал

[1]Вехов В.Б. Компьютерные преступления: способы совершения, методики расследования. М., 1996. С.31-36; Лопатина Т.М. Криминологические и уголовно-правовые основы противодействия компьютерной преступности: автореф. дис. … докт.юрид.наук: М., 2006. С.30, 31; Побегайло А.Э. Киберпреступность: лекция. С. 35.

[2]Дворецкий М.Ю., Копырюлин А.Н. Оптимизация уголовной ответственности и проблемы квалификации преступлений в сфере компьютерной информации. С.172.

[3]Дремлюга Р.И., Интернет-преступность. дис. ... канд. юрид. наук. Владивосток, 2007. С.143

начальник Бюро специальных технических мероприятий МВД РФ А.Н. Мошков. По его данным, в 2013-2015 гг. почти все киберпреступления, зафиксированные в Российской Федерации, были совершены из корыстных побуждений[2].

Возраст. При сравнении данных о возрасте киберпреступника с данными о возрасте преступника, совершающего аналогичные преступления без использования компьютера и киберпространства, выявляется своя специфика. Так, если средний возраст мошенника (ст. 159 УК РФ), совершающего преступление в материальном мире (без средств компьютерной техники), колеблется от 23 до 39 лет[3], то средний возраст кибер-мошенника варьируется от 18 до 26 лет[4]. При этом если доля несовершеннолетних, совершающих экономические киберпреступления, составляет 30%, то в материальном мире она лишь 3%[5]. Также при сравнении данных о возрасте киберпреступника с начала 2000-х годов по наше время прослеживается тенденция к омоложению киберпреступника: если средний возраст в 2002 году составлял примерно 30[6] лет, то сегодня – только 24 года[7]. Такая тенденция очень опасна, поскольку может привести к тому, что средний возраст киберпреступника снизится ниже планки совершеннолетия, и киберпреступность станет ювенальной.

Представляется, что омоложение личности киберпреступника связано с омоложением личности пользователя сети «Интернет». Как верно указывает О.С. Гузеева, наиболее активна в овладении сетью Интернет молодёжь, составляющая 48% от всех пользователей[8]. Средний возраст пользователей сети

---

[1]Дремлюга Р.И. Интернет-преступность: монография. С.140.

[2]Мошков А.Н. Информационная безопасность России: аналитический сборник // М., Инфофорум.рф. 2014. Вып.1. С.86

[3] Официальный сайт МВД РФ [Электронный ресурс] URL: http://68.mvd.ru/news/item/576876 (Дата обращения: 01.08.2014).

[4] Кибермошенничество было взято за пример как наиболее распространённое киберпреступление.

[5] Официальный сайт МВД РФ [Электронный ресурс] URL: http://68.mvd.ru/news/item/576876 (Дата обращения: 01.08.2014).

[6]Дремлюга Р.И. Интернет-преступность: монография. С.137; Кесареева Т.П. Криминалистическая характеристика и проблемы предупреждения преступности в российском сегменте сети Интернет: дис…. канд.юрид.наук. М., 2002. С. 103.

[7]Дворецкий М.Ю., Копырюлин А.Н. Оптимизация уголовной ответственности и проблемы квалификации преступлений в сфере компьютерной информации. С.178.

[8] Гузеева О.С. Предупреждение размещения информации, способствующей распространению наркотических средств, в российском сегменте сети Интернет (криминологические и уголовно-правовые проблемы). автореф. дис. … канд. юрид. наук. М., 2008. С. 4.

«Интернет» в 2004-2006 годах составлял 30 лет[1], а в настоящее время находится на отметке от 14 до 24 лет. По данным Всероссийского центра изучения общественного мнения (ВЦИОМ), люди именно этого возраста проявляли наибольшую активность в сети «Интернет» (90%) в 2014 году[2].

Со схожими цифрами выступают почти все ученые (Р.И. Дремлюга, Т.П. Кесареева, М.Ю. Дворецкий и А.Н. Копырюлин, А.Э. Побегайло). По их мнению, возраст киберпреступника колеблется от 15 до 45 лет, а социальное положение в обществе – от школьника и студента до ответственного сотрудника государственного учреждения или фирмы.

Пол. Определённые изменения выявляются при сравнении данных о поле преступника, совершающего экономические киберпреступления, с данными о преступниках, совершающих аналогичные преступления в материальном мире. Так, если соотношение мужчина/женщина в экономических преступлениях составляло 70% на 30%[3], то в киберпреступлениях доля мужчин-преступников составляет уже 97%[4], а женщин – лишь 3%. По данным А.А. Комарова среди киберпреступников было зафиксировано 76% мужчин и 24% женщин[5]. Т.П. Кесареева указывает, что 98,2% всех киберпреступников – это мужчины[6].

По нашим данным, большая часть киберпреступников также мужчины (89%).[7] Учитывая средний возраст киберпреступника, такая статистика может объясняться как повышенным интересом к компьютерным технологиям со стороны несовершеннолетних мальчиков, так и тем, что большинство киберпреступлений (79%) – это мошенничества (ст. 159, 159.6 УК РФ), которые, как правило, совершаются мужчинами (94%) и только в редких случаях

---

[1]Деловая пресса [Электронный ресурс] // URL:http://www.businesspress.ru/newspaper/article_mId_21961_aId_317463.html (Дата обращения: 02.08.2014).

[2]Информационный ресурс «Bizhit». Интернет в России и в мире. [Электронный ресурс] // URL:http://www.bizhit.ru/index/users_count/0-151 (Дата обращения: 02.08.2014).

[3]Официальный сайт МВД РФ [Электронный ресурс] // URL: http://68.mvd.ru/news/item/576876 (Дата обращения: 01.08.2014).

[4]Дремлюга Р.И. Интернет-преступность: монография. С. 136.

[5]Комаров А.А. Криминологические аспекты мошенничества в глобальной сети «Интернет». дис… канд. юрид. наук. Пятигорск, 2011. С.97-105.

[6]Кесареева Т.П. Криминалистическая характеристика и проблемы предупреждения преступности в российском сегменте сети Интернет: дис…. канд.юрид.наук. М., 2002. С.101-105.

[7] См.: Приложение №3. Таблица работы с судебными документами.

женщинами (6%). В то же время если взять другое, менее распространённое киберпреступление, например, присвоение и растрату (ст. 160 УК РФ), то доля мужчин среди общего числа преступников снизится до 50%.

Семейное положение. Как правило, киберпреступления совершаются лицами, официально не состоящими в браке. Количество холостых лиц из общего числа киберпреступников составляет 70%, в то время как состоящих в браке – 30%. Данное соотношение справедливо для преступников, совершающих как преступления против собственности, так и преступления в сфере экономической деятельности. Представляется, что это связано в первую очередь с небольшим средним возрастом киберпреступника, а также с рядом субъективных факторов: семейные люди реже совершают преступления, нежели одинокие, опасаясь, что это негативно скажется на их близких.

Образование. Анализируя судебную практику по делам о преступлениях, совершаемых с использованием высоких технологий и киберпространства, можно прийти к выводу, что данная группа преступлений относится к группе высокоинтеллектуальных преступлений. Почти треть (28%) всех киберпреступников имеют высшее образование. При этом 14% киберпреступников имеют неоконченное высшее образование. В большинстве случаев на момент совершения преступления они являлись студентами высших учебных заведений. 32% киберпреступников имеют среднее специальное образование, 21,5% – среднее общее и лишь 4,5% – неполное среднее образование.[1]

Достаточно велик процент лиц, имеющих технические специальности «Прикладная информатика», «Информационные системы и технологии», «Программная инженерия», «Информационная безопасность» и др., – примерно 33%. Киберпреступники именно данной группы зачастую используют вредоносные программы и вирусы. Они знают принципы работы информационно-телекоммуникационных сетей, знают их уязвимости и пользуются этим.

[1] См.: Приложение №3. Таблица работы с судебными документами.

По данным А.Э Побегайло, 60% киберпреступников имели высшее образование, 20% среднее специальное и 20% среднее общее[1]. Согласно Р.И. Дремюге, 38,2% преступников, совершавших преступления в сети Интернет, имели высшее образование либо обучались в высших учебных заведениях, 25,7% из которых – на технических специальностях[2]. Как указывает Т.П. Кесареева, 39,3% киберпреступников – это учащиеся высших учебных заведений или техникумов[3]. По данным А.А. Комарова, 78% киберпреступников имеют высшее образование[4].

Место работы. Как показывает судебная практика, 51% лиц, совершивших экономическое киберпреступление, не имеют постоянного места работы. Как правило, данные лица совершают мошенничества (ст. 159, 159.6 УК РФ) и незаконное получение сведений, составляющих коммерческую, налоговую или банковскую тайну (ст. 183 УК РФ). Среди оставшихся 49% большую часть занимают менеджеры низшего и среднего звена (продавцы, как в простых, так и в Онлайн-магазинах), реже встречаются должностные лица (бухгалтеры) и программисты (работники Интернет-кафе, техники-программисты, ведущий инженер-программист).

По данным Р.И. Дремлюги, 31,3% лиц, совершивших преступления в сети «Интернет», имели постоянное место работы. По данным Т.П. Кесареевой этот процент составляет 33%.

Место жительства. Как правило, экономические киберпреступления совершаются в крупных городах (Москва, Санкт-Петербург, Казань, Саратов, Тамбов, Владимир, Пенза и др.). Представляется, что это связано с рядом факторов: во-первых, в крупных городах развиты информационно-телекоммуникационные технологии и есть доступ к безлимитному широкополосному «Интернету»; во-вторых, в таких городах больше население,

[1]Побегайло А.Э. Киберпреступность: лекция. С.38.

[2]Дремлюга Р.И. Интернет-преступность: монография. С.140.

[3]Кесареева Т.П. Криминалистическая характеристика и проблемы предупреждения преступности в российском сегменте сети Интернет: дис…. канд.юрид.наук. М., 2002. С.101-105.

[4]Комаров А.А. Криминологические аспекты мошенничества в глобальной сети «Интернет». дис… канд. юрид. наук. Пятигорск, 2011. С.97-105.

что напрямую сказывается на статистике. Однако в судебной практике встречались случаи совершения киберпреступлений в небольших посёлках, станицах и сёлах, в которых также был проведён «Интернет».

Географически большая часть экономических киберпреступлений совершались в Центральном (32%), Приволжском (27%) и Дальневосточном федеральных округах (10%), реже в Южном (9%), Северо-Западном (6%), Сибирском (6%), Уральском (5%) и Северо-Кавказском федеральных округах (5%).[1] Представляется, что это также связано с количеством населения в данных федеральных округах. Так, по данным Росстата на 1 января 2015 года наибольшее число жителей было зафиксировано именно в Центральном (38 944 837 человек) и Приволжском федеральных округах (29 717 813 человек)[2].

Судимость. Из анализа судебной практики видно, что 78% лиц, признанных виновными в совершении киберпреступлений, ранее не привлекались к уголовной ответственности, а лишь 22% имели непогашенную или неснятую судимость. При этом примерно 50% из них имели судимость за совершение экономических преступлений (как правило, ст. 158 и 159УК РФ), 33% имели судимость за преступления в сфере компьютерной информации (преимущественно ст. 272 и 273 УК РФ), а оставшиеся 16% имели судимость за иные неэкономические преступления (ч. 1 ст. 264, ст. 228 УК РФ и др).[3]

Данные результаты подтверждаются исследованиями других авторов. Так, Т.П. Кесареева[4] указывает, что 91% лиц, совершивших киберпреступления, ранее не судим; по данным Р.И. Дремлюги – 100%[5].

Подводя итог анализу личности киберпреступника, можно составить криминологический портрет лица, совершающего экономические преступления в киберпространстве, это:

---

[1] См.: Приложение №3. Таблица работы с судебными документами.

[2]Официальный сайт Федеральной службы государственной статистики. [Электронный ресурс] // URL:http://www.gks.ru/wps/wcm/connect/rosstat_main/rosstat/ru/statistics/population/ (Дата обращения: 19.02.2015).

[3] См.Приложение № 3. Таблица работы с документами.

[4]Кесареева Т.П. Криминалистическая характеристика и проблемы предупреждения преступности в российском сегменте сети Интернет: дис…. канд.юрид.наук. М., 2002. С.101-105.

[5]Дремлюга Р.И. Интернет-преступность: монография. С.140.

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

Также нами предлагается выделить два основных типа киберпреступников.

1. **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).

2. **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.).

Данные типы киберпреступников во многом отличаются друг от друга. Так, традиционные киберпреступники, как правило, старше и опытнее хакеров – именно в данной группе киберпреступников наибольшее число лиц, имеющих судимость. Хакеры, наоборот, как правило, моложе и являются выпускниками или учащимися высших учебных заведений технической направленности либо специальных техникумов и колледжей.

Киберпреступники первого типа совершают традиционные преступления, то есть те, которые совершаются и без использования киберпространства (мошенничества, вымогательства, незаконное разглашение сведений,

составляющих коммерческую тайну). Такие киберпреступники при совершении преступлений не используют сложные вредоносные программы и вирусы, а пользуются возможностями киберпространства, которые есть в общем доступе: мошенничество путём обмана они совершают в социальных сетях, вымогательство – через электронную почту, а коммерческую тайну распространяют на форумах и т.д.

Киберпреступники второго типа при совершении преступлений пользуются техническими уязвимостями киберпространства, взламывают электронные почтовые ящики, мобильные телефоны, банковские Онлайн-счета и электронные кошельки. Такие киберпреступники хорошо разбираются в сложных компьютерных программах, знают принципы работы информационно-телекоммуникационных сетей и умеют пользоваться вирусами и иным вредоносным программным обеспечением.

Анализ личности жертвы. Дав анализ личности киберпреступника, необходимо дать анализ личности его жертвы, что в свою очередь позволит создать более эффективные меры противодействия киберпреступности. Данное обстоятельство представляется наиболее актуальным, если учесть, что согласно данным ООН от 2011 года, по меньшей мере, 2,3 миллиарда человек (более 1/3 от общей численности населения Земли) имели доступ к «Интернету», а к 2017 году ожидается удвоение общего числа пользователей – доступ к мобильному, широкополосному «Интернету» получат 70% от общего населения планеты. В России количество пользователей уже значительно возросло: с 47 миллионов в 2009 году[1] до 74,4 миллионов в 2013 году[2]. При этом 85% всех опрошенных в России за 2013 год хотя бы раз становились жертвами киберпреступлений, а

[1]Номоконов В.А., Тропина Т.Л. Киберпреступность: прогнозы и проблемы борьбы. // Библиотека криминалиста. 2013. №5(10). С.148.

[2]Смирнов А.А. Сеть «Интернет» в механизме криминологической детерминации. // Библиотека криминалиста. 2013. №5(10). С.161.

общее количество таких жертв в 2013 году в мире составляет более 380 миллионов человек (погрешность ± 0,9%)[1].

Возраст. В 2006 году средний возраст потерпевшего составлял около 30 лет[2], однако к 2013 году эта цифра изменилась. Согласно данным «Norton Report» большинство опрошенных лиц в возрасте от 18 до 34 лет (66%) в 2013 году стали жертвами киберпреступлений, а средний возраст жертвы снизился до 22-26 лет[3]. Представляется, что омоложение личности жертвы киберпреступлений связано с омоложением личности пользователя сети «Интернет».

Пол. В отличие от возраста, средний показатель пола жертвы почти не изменился. Так, согласно показателям за 2006 год среди всех жертв киберпреступлений мужчины составили 55%, женщины – 45%[4], а по данным компании «Symantec» за 2013 год 64% опрошенных мужчин и 58% опрошенных женщин стали жертвами киберпреступлений[5].

Образование. Уровень образования также влияет на виктимность пользователей сети «Интернет». Необразованные, доверчивые люди могут стать жертвой киберпреступления в любом возрасте.

На национальных форумах информационной безопасности «Инфофорум» в 2013-2015 гг. многие ученые, представители Государственной Думы Российской Федерации, представители ФСБ и МВД РФ неоднократно говорили о том, что низкий уровень технического образования, низкий уровень культуры информационной безопасности является одним из наиболее виктимных факторов киберпреступности.

---

[1]Доклад компании Norton «Norton Report-2013: Symantec» [Электронный ресурс] // URL:http://www.symantec.com/about/news/resources/press_kits/detail.jsp?pkid=norton-report-2013 (Дата обращения: 26.04.2014).

[2]Дремлюга Р.И. Интернет-преступность: монография. С.148.

[3] Доклад компании Norton «Norton Report-2013: Symantec» [Электронный ресурс] // URL:http://www.symantec.com/about/news/resources/press_kits/detail.jsp?pkid=norton-report-2013 (Дата обращения: 26.04.2014).

[4]Дремлюга Р.И. Там же.

[5]Доклад компании Norton «Norton Report-2013: Symantec» [Электронный ресурс] // URL:http://www.symantec.com/about/news/resources/press_kits/detail.jsp?pkid=norton-report-2013 (Дата обращения: 26.04.2014).

Уровень специальных технических знаний влияет на виктимность пользователя сети «Интернет» сильнее всех остальных факторов. Статистически лица, обладающие такими знаниями, более осведомлены об основных методах хакерских атак и, следовательно, защищены от них. Такие люди следят за последними техническими новинками в области защиты персональных данных и знают самые эффективные способы борьбы с кибер-атаками, вирусами и иными вредоносными программами, они знают самые незащищенные области каждой из используемых операционных систем и зачастую используют более старую, но надёжную версию. Однако в масштабе страны общее количество людей, обладающих подобными знаниями, объективно мало.

Уровень технической защищённости. Пользователи стационарных персональных компьютеров (ПК) и ноутбуков, неоднократно сталкивавшиеся с вирусами или фактами неправомерного доступа к компьютерной информации, как правило, используют разнообразные защитные программы: анти-вирусы, анти-спамы, анти-шпионы и т.д. Однако лица, только начинающие пользоваться компьютером (как дети, так и взрослые), игнорируют данные защитные средства, поскольку те влияют на производительность компьютера или по другим причинам.

Сильным виктимогенным фактором является то, что большинство пользователей мобильных устройств (смартфонов, планшетов, умных часов или очков) ошибочно предполагают, что компьютерные вирусы опасны лишь для стационарных компьютеров и ноутбуков и поэтому не устанавливают антивирусную программу на мобильное устройство. При этом более 60% всех жертв вирусных кибер-атак – это пользователи именно мобильных устройств[1].

Как сообщает А.Н. Мошков, начальник Бюро специальных технических мероприятий МВД России (Управление “К”), в мире только на одну треть мобильных устройств установлен антивирус, при этом, для того чтобы воспользоваться услугами Интернет-банкинга, пользователи вводят персональные

[1]Материалы «Инфофорум-2014». Архив автора.

данные о номере счета и пароле именно с телефона, что повышает их виктимность[1].

Характер поведения жертвы в киберпространстве. Особое значение в поведении жертвы имеет её активность в киберпространстве, то есть то, как часто она пользуется конкретными сайтами и какие действия осуществляет на них.

Жертвами мошенничества в Интернет-магазинах или на Интернет-аукционах чаще всего становятся менее опытные покупатели, либо лица, впервые зашедшие на данный сайт. Для обмана покупателей в Интернет-магазине преступник может установить сумму за товар в несколько раз ниже средне-розничной с условием определённого процента предоплаты (от 50 до 100%). Пользователи, которые не раз совершали покупки на таких сайтах, обходят подобные объявления стороной, осознавая возможность мошенничества, в то время как менее опытные пользователи могут заинтересоваться «выгодным предложением».

А.А. Смирнов выделил некоторые виктимологические аспекты детерминации преступности, связанные с поведением жертв киберпреступлений: в 2010 году в 11 регионах России от 60 до 80 % российских школьников выложили в «Интернет» фамилию, точный возраст, номер школы, а 21% – и адрес проживания; около 70% российских детей выходили в «Интернет» каждый день, каждый пятый ребёнок проводил в «Интернете» более 3 часов в день, а средний возраст начала пользования сетью «Интернет» составлял 10 лет; более 75% детей имели профиль в социальных сетях, при этом почти 1/3 имели больше 1 профиля в разных социальных сетях; каждый пятый российский ребёнок (19%) имел более 100 «друзей» в социальных сетях[2].

Основываясь на вышесказанном, жертвами киберпреступников могут стать:

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-банки), с низкой культурой

[1]Там же.

[2]Смирнов А.А. Сеть «Интернет» в механизме криминологической детерминации. // Библиотека криминалиста.2013. №5(10). С.170.

информационной безопасности, как правило, пользователи мобильных устройств, пренебрегающие средствам компьютерной защиты (антивирусами) либо использующие контрафактные средства защиты.

Учитывая типологию личности киберпреступника, по нашему мнению, жертв киберпреступников можно также разделить на две группы: жертвы традиционных киберпреступников и жертвы хакерских атак.

Так, для совершения таких преступлений, как мошенничество, вымогательство, принуждение к совершению сделки, преступник вступает в контакт с жертвой посредством личной переписки в социальной сети, аудио- или видео-чате либо через электронную почту. В таком случае основными виктимогенными факторами могут выступать: необразованность, излишняя доверчивость, неопытность, то есть те же самые факторы, которые являются виктимогенными для традиционных преступлений.

Однако для совершения ряда других киберпреступлений (мошенничество в сфере компьютерной информации, незаконное получение сведений, составляющих коммерческую тайну, и др.), жертва и преступник не вступают в контакт друг с другом, поскольку преступник при совершении данных преступлений может использовать вредоносные программы, то главную роль будут играть уже такие виктимогенные факторы, как низкий уровень технической защищённости, наличие либо отсутствие антивируса и т.д.

В зависимости от того, к какой группе принадлежит та или иная жертва киберпреступления, прослеживаются те или иные виктимогенные факторы, следовательно, к разным группам жертв должны применяться разные меры противодействия от киберпреступности. Никакие антивирусные программы не уберегут самого опытного программиста от простого мошенничества или вымогательства в социальной сети, как и никакие знания не уберегут опытного юриста от банального компьютерного вируса.

Подводя итог параграфу, можно сделать следующие выводы.

1. Даётся 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. Предлагается авторская 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.).

3. Даётся 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.

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

Следует внести ясность в использовании термина «меры противодействия», поскольку наряду с данным термином в научной литературе применяются и такие термины как «меры борьбы», «меры профилактики» и «меры предупреждения».

Термин «борьба» подразумевает победу одной стороны над другой, к преступность данный термин не применим. Меры «профилактики» и «предупреждения» направлены лишь на будущие преступления, в то время как меры «противодействия» являются ответными мерами появления новых способов совершения преступлений или появления нового вида преступности. Меры профилактики можно отнести лишь к частному случаю мер противодействия.

Изучив историю возникновения экономической киберпреступности в России и других странах, определив основные виды экономических киберпреступлений, выявив их основные причины и условия, можно сформировать систему мер противодействия экономическим киберпреступлениям в Российской Федерации, направленных на:

1) выявление, устранение либо ослабление и нейтрализацию причин экономической киберпреступности;

2) выявление и устранение ситуаций, непосредственно мотивирующих либо провоцирующих на совершение экономических преступлений в киберпространстве;

3) выявление лиц повышенного криминального риска и снижение этого риска;

4) выявление лиц, поведение которых указывает на реальную возможность совершения экономических киберпреступлений, и оказание на них сдерживающего и корректирующего воздействия[1].

По способу противодействия данные меры следует разделить на две основные группы: правовые и криминологические.

Правовые меры направлены на одно из основных условий экономической киберпреступности – несовершенство законодательства. Они включают предложения по совершенствованию законодательства об уголовной ответственности за экономические преступления и преступления в сфере компьютерной информации; законодательства об информации, о связи и персональных данных. Правовые меры неразрывно связаны с организационными, поскольку они обеспечивают их исполнение на законодательном уровне. Без должного правового регулирования большинство организационных мер будут неэффективны.

Криминологические меры включают предложения по противодействию таким детерминантам экономической киберпреступности, как анонимность преступников, экстерриториальность преступлений, отсутствие культуры цифровой безопасности у населения и наличие субкультуры хакеров. Криминологические меры содержат предложения по профилактике информационной безопасности среди отдельных групп населения, предложения по совершенствованию информационных технологий, а также предложения по квалификации экономических преступлений, совершаемых в киберпространстве.

Поскольку все экономические киберпреступления по способу их совершения и объекту посягательства можно разделить на две самостоятельные группы (киберпреступления, совершаемые путём воздействия на человека, и киберпреступления, совершаемые путём воздействия на оборудование), то и меры противодействия экономическим киберпреступлениям по объекту

[1] Желудков М.А. Обоснование реализации системных защитных мер в механизме предупреждения корыстной преступности // Вестник Волгоградской академии МВД России. − 2014. − № 4 (31) – С. 47-51.

противодействия можно разделить на социальные и технические меры. Социальные меры направлены на развитие социальных качеств граждан (пользователей киберпространства): развитие культуры информационной безопасности и информационной грамотности, а также искоренение субкультуры хакеров. Социальные меры по способу противодействия также можно разделить на правовые и криминологические.

Как верно отмечает М. А. Желудков, многие преступления против собственности можно зафиксировать и предотвратить только с помощью специальных технических средств[1]. При этом технические меры должны определяться в зависимости от характера и специфики защищаемого объекта и построения средств зашиты на основе высоких технологий[2]. Технические меры направлены на развитие информационных технологий: разработку антивирусных программ, внедрение новейших информационных технологий в государственные и коммерческие организации, противодействие анонимности пользователей киберпространства и т.д.

Правовые меры. *Международно-правовые меры.* Отсутствие четко определённых границ в киберпространстве создаёт множество трудностей в привлечении виновных к уголовной ответственности, и единственное решение проблемы трансграничности киберпреступлений, по нашему мнению, заключается в международном сотрудничестве.

Российская Федерация активно участвует в международном сотрудничестве по борьбе с киберпреступлениями, в том числе и экономическими. За последние пятнадцать лет Российская Федерация заключила десятки соглашений о сотрудничестве в борьбе с киберпреступлениями[3]. В данных соглашениях

[1] Желудков М.А., Ююкина М. В. Системные особенности информационного обеспечения защиты объектов собственности от корыстных преступлений против собственности // Вестник Тамбовского университета. Серия: Гуманитарные Науки. − 2013. − №7(123). – С. 361.

[2] Желудков М.А. Развитие системы криминологического обеспечения защиты личности и общества от корыстных преступлений против собственности: автореф.дис. … докт. юрид. наук. М., 2012. С. 37.

[3] См: Соглашение о сотрудничестве государств - участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации. Заключено в г. Минске 01 июня 2001. // СПС «КонсультантПлюс»; Соглашение между Правительством Российской Федерации и Правительством Латвийской Республики о сотрудничестве в борьбе с преступностью, особенно в ее организованных формах. Заключено в г.

государства договариваются о сотрудничестве в противодействии компьютерным преступлениям, преступлениям в сфере компьютерной информации, киберпреступлениям (в том числе и экономическим), об установлении кибербезопасности, а также защите киберпространства.

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

Москве 20 декабря 2010) // СПС «КонсультантПлюс»; Соглашение о сотрудничестве между Министерством внутренних дел Российской Федерации и Министерством общественной безопасности Социалистической Республики Вьетнам. Заключено в г. Ханое 27 марта 2002. // СПС «КонсультантПлюс»; Соглашение между Правительствами государств-членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности. Заключено в г. Екатеринбурге 16 июня 2009. // СПС «КонсультантПлюс»; Соглашение между Правительством Российской Федерации и Правительством Малайзии о сотрудничестве в области информационных и коммуникационных технологий. Заключено в г. Путраджайе 05 августа 2003. // СПС «КонсультантПлюс»; Соглашение между Правительством Российской Федерации и Правительством Республики Беларусь о сотрудничестве в области обеспечения международной информационной безопасности. Заключено в г. Москве 25 декабря 2013. // СПС «КонсультантПлюс».

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:

«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».

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.

Криминологические меры. *Стратегия кибербезопасности.* По нашему мнению, в целях противодействия экономическим преступлениям, совершаемым в киберпространстве, и всем киберпреступлениям в целом, в Российской Федерации в первую очередь необходимо приять Национальную Стратегию кибербезопасности. В данной Стратегии должны быть разъяснены основные понятия (киберпространство, киберпреступление) и принципы противодействия кибер-угрозе, а также установлены основные направления деятельности органов власти в сфере противодействия киберпреступлениям. На основе анализа ряда зарубежных стратегий кибербезопасности основными направлениями Стратегии кибербезопасности РФ должны быть:

- защита стратегических и правительственных объектов (энергетики, нефтяного, газового и военно-промышленного комплекса, ЖКХ и т.д.);
- обеспечение безопасности граждан, организаций и государства, как в сфере компьютерной информации, так и в сфере экономических отношений (отношений собственности и отношений в сфере экономической деятельности);
- совершенствование законодательства;
- борьба с анонимностью;
- международное сотрудничество;
- развитие специальных правоохранительных органов;
- развитие информационных технологий;
- повышение цифровой грамотности населения.

Правоприменительные меры. Предлагается принять новую редакцию Постановления Пленума Верховного Суда Российской Федерации от 27.12.2007 N 51 «О судебной практике по делам о мошенничестве, присвоении и растрате». В постановлении следует разъяснить, что хищение, предусмотренное статьёй 159.6 УК РФ, совершается не путём обмана или злоупотребления доверием, а путем ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-

телекоммуникационных сетей и является новой, самостоятельной формой хищения.

В Постановлении также необходимо указать, что так называемые «фишинг», «вишинг» и «фарминг» следует отличать от деяния, предусмотренного статьёй 159.6 УК РФ. Обман в данных случаях – 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.

В Постановлении также необходимо разъяснить, что предметом преступления, предусмотренного статьёй 159.6 УК РФ, может быть также цифровой информационный продукт, в том числе криптовалюта, то есть денежный суррогат, эмиссия и учёт которого основаны на криптографических методах шифрования компьютерной информации. Криптовалюта обладает всеми признаками товара (имеет собственную экономическую стоимость и может быть обменена на реальные деньги), по смыслу статьи 128 ГК РФ её можно отнести к категории «иное имущество», её неправомерное обращение в пользу виновного либо третьих лиц причиняет вред не столько отношениям, складывающимся в сфере нормального оборота компьютерной информации, сколько отношениям собственности.

Предлагается принять новую редакцию Постановления Пленума Верховного Суда РФ от 04.05.1990 N3 «О судебной практике по делам о вымогательстве». В Постановлении необходимо разъяснить, что вымогательство (ст. 163 УК РФ) и принуждение к совершению сделки, а также отказу от её совершения (ст. 179 УК РФ), могут быть совершены 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, если такое уничтожение, блокирование, модификация либо иное вмешательство способно причинить существенный вред правам или законным интересам потерпевшего или его близких. Дополнительная квалификация по статье 272 УК РФ будет необходима только в случае реализации удаления, блокирования либо модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей.

Предлагается принять новую редакцию Постановления Пленума Верховного Суда РФ от 18.11.2004 N23 «О судебной практике по делам о незаконном предпринимательстве и легализации (отмывании) денежных средств или иного имущества, приобретенных преступным путем». В Постановлении необходимо разъяснить, что осуществление деятельности по предоставлению работ и услуг в киберпространстве («фриланс») может быть признано предпринимательской деятельностью, если оно направлено на систематическое извлечение прибыли. Лицо, осуществляющее данный вид деятельности («фрилансер»), должно быть зарегистрировано в качестве индивидуального предпринимателя либо юридического лица. При отсутствии регистрации и в случае причинения гражданам, организациям либо государству данной деятельностью ущерба свыше одного миллиона пятисот тысяч рублей либо в случае извлечения дохода в том же размере образуется состав незаконного предпринимательства. Такое деяние необходимо квалифицировать по статье 171 УК РФ.

В данном Постановлении также необходимо разъяснить, что финансовые операции с криптовалютой, полученной преступным путём, в результате которых криптовалюте был придан правомерный вид, необходимо квалифицировать по статье 174 УК РФ как легализацию (отмывание) иного имущества,

приобретённого преступным путём. Также, на наш взгляд, необходимо разъяснить иные способы легализации (отмывания) денежных средств в киберпространстве.

Представляется, что назрела необходимость в принятии Постановления Пленума Верховного Суда РФ «О судебной практике по делам о компьютерных преступлениях». В данном Постановлении должны быть разрешены вопросы квалификации, как преступлений в сфере компьютерной информации, так и преступлений, в которых компьютер, сеть «Интернет» и киберпространство являлись средством из совершения (преступления против личности, в сфере экономики, против общественного порядка и общественной безопасности и др.).

В Постановлении необходимо разъяснить, что в случае неправомерного доступа к компьютерной информации, содержащей коммерческую, банковскую либо налоговую тайну, деяние необходимо квалифицировать по части 1 статьи 183 УК РФ. По тому же принципу необходимо разъяснить, что внесение заведомо недостоверных сведений в Реестр владельцев ценных бумаг или систему депозитарного учета путем неправомерного доступа к данному реестру, либо к данной системе в киберпространстве или информационно-телекоммуникационных сетей, необходимо квалифицировать только по части 2 статьи 170.1 УК РФ. Дополнительная квалификация по статье 272 УК РФ необходима лишь в том случае, если помимо модификации реестра иная компьютерная информация подверглась уничтожению, модификации, блокированию либо копированию.

Развитие специальных правоохранительных органов (работа с кадрами). Основным ядром противодействия кибер-угрозе в системе МВД РФ на сегодняшний день является Управление «К» при Бюро специальных технических мероприятий. За историю своего существования Управлением «К» были обнаружено тысячи случаев киберпреступлений и пресечена деятельность множества организованных групп хакеров и иных киберпреступников. По нашему мнению, наличие данного подразделения является обязательным условием

кибербезопасности Российской Федерации, а также требует стимулирования её деятельности путём повышения финансирования со стороны государства.

Однако одно лишь Управление само по себе малоэффективно без взаимодействия с остальной системой МВД. Так, многие сотрудники полиции просто не знают о таких киберпреступлениях, как «кремминг», «фарминг» и т.д. Следовательно, они могут допустить ошибку и не среагировать на обращение граждан, например, о хищении виртуальной валюты. Представляется, что при подготовке сотрудников правоохранительных органов необходимо проводить специальные курсы о преступлениях, совершаемых в киберпространстве, а с действующими сотрудниками ежегодно проводить семинары о новых видах и новых способах совершения киберпреступлений. Такие же семинары систематически необходимо проводить в суде, прокурате, Следственном Комитете, Роскомнадзоре, Росфинмониторинге, ФСКН, ФСБ и других правоохранительных органах.

Профилактика киберпреступности, повышение информационной грамотности граждан. Данные идеологические меры противодействия киберпреступности представляют целый комплекс методов и средств противодействия, направленных на устранение в определенных группах и у определенных индивидов антиобщественных установок, а также на выработку негативного общественного отношения к киберпреступникам[1]. К ним можно отнести деятельность традиционных и Интернет-СМИ, занятия в школах и высших учебных заведениях, занятия на курсах повышения квалификации и т.д. Однако конкретные идеологические меры будут наиболее эффективны лишь для конкретной аудитории.

Поскольку прослеживается снижение среднего возраста киберпреступника и его жертвы, увеличение общего числа несовершеннолетних преступников, то наиболее эффективным методом идеологического воздействия на них будет информирование об киберпреступлениях и уголовной ответственности за их совершение в социальных сетях («Вконтакте», «Одноклассиники», «Facebook»).

[1]Дремлюга Р.И. Интернет-преступность: монография. С.213.

Популярность разных социальных сетей среди несовершеннолетних является необходимым условием эффективной профилактики киберпреступности, а если учесть, что более 75% детей имеют профиль в социальных сетях, при этом почти треть имеют больше одного профиля в разных социальных сетях и посещают их почти каждый день[1], то такая профилактика будет максимально эффективной. Кроме того, поскольку пользоваться компьютером и «Интернетом» начинают уже с малых лет (5-6 лет), то культуру информационной безопасности необходимо закладывать уже с этого возраста.

Необходимо выработать у пользователей киберпространства устойчивую привычку проверять свой компьютер на вирусы, устанавливать защитные программы и вовремя обновлять их. Представляется, что такая полезная привычка должна прививаться с детства, как привычка чистить зубы или мыть руки. Необходимо уберечь пользователей киберпространства от бесконтрольного распространения персональных данных. Как на улице нельзя заводить разговоры с незнакомцами, так и в социальных сетях или по электронной почте это не желательно. При таком общении необходимо быть более бдительным, нежели при живом общении, хотя бы потому, что вы не видите своего собеседника. Необходимо, чтобы пользователи киберпространства были сдержаны в общении, не разглашали важную информацию и персональные данные.

Помимо этого, для повышения цифровой грамотности и разработки новых методов противодействия киберпреступности, необходимо проводить молодежные, популярные, научные и научно-практические конференции и форумы, такие как «Инфофорум» и «Селигер».

Технические криминологические меры. Как отмечает М.А. Желудков, к техническим мерам защиты криминология относит различные средства и приспособления, затрудняющие совершение тех или иных преступлений, однако в современном высокотехнологичном мире к ним следует отнести разнообразные

[1]Смирнов А.А. Сеть «Интернет» в механизме криминологической детерминации. // Библиотека криминалиста. 2013. №5(10). С.170.

механизмы и способы информационного контроля[1]. В качестве организационно-технических мер нами предлагаются специальные механизмы и способы информационного контроля, направленные на противодействие анонимности экономических киберпреступлений и на техническое совершенствование самого киберпространства.

Противодействие анонимности. Борьба с анонимностью пользователей киберпространства и анонимностью информационных сетей, по нашему мнению, является одной из основ противодействия как экономической киберпреступности, так и всей киберпреступности в целом. В связи с особенностями существующих технологий невозможно достоверно определить, кто в момент совершения киберпреступлений был за компьютером, поскольку пользователи киберпространства общаются не напрямую, а посредством аккаунтов. Любой может утверждать, что во время совершения преступления за компьютером был кто-то другой, кто просто совершал преступления под его аккаутом. Даже при определении IP-адреса или MAC-адреса устройства эта проблема остаётся, что сильно усложняет работу правоохранительных органов и приводит к высокому уровню латентности.

Наиболее эффективным решением, на наш взгляд, является персонализация пользователей киберпространства. Любой человек, пользующийся сетью «Интернет» либо другими информационно-телекоммуникационными сетями, должен оставлять свой уникальный след. Таким следом может быть номер паспорта, электронная подпись, фотография лица либо отпечаток пальца.

По нашему мнению, несмотря на отрицательный опыт Китая, идея персонализации пользователей киберпространства по номеру паспорта является эффективным решением проблемы анонимности, однако её необходимо было внедрять постепенно.

[1] Желудков М.А. Ююкина М.В. Вопросы повышения эффективности обеспечения безопасности собственности при совершении корыстных преступлений // Вестник Тамбовского университета. Серия: Гуманитарные Науки. 2013. №8(124). С. 398.

Подобная идея уже реализовывается на портале государственных услуг города Москвы[1]. Указав паспортные данные в личном кабинете и подтвердив их, можно дистанционно пользоваться различными государственными услугами, к примеру, дистанционно зарегистрировать брак. Однако предоставление паспортных данных в данном портале носит не обязательный, а скорее рекомендательный характер. В случае успешного внедрения такой практики в социальные сети («Вконтакте», «Одноклассники»), которыми пользуются десятки миллионов граждан в день, анонимность перестанет представлять угрозу для прав и свобод граждан.

Персонализация пользователей также может быть реализована путём предоставления всем гражданам собственной электронной подписи. Она может храниться в ключ-карте или флеш-устройстве, которые необходимо будет подключать для выхода в сеть «Интернет». Подобная идея была предложена А.А. Комаровым в рамках технологии «Интернет-паспорта»[2]. Однако, на наш взгляд, подобная технология не в полной мере решает проблему анонимности, поскольку не учтена возможность использования чужого Интернет-паспорта, что способно привести к привлечению невиновных к уголовной ответственности. Но несомненным плюсом «Интернет-паспорта» является тот факт, что сегодня уже существует реальная возможность для массового внедрения такой технологии.

Тем не менее, наилучшим решением в борьбе с анонимностью является развитие и внедрение биометрических технологий, таких как сканер лица и сканер отпечатков пальцев.

Сегодня практически во всех новых компьютерах, ноутбуках, смартфонах и планшетах встроена камера, которая с помощью специального программного обеспечения способна распознать лицо пользователя. Данное программное обеспечение можно интегрировать, например, в мобильные приложения банковского обслуживания, такие как «Сбербанк-Онлайн». При каждой

[1]Портал государственных услуг Москвы. [Электронный ресурс] URL:http://pgu.mos.ru/ru/ // (Дата обращения: 12.09.2014).

[2]Комаров А.А. Криминологические аспекты мошенничества в глобальной сети Интернет. дис. …канд. юрид. наук. Пятигорск, 2011. С.167.

финансовой операции приложение будет требовать поднести камеру к лицу и в случае совпадения биометрических показателей разрешит проводить операцию. В будущем, когда такая технология станет автоматической, её можно внедрить, например, в социальные сети. Тогда при переписке мошенника или вымогателя с потерпевшим в сети «Интернет» останутся их биометрические данные. В случае массовой реализации такой технологии пользователи киберпространства будут оставлять неоспоримые следы своей деятельности – фотографии лица.

Преимуществом такой технологии является то, что между пользователем киберпространства и его аккаунтом больше нет посредника в виде логина, пароля, Интернет-паспорта либо флеш-устройства. Компьютер автоматически определяет личность пользователя, основываясь напрямую на его биометрических данных. Ещё одним преимуществом сканера лица является то, что подобная технология может быть массово внедрена уже сегодня.

Следующим этапом персонализации пользователей должно стать внедрение сканера отпечатков пальцев. Уже сегодня существуют мобильные устройства с интегрированным сканером отпечатков пальцев (Samsung SM-G850F, iPhone 5 и iPhone 6), платежи по которым можно совершать, предоставив свой отпечаток. В то же время сама технология сканера отпечатков пальцев также развивается. В 2015 году появился новый вид сканера – ультразвуковой. Особенность данного сканера в том, что его можно интегрировать под любую поверхность (стекло, пластик, металл). Если такой сканер интегрировать в компьютерную мышь, под «тачпад» ноутбука либо под экран смартфона и планшета, то появится возможность достоверно вычислить личность любого пользователя киберпространства. Но для этого потребуется полный отказ от устройств, не оборудованных данной технологией, что выявляет главную проблему такой меры – колоссальные финансовые затраты. Ещё один серьёзный минус технологии – это время её внедрения. Представляется, что при постепенном развитии технологии сканера отпечатков пальцев и постепенном его внедрении в государственные учреждения, затем в банковский сектор и только после этого в общественный сектор потребуется от 10 до 20 лет.

На наш взгляд, персонализация пользователей киберпространства является единственным решением проблемы анонимности, а её реализация – это уже вопрос технологий.

Техническое совершенствование киберпространства. Основными техническими мерами противодействия компьютерной преступности на государственном уровне является деятельность Бюро специальных технических мероприятий МВД РФ в области разработки специальных методов по вычислению хакеров и иных компьютерных преступников. Информация о подобных методах засекречена.

К негосударственным техническим мерам противодействия можно отнести деятельность коммерческих IT-компаний, таких как «Национальная компьютерная корпорация», ГК «ЛАНИТ», «Ситроникс», ГК «Техносерв», КРОК, ГК R-Style, ГК IBS, «Энвижн Груп», ГК «Компьюлинк», «Доктор Веб», «Яндекс», «Mail.ru Group» и «Лаборатория Касперского».

ЗАО «Лаборатория Касперского» и ООО «Доктор Веб», к примеру, занимаются разработкой отечественных защитных программ (анти-вирусов, анти-спамов, анти-шпионов и т.д.), и на данный момент они являются одними из ведущих компаний среди создателей антивирусных систем в мире[1].

Подобные антивирусы сильно снижают уровень виктимности в киберпространстве, поскольку попросту блокируют доступ к опасным сайтам или программам, выявляют уязвимости компьютерной системы и борются с вирусами и иными вредоносными программами, как на персональном компьютере, так и в самой сети «Интернет».

Многие коммерческие сайты (как правило, социальные сети) противодействуют киберпреступности своими силами. К примеру, с массовым появлением случаев мошенничества в киберпространстве крупные отечественные социальные сети перестали регистрировать анонимных пользователей или пользователей, использующих «подозрительные» имена, содержащие цифры и

[1]Официальный сайт «Kaspersky Lab». [Электронный ресурс]// URL: http://www.kaspersky.ru/about (Дата обращения: 26.04.2014).

другие символы. Также повышается популярность предоставления «официального аккаунта», для которого пользователь сам предоставляет администрации социальной сети паспортные данные. Подобная деятельность является первым шагом к решению проблемы анонимности киберпространства.

Внедрение других защитных технологий в отечественный сегмент сети «Интернет», к примеру, такой как «привязка аккаунта», является эффективной криминологической мерой противодействия преступлениям, совершаемым в киберпространстве.

Примером эффективности могут послужить статистические данные МВД РФ за 2009-2010 годы по преступлениям в сфере компьютерной информации. За 2009 год было зарегистрировано 11 636 фактов совершения преступлений в сфере компьютерной информации[1], в 2010 году данный показатель упал до 7 398[2]. Падение уровня преступности свыше чем на 35% в МВД связывают с повсеместным внедрением привязки аккаунтов абонентов Интернет-провайдеров к конкретному порту компьютера.

В настоящее время привязка аккаунтов к номерам телефонов повсеместно используется в крупных социальных сетях («ВКонтакте»), сайтах с виртуальными кошельками («Яндекс.Деньги») и в сфере Интернет-банкинга («Сбербанк-ОНЛ@ЙН»). Привязка аккаунта к мобильному приложению, к специальному устройству (генератору ключей) или к номеру паспорта отечественными IT-компаниями пока не применяется, однако данная практика распространена во многих западных странах (США, Канада).

Представляется, что развитие высоких технологий в Российской Федерации и внедрение опыта зарубежных компаний в отечественную Интернет-индустрию будет эффективным методом противодействия экономической киберпреступности.

На основе результатов исследования предлагается комплекс мер противодействия экономическим преступлениям, совершаемым в

[1]Официальный сайт МВД РФ [Электронный ресурс] URL: http://mvd.ru/upload/site1/import/65afff0dd0.pdf (Дата обращения: 06.09.2013).

[2]Там же.

киберпространстве, включающий в себя меры уголовно-правового характера (предложение о включении в перечень обстоятельств, отягчающих наказание следующее обстоятельство «совершение преступления дистанционно с использованием средств компьютерной техники, информационно-телекоммуникационных сетей и киберпространства»; положения о внесении изменений в уголовное законодательство Российской Федерации (ст. 159.6 , 163, 179, ч. 2 ст. 272, ч. 2 ст. 273 УК РФ); положение о внесении дополнений в уголовное законодательство Российской Федерации статьи 165.1 «Причинение имущественного ущерба в сфере компьютерной информации»; положение о внесении дополнений в уголовное законодательство Российской Федерации части 2.1 статьи 273 УК РФ «сбыт компьютерных программ либо иной компьютерной информации, заведомо предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации») и криминологического характера (положение о принятии Национальной Стратегии кибербезопасности Российской Федерации; положение о принятии Постановления Пленума Верховного Суда Российской Федерации «О судебной практике по делам о компьютерных преступлениях»; положение о принятии разработанного комплекса профилактических мер противодействия экономическим преступлениям, совершаемым в киберпространстве; положение о принятии комплекса технических мер противодействия экономическим преступлениям, совершаемым в киберпространстве - системы персонализации пользователей информационных ресурсов в киберпространстве, основанной на биометрических признаках пользователя цифрового устройства).

ЗАКЛЮЧЕНИЕ

Исследование экономических преступлений, совершаемых в киберпространстве, позволило нам выдвинуть ряд научно обоснованных положений.

1. С появлением новых технологий наблюдается появление нового, более сложного вида преступности. 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.

2. Киберпреступления – это новый, самостоятельный вид компьютерных преступлений (то есть преступлений, совершённых с использованием средств компьютерной техники). Под киберпреступлением следует понимать преступление, причиняющее вред разнородным общественным отношениям, совершаемое дистанционно, путём использования средств компьютерной техники, информационно-телекоммуникационных сетей и образованного ими киберпространства. Экономическим киберпреступлением следует считать киберпреступление, причиняющее вред экономическим отношениям. Киберпреступления экономического характера являются самыми распространёнными преступлениями в сети «Интернет».

3. Главными причинами и условиями существования экономической киберпреступности являются анонимность пользователей киберпространства и анонимность информационных сетей, экстерриториальность киберпространства, техническое несовершенство киберпространства, а также низкий уровень информационной безопасности граждан.

4. Сложившееся в обществе положение усугубляется высоким уровнем латентности экономических киберпреступлений, который достигает 83,53%. Правоохранительным органам становится известна лишь одна пятая часть всех совершаемых экономических киберпреступлений.

5. Наблюдается тенденция к омоложению лиц, совершающих преступления в киберпространстве. С начала 2000-х по настоящее время средний возраст киберпреступника снизился на 6 лет (с 30 до 24 лет). Динамика снижения среднего возраста киберпреступника создает предпосылки формирования нового вида преступности среди несовершеннолетних, что требует адекватных профилактических мер по ее предупреждению.

6. 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).

7. Учитывая вышесказанное, основными направлениями противодействия экономической киберпреступности должны стать правовое регулирование, организационные и организационно-технические меры.

8. Правовые меры необходимо направить на совершенствование норм, как Особенной, так и Общей части Уголовного кодекса Российской Федерации. Также необходимо провести редакцию Федерального закона «Об информации, информационных технологиях и защите информации», включив в него понятие «киберпространство». Помимо этого, в связи с экстерриториальным и трансграничным характером киберпреступлений, также необходимо разработать и принять единую Конвенцию о киберпреступлениях под эгидой ООН.

9. Кроме правовых мер, необходимо принять ряд мер: принять Национальную Стратегию кибербезопасности России; принять Постановление Пленума Верховного Суда Российской Федерации «О судебной практике по делам о компьютерных преступлениях»; принять новую редакцию ряда действующих Постановлений Пленума Верховного Суда Российской Федерации по делам о мошенничестве, вымогательстве, легализации и незаконном предпринимательстве; необходимо расширить предмет хищения, включив в него криптовалюту; кроме этого, необходимо с детства развивать культуру

информационной грамотности и информационной безопасности граждан, проводя специальные уроки в школах и семинары в вузах.

10. Учитывая специфику киберпреступности, одновременно с правовыми и организационными мерами противодействия необходимо принять ряд организационно-технических мер, направленных на персонализацию пользователей киберпространства, путём внедрения биометрических технологий (сканер лица и сканер отпечатков пальцев).

В заключение следует отметить, что киберпространство нельзя оставить вне рамок правового поля. Информационные технологии уже проникли во все жизненно важные сферы общества и стали неотъемлемой их частью. Игнорирование кибер-угрозы может привести лишь к краху современного общества. Необходима оперативная реализация мер противодействия киберпреступности, в том числе в экономической сфере.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

Нормативные акты Российской Федерации

1. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993) (с учетом поправок, внесенных Законами РФ о поправках к Конституции РФ от 30.12.2008 N 6-ФКЗ, от 30.12.2008 N 7-ФКЗ, от 05.02.2014 N 2-ФКЗ, от 21.07.2014 N 11-ФКЗ) // Собрание законодательства РФ. 2014. N 31. Ст. 4398.

2. Налоговый кодекс Российской Федерации (часть первая) от 31 июля 1998 N146-ФЗ (ред. от 28.12.2013) // Собрание законодательства РФ. 1998. №31. Ст. 3824.

3. Уголовный кодекс Российской Федерации от 13 июня 1996 N 63-ФЗ (ред. от 10 октября 2015) // Собрание законодательства РФ. 1996. N 25. Ст. 2954.

4. Гражданский кодекс Российской Федерации (часть первая) от 30.11.1994 N 51-ФЗ (ред. от 31.12.2014)// Собрание законодательства РФ. 1994. N 32. Ст. 3301.

5. Федеральный закон от 29 ноября 2012 N 207-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации»// Собрание законодательства РФ, .2012. N 49. Ст. 6752.

6. Федеральный закон от 27 июня 2011 N 161-ФЗ (ред. от 25декабря 2012) «О национальной платежной системе» // Собрание законодательства РФ. 2011. N 27. Ст. 3872.

7. Федеральный закон от 29.12.2006 N 244-ФЗ (ред. от 23.07.2013) «О государственном регулировании деятельности по организации и проведению азартных игр и о внесении изменений в некоторые законодательные акты Российской Федерации» // Российская газета. 2006. 31 дек. N 297.

8. Федеральный закон от 29 декабря 2006 N 244-ФЗ (ред. от 23 июля 2013) «О государственном регулировании деятельности по организации и проведению азартных игр и о внесении изменений в некоторые законодательные акты Российской Федерации»// Собрание законодательства РФ. 2007. N 1(1ч.). Ст. 7.

9. Федеральный закон от 02 декабря 1990 N 395-1 (ред. от 30 сентября 2013) «О банках и банковской деятельности»// Собрание законодательства РФ. 1996. N6. Ст. 492.

10. Федеральный закон от 27 июля 2006 N 149-ФЗ (ред. от 21 июля 2014) «Об информации, информационных технологиях и о защите информации»// Собрание законодательства РФ. 2006. N 31 (1 ч.). Ст. 3448;

11. Федеральный закон от 27 июля 2006 N 152-ФЗ (ред. от 21 июля 2014) «О персональных данных»// Собрание законодательства РФ. 2006.N 31 (1 ч.). Ст. 3451.

12. Федеральный закон от 7 июля 2003 N 126-ФЗ (ред. от 21 июля 2014, с изм. от 01 декабря 2014) «О связи» // Собрание законодательства РФ. 2003. N 28. Ст. 2895.

13. Федеральный закон от 21 июля 2014 N 242-ФЗ (ред. от 31 декабря 2014) «О внесении изменений в отдельные законодательные акты Российской Федерации в части уточнения порядка обработки персональных данных в информационно-телекоммуникационных сетях»// Собрание законодательства РФ. 2014. N 30 (Часть I). Ст. 4243.

Подзаконные акты Российской Федерации

14. Информация Банка России от 27 января 2014 «Об использовании при совершении сделок «виртуальных валют», в частности, Биткойн» // СПС «КонсультантПлюс».

15. Информационное сообщение Росфинмониторинга «Об использовании криптовалют» // СПС «КонсультантПлюс».

16. Официальный отзыв Правительства РФ от 02 августа 2012 N 3904п-П4 «На проект Федерального закона «О внесении изменений в Уголовный кодекс Российской Федерации и иные законодательные акты Российской Федерации»// СПС «Консультант Плюс».

Международные соглашения

17. Соглашение между Правительствами государств-членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности. Заключено в г. Екатеринбурге 16 июня 2009 // СПС «Консультант плюс».

18. Соглашение между Правительством Российской Федерации и Правительством Латвийской Республики о сотрудничестве в борьбе с преступностью, особенно в ее организованных формах. Заключено в г. Москве 20 декабря 2010 // СПС «Консультант плюс».

19. Соглашение между Правительством Российской Федерации и Правительством Малайзии о сотрудничестве в области информационных и коммуникационных технологий. Заключено в г. Путраджайе 05 августа 2003 // СПС «Консультант плюс».

20. Соглашение между Правительством Российской Федерации и Правительством Республики Беларусь о сотрудничестве в области обеспечения международной информационной безопасности (Заключено в г. Москве 25 декабря 2013) // СПС «Консультант плюс».

21. Соглашение о сотрудничестве государств-участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации. Заключено в г. Минске 1 июня 2001 // СПС «Консультант плюс».

22. Соглашение о сотрудничестве между Министерством внутренних дел Российской Федерации и Министерством общественной безопасности Социалистической Республики Вьетнам. Заключено в г. Ханое 27 марта 2002) // СПС «Консультант плюс».

Судебная практика

23. Апелляционное определение Московского городского суда №10-2076 от 06.05.2013 // СПС «Консультант Плюс».

24. Апелляционное определение Московского городского суда №10-8391 от 23.09.2013 // СПС «Консультант Плюс».

25. Постановление Московского городского суда №4у/2-9352 от 05 декабря 2013 // СПС «Консультант Плюс».

26. Постановление Пленума Верховного Суда РФ от 26.04.2007 N 14 «О практике рассмотрения судами уголовных дел о нарушении авторских, смежных, изобретательских и патентных прав, а также о незаконном использовании товарного знака»// СПС «КонсультантПлюс».

27. Постановление Пленума Верховного Суда РФ от 05.04.2012 N 6 «О внесении в Государственную Думу Федерального Собрания Российской Федерации проекта Федерального закона «О внесении изменений в Уголовный кодекс Российской Федерации и иные законодательные акты Российской Федерации»// СПС «КонсультантПлюс».

28. Постановление Пленума Верховного Суда РФ от 05.06.2002 N 14 (ред. от 18.10.2012) «О судебной практике по делам о нарушении правил пожарной безопасности, уничтожении или повреждении имущества путем поджога либо в результате неосторожного обращения с огнем»// Бюллетень Верховного Суда РФ. 2002. N 8.

29. Постановление Пленума Верховного Суда РФ от 11.06.1999 № 40 «О практике назначения судами уголовного наказания» // Бюллетень Верховного Суда РФ. 1999. N 8.

30. Постановление Пленума Верховного Суда РФ от 27.12.2007 N 51 «О судебной практике по делам о мошенничестве, присвоении и растрате»// Бюллетень Верховного Суда РФ. 2008. N 2.

31. Постановление Пленума Верховного Суда РФ от 28.12.2006 N 64 «О практике применения судами уголовного законодательства об ответственности за налоговые преступления»// Бюллетень Верховного Суда РФ. 2007. N 3.

32. Приговор Курского районного суда Ставропольского края от 08.08.2013 по делу N 1-132/2013 ст.160 ч. 2 УК РФ// СПС «Консультант Плюс».

33. Приговор Октябрьского районного суда города Пензы от 14.06.2012 по делу N 1-166/2012 // СПС «Консультант Плюс».

34. Приговор Октябрьского районного суда города Тамбова №1-324/09 от 29.05.2009 // Архив Октябрьского районного суда города Тамбова.

35. Приговор Приволжского районного суда города Казани от 28.02.2014 по делу N 1-13 2013;1-86 2012 ст.180 ч. 3 УК РФ// СПС «Консультант Плюс».

36. Приговор Хорошевского районного суда города Москвы от 01.12.2014 по делу N 1-587/2014. ст.163 ч. 1; ст. 273 ч. 1; ст. 273 ч. 2; ст. 273 ч. 2; ст. 273 ч. 2 УК РФ.// СПС «Консультант Плюс».

Диссертации

37. Абдулгазиев Р. З. Вымогательство по российскому уголовному праву: дис... канд. юрид. наук: 12.00.08 / Абдулгазиев Руслан Заурбекович. - Махачкала, 2003. − 171 с.

38. Алиева Д.Н. Мошенничество: уголовно-правовой и криминологический анализ: По материалам Республики Дагестан: дис... канд. юрид. наук: 12.00.08 / Алиева Диана Нупмагомедовна.- Махачкала, 2005. − 189 с.

39. Бакрадзе А. А. Присвоение и растрата как формы хищения в уголовном праве России: дис... канд. юрид. наук: 12.00.08/ Бакрадзе Андрей Анатольевич. - М., 2004. − 206 с.

40. Барышев Р. А. Киберпространство и проблема отчуждения: дис…. канд. фил. наук: 09.00.11. / Барышев Руслан Александрович. – Красноярск, 2009. − 130 с.

41. Беляк О. С. Ответственность за мошенничество по уголовному праву России: дис... канд. юрид. наук: 12.00.08 / Беляк Ольга Сергеевна. - М., 2006. − 153 с.

42. Бикмурзин М.П. Предмет преступления: теоретико-правовой анализ: дис… канд. юрид. наук: 12.00.08 / Бикмурзин Максим Петрович. - Уфа, 2005. − 196 с.

43. Богомолов А.А. Вымогательство в системе преступлений против собственности: криминологический анализ и предупреждение: дис... канд. юрид. наук: 12.00.08 / Богомолов Андрей Анатольевич. - М., 2005. − 145 с.

44. Буранова А.Г. Вымогательство и меры его предупреждения: дис... канд. юрид. наук: 12.00.08 / Буранова Анна Григорьевна. - Ростов-н/Д., 2011. − 221 с.

45. Ветошкина М.М. Ценные бумаги как предмет хищения: дис. … канд. юрид. наук: 12.00.08 / Ветошкина Марина Михайловна. – Екатеринбург, 2001. − 157 с.

46. Виноградов С.П. Противодействие незаконному предпринимательству: криминологический и уголовно-правовой аспекты: дис... канд. юрид. наук: 12.00.08 / Виноградов Сергей Павлович. - М., 2006. − 195 с.

47. Винокурова Н.С. Личность преступника и жертвы в механизме вымогательства и предупреждение этих преступлений: дис... канд. юрид. наук: 12.00.08 / Винокурова Наталья Сергеевна. - М., 2003. − 176 с.

48. Вишнякова Н.В. Объект и предмет преступлений против собственности: дис… канд. юрид. наук: 12.00.08 / Вишнякова Наталья Валерьевна. - Омск, 2003. − 210 с.

49. Вылков Р. И. Киберпространство как социокультурный феномен, продукт технологического творчества и проективная идея: дис. …канд. фил. наук: 09.00.01. / Вылков Ростислав Ильич. – Екатеринбург, 2009. − 151 с.

50. Гаджиев М.С. Криминологический анализ преступности в сфере компьютерной информации (по материалам Республики Дагестан): дис. … канд. юрид. наук: 12.00.08./ Гаджиев Марат Салахетдинович. – Махачкала, 2004. – 168 с.

51. Гарбатович Д.А. Квалификация уголовно-правовых деяний по субъективной стороне: дис. ... канд. юрид. наук: 12.00.08 / Гарбатович Денис Александрович. - Челябинск, 2004. − 208 с.

52. Гарькуша М. С. Электронные деньги как феномен виртуальной экономики: функции и способы институционализации: дис... канд. экон. наук: 08.00.01 / Гарькуша Марина Степановна. - Краснодар, 2010. − 147 с.

53. Гейцан Б. В. Совершенствование рыночного механизма электронных платежей: дис... канд. экон. наук.: 08.00.05 / Гейцан Богдан Владимирович. - М., 2008. − 173 с.

54. Герасимова Е.В. Предмет хищения в российском уголовном праве: дис…канд. юрид. наук: 12.00.08 / Герасимова Елена Владимировна. - М., 2006. − 194 с.

55. Головизнина И.А. Незаконное использование товарного знака: проблемы квалификации и правоприменения: дис... канд. юрид. наук: 12.00.08 / Головизнина Ирина Александровна - М., 2008. − 201 с.

56. Горюков Е. В. Электронные деньги: анализ практики использования и прогноз развития: дис... канд. экон. наук.: 08.00.10 / Горюков Евгений Валерьевич - Иваново, 2004. − 162 с.

57. Гребенюк А.В. Вина в российском уголовном праве: дис. ... канд. юрид. наук: 12.00.08 / Гребенюк Александр Владимирович - Ростов-н/Д., 2004. − 212 с.

58. Григорьева Л.В. Уголовная ответственность за мошенничество в условиях становления новых экономических отношений: дис... канд. юрид. наук: 12.00.08 / Григорьева Людмила Викторовна. - Саратов, 1996. − 197 с.

59. Гусейнова С.М. Проблемы уголовно-правовой регламентации легализации (отмывания) денежных средств или иного имущества, приобретенных преступным путем: дис... канд. юрид. наук: 12.00.08 / Гусейнова Салихат Магомедовна. - Ростов-н/Д., 2003. − 214 с.

60. Демьяненко Е. В. Уголовная ответственность за незаконное использование товарного знака: дис... канд. юрид. наук: 12.00.08 / Демьяненко Елена Владимировна. - Ростов-н/Д., 2003. − 185 с.

61. Дремлюга Р.И. Интернет-преступность: дис. ... канд. юрид. наук: 12.00.08 / Дремлюга Роман Игоревич. - Владивосток, 2007. − 248 с.

62. Егиазарян Ш.П. Электронные деньги в современной системе денежного оборота: дис... канд. экон. наук.: 08.00.10 / Егиазарян Шаген Петрович. - М., 1999. − 141 с.

63. Жайворонок А.В. Незаконное использование товарного знака: криминологическое и уголовно-правовое исследование: дис... канд. юрид. наук: 12.00.08 / Жайворонок Артем Викторович. - Омск, 2010. − 215 с.

64. Жариков Р.А. Детерминанты вымогательства и особенности его предупреждения в сверхкрупном городе: дис... канд. юрид. наук: 12.00.08 / Жариков Рустэм Александрович. - Челябинск, 2004. − 210 с.

65. Жданухин Д.Ю. Уголовно-правовая характеристика шантажа: дис... канд. юрид. наук: 12.00.08 / Жданухин Дмитрий Юрьевич. - Екатеринбург, 2005. − 146 с.

66. Жмыхов А.А. Компьютерная преступность за рубежом и ее предупреждение: дис. … канд. юрид. наук: 12.00.08 / Жмыхов Александр Александрович. – М., 2003. − 178 с.

67. Зубова М. А. Компьютерная информация как объект уголовно-правовой охраны: дис…. канд. юрид. наук: 12.00.08 / Зубова Марина Александровна. - Казань, 2008. − 215 с.

68. Зыков Д.А. Виктимологические аспекты предупреждения компьютерного мошенничества: дис. … канд. юрид. наук: 12.00.08 / Зыков Даниил Алексеевич. – Владимир, 2002. − 211 с.

69. Ивахненко А. М. Квалификация бандитизма, разбоя, вымогательства: проблемы соотношения составов: дис... канд. юрид. наук: 12.00.08 / Ивахненко Алла Михайловна. - М., 1996. − 272 с.

70. Качурин Д.В. Уголовная ответственность за обман и злоупотребление доверием (мошенничество) в отношении предприятий, организаций и коммерческих структур с различными формами собственности в период рыночных отношений: дис... канд. юрид. наук: 12.00.08 / Качурин Дмитрий Владимирович. - М., 1996. − 178 с.

71. Кесареева Т.П. Криминалистическая характеристика и проблемы предупреждения преступности в российском сегменте сети Интернет: дис…. канд. юрид. наук: 12.00.08 / Кесареева Татьяна Петровна. - М., 2002. − 195 с.

72. Комаров А.А. Криминологические аспекты мошенничества в глобальной сети «Интернет»: Дис… канд. юрид. наук: 12.00.08 / Комаров Антон Анатольевич. - Пятигорск. 2011. − 262 с.

73. Кондрашина В.А. Уголовная ответственность за незаконное использование товарного знака по законодательству России и зарубежных стран: дис... канд. юрид. наук: 12.00.08 / Кондрашина Валентина Анатольевна. - Казань, 2004. − 229 с.

74. Кораблёва С.Ю. Вина как уголовно-правовая категория и её влияние на квалификацию преступлений: дис. ... канд. юрид. наук: 12.00.08 / Кораблева Светлана Юрьевна. - М., 2013. − 212 с.

75. Корепанова И. А. Социальная специфика экономической преступности в современной России: дис... канд. соц. наук: 22.00.03 / Корепанова Ирина Анатольевна. - Новочеркасск, 2011. − 168 с.

76. Кочергин Д.А. Современные системы электронных денег: дис... докт. экон. наук:08.00.10 / Кочергин Дмитрий Анатольевич. - СПб., 2006. − 352 с.

77. Краснопеев В.А. Объект преступления в российском уголовном праве: теоретико-правовой анализ: дис. ... канд. юрид. наук: 12.00.08 / Краснопеев Владимир Александрович. - Кисловодск, 2001. − 186 с.

78. Кузахметов Д. Р. Легализация (отмывание) денежных средств или иного имущества, приобретенных преступным путем: вопросы теории, законодательного регулирования и практики: дис... канд. юрид. наук: 12.00.08 / Кузахметов Денис Рафаэльевич. - Казань, 2006. − 221 с.

79. Лейкина Н.С. Личность преступника и уголовная ответственность: дис... докт. юрид. наук. 12.00.08 / Лейкина Нина Семеновна. – Л.,1969. – 646 с.

80. Лесняк В.И. Мошенничество: уголовно-правовой и криминологический аспекты: дис... канд. юрид. наук: 12.00.08 / Лесняк Виктор Иванович. - Екатеринбург, 2000. − 202 с.

81. Лубешко В.Н. Незаконное предпринимательство как вид преступного посягательства против установленного порядка экономической деятельности:

уголовно-правовой и криминологический аспекты: дис.... канд. юрид. наук: 12.00.08 / Лубешко Валерий Николаевич. - Ростов-н/Д., 2004. − 231 с.

82. Лукьянова И. В. Угроза как преступление в уголовном праве России: дис. ... канд. юрид. наук: 12.00.08 / Лукьянова Инна Викторовна. - М., 2004. − 184с.

83. Лунин Н.Н. Мошенничество по уголовному законодательству России: уголовно-правовая характеристика и квалификация: дис... канд. юрид. наук: 12.00.08 / Лунин Николай Николаевич. - Орел, 2006. − 207с.

84. Мазуренко Е.А. Объект и предмет уголовно-правовой охраны преступлений против собственности: современные проблемы квалификации: дис... канд. юрид. наук: 12.00.08 / Мазуренко Елена Александровна. - М., 2003. − 248 с.

85. Марданов А. Б. Личность современного экономического преступника: дис... канд. юрид. наук: 12.00.08 / Марданов Азер Балай оглы. - Сургут, 2010. − 240 с.

86. Медведев С.С. Мошенничество в сфере высоких технологий: дис...канд. юрид. наук: 12.00.08 / Медведев Сергей Сергеевич. – Краснодар, 2008. − 210 с.

87. Мусаев Ф.А. Преступления против общего порядка осуществления экономической деятельности (ст. 171, 172–174.1 УК РФ): вопросы законодательной техники и дифференциации ответственности: дис... канд. юрид. наук: 12.00.08 / Мусаев Фарид Агарза оглы. - Ярославль, 2005. − 191 с.

88. Окружко В.Ю. Современное мошенничество: криминологическая характеристика и предупреждение: дис.... канд. юрид. наук: 12.00.08 / Окружко Виктория Юрьевна. - Ростов-н/Д., 2009. − 182 с.

89. Оленев Р.Г. Мошенничество как вид девиантного экономического поведения: дис... канд. экон. наук: 22.00.03 / Оленев Роман Георгиевич. - СПб., 2000. − 163 с.

90. Павлов С.Н. Объект и последствия преступления в теории уголовного права: дис. ... канд. юрид. наук: 12.00.08 / Павлов Сергей Николаевич. - Ростов-н/Д., 2011. − 206 с.

91. Паньков И.В. Умышленная вина по российскому уголовному праву: теоретический и нормативный аспекты: дис. ... канд. юрид. наук: 12.00.08 / Паньков Илья Владимирович. - СПб., 2010. − 323 с.

92. Педун О.Л. Легализация денежных средств или иного имущества, приобретенных преступным путем: дис... канд. юрид. наук: 12.00.08 / Педун Ольга Леонидовна. - М., 2004. − 194 с.

93. Плотников С.А. Уголовная ответственность за незаконное предпринимательство: дис... канд. юрид. наук: 12.00.08 / Плотников Сергей Анатольевич. - М., 2003. С− 219 с.

94. Радзевановская Ю. В. Легализация (отмывание) денежных средств или иного имущества, приобретенных преступным путем: уголовно-правовая и криминологическая характеристика: дис... канд. юрид. наук: 12.00.08 / Радзевановская Юлия Викторовна. - Уфа, 2005. − 182 с.

95. Рассказов М. Ю. Уголовная ответственность за вымогательство: дис... канд. юрид. наук: 12.00.08 / Рассказов Михаил Юрьевич. - Ростов-н/Д., 2002. − 161 с.

96. Рищенко Д.В. Рынок информационного продукта: особенности и методизмы функционирования. дис... канд. экон. наук: 08.00.01 / Рищенко Дмитрий Викторович. - М., 1996. − 139 с.

97. Рыбаков Д. В. Легализация денежных средств или иного имущества в российском уголовном праве: дис... канд. юрид. наук: 12.00.08 / Рыбаков Денис Валерьевич. - М., 2002. − 167 с.

98. Рыжкова И.Д. Вымогательство: теоретико-правовой анализ и криминологическая характеристика: дис... канд. юрид. наук: 12.00.08 / Рыжкова Ирина Дмитриевна. - М., 2008. − 257 с.

99. Саркисян А.Ж. Незаконная банковская деятельность: уголовно-правовые аспекты: дис... канд. юрид. наук: 12.00.08 / Саркисян Армен Жораевич. - Ростов-н/Д., 2007. − 181 с.

100. Селиванов И. О. Присвоение или растрата: уголовно-правовые и криминологические аспекты: дис... канд. юрид. наук: 12.00.08 / Селиванов Игорь Олегович. - Калининград, 2002. − 178 с.

101. Семина Л.В. Уголовно-правовые и криминологические аспекты мошенничеств, совершаемых в сфере экономической деятельности: дис... канд. юрид. наук: 12.00.08 / Семина Людмила Васильевна. - Краснодар, 2003. – 215 с.

102. Семченков И. П. Объект преступления: социально-философские и методологические аспекты проблемы: дис. ... канд. юрид. наук: 12.00.08 / Семченков Игорь Павлович. - М., 2003. − 192 с.

103. Скляров С.В. Вина и мотивы преступного поведения как основание дифференциации и индивидуализации ответственности: дис… докт. юрид. наук: 12.00.08 / Скляров Сергей Валерьевич. - М., 2004. – 495 с.

104. Склярук С.А. Уголовная ответственность за незаконное использование товарного знака: дис... канд. юрид. наук: 12.00.08 / Склярук Сергей Анатольевич. - М., 1999. − 210 с.

105. Скрипников Д.Ю. Присвоение и растрата как способы изъятия и обращения чужого имущества, вверенного виновному: дис... канд. юрид. наук: 12.00.08 / Скрипников Денис Юрьевич. - М., 2009. − 202 с.

106. Спиридонова О.Е. Символ как предмет преступления: дис... канд. юрид. наук: 12.00.08 / Спиридонова Ольга Евгеньевна. - Ярославль, 2002. − 215 с.

107. Станицкий С.С. Мобильные деньги как средство осуществления расчётов в информационной экономике: дис... канд. экон. наук: 08.00.01 / Станицкий Станислав Сергеевич. - М., 2003. − 239 с.

108. Старичков М.В. Умышленные преступления в сфере компьютерной информации: уголовно-правовая и криминологическая характеристика: дис.... канд. юрид. наук: 12.00.08 / Старичков Максим Владимирович. – Иркутск, 2006. − 237 с.

109. Степанов-Егиянц В.Г. Преступления сфере безопасности обращения компьютерной информации: сравнительный анализ: дис. …канд. юрид. наук: 12.00.08 / Степанов-Егиянц Владимир Георгиевич. — М., 2005. − 168 с.

110. Субботина И.В.Уголовная ответственность за принуждение к совершению сделки или отказу от ее совершения: дис... канд. юрид. наук: 12.00.08 / Субботина Ираида Васильевна. - Пятигорск, 2006. − 197 с.

111. Сунчалиева Л.Э. Мошенничество: уголовно-правовой и криминологический аспект: дис... канд. юрид. наук: 12.00.08 / Сунчалиева Лейла Эмирбековна. - Ставрополь, 2004. − 187 с.

112. Суслина Е.В. Ответственность за мошенничество по Уголовному кодексу Российской Федерации: дис... канд. юрид. наук: 12.00.08 / Суслина Елена Владимировна. - Екатеринбург, 2007. − 191 с.

113. Тагиев Т.Р. Вымогательство по уголовному праву России: дис... канд. юрид. наук: 12.00.08 / Тагиев Табриз Рафаил-оглы. - Томск, 2011. − 211 с.

114. Таций В.Я. Проблема ответственности за хозяйственные преступления: объект и система: дис… докт. юрид. наук: 12.00.08 / Таций Василий Яковлевич. - Харьков, 1984. − 424 с.

115. Тер-Аванесов И.Г. Легализация денежных средств или иного имущества, приобретенных преступным путем: дис... канд. юрид. наук: 12.00.08 / Тер-Аванесов Игорь Геннадьевич. - Ставрополь, 2005. − 191 с.

116. Трейгер С.М. Уголовная ответственность за незаконное использование товарного знака: дис... канд. юрид. наук: 12.00.08 / Трейгер Семен Михайлович. - М., 2011. − 199 с.

117. Тропина Т.Л. Киберпреступность: понятие, состояние, уголовно-правовые меры борьбы: дис. …канд. юрид. наук: 12.00.08 / Тропина Татьяна Львовна. — Владивосток. 2005. − 235 с.

118. Урда М.Н. Проблемы применения нормы, устанавливающей ответственность за незаконное предпринимательство: дис... канд. юрид. наук: 12.00.08 / Урда Маргарита Николаевна. - Курск, 2010. − 209 с.

119. Флоря Е.К. Личность преступника: криминологическое и уголовно-правовое исследование: дис... канд. юрид. наук: 12.00.08 / Флоря Евгений Константинович. - Кишинев, 2002. − 185 с.

120. Фомичева М.А. Угроза как способ совершения преступления: дис. ... канд. юрид. наук: 12.00.08 / Фомичева Марина Александровна. - М., 2008. – 205 с.

121. Хуторной С.Н. Киберпространство и становление сетевого общества: дис… канд. фил. наук: 09.00.11 / Хуторной Сергей Николаевич. – Воронеж, 2013. − 166 с.

122. Черепенников Р.В. Цели преступного деяния и их уголовно-правовое значение: дис. ... канд. юрид. наук: 12.00.08 / Черепенников Роман Валентинович. - М., 2011. − 225 с.

123. Шебунов А.А. Легализация денежных средств и иного имущества, приобретенных незаконным путем: дис... канд. юрид. наук: 12.00.08 / Шебунов Антон Анатольевич. - М., 1998. − 195 с.

124. Шульга А.В. Объект и предмет преступления против собственности в условиях рыночных отношений и информационного общества: дис… докт. юрид. наук: 12.00.08 / Шульга Андрей Владимирович. - Волгоград, 2008. − 422 с.

125. Шульга А.В. Присвоение или растрата в условиях становления рыночных отношений: дис... канд. юрид. наук: 12.00.08 / Шульга Андрей Владимирович. - Краснодар, 2000. − 192с.

126. Щербина В.В. Ответственность за вымогательство: социально-правовые аспекты: дис... канд. юрид. наук: 12.00.08 / Щербина Владимир Васильевич. - Ростов-н/Д., 1999. − 203 с.

127. Яшков С.А. Информация как предмет преступления: дис. …канд. юрид. наук: 12.00.08 / Яшков Сергей Александрович. - Екатеринбург, 2005. − 151 с.

Авторефераты диссертаций

128. Авдеева О.А. Незаконное предпринимательство: уголовно-правовая характеристика и ответственность: автореф. дис.... канд. юрид. наук: 12.00.08 / Авдеева Ольга Анатольевна.- Иркутск, 2009. − 21 с.

129. Вехов В.Б. Криминалистическая характеристика и совершенствование практики расследования и предупреждения преступлений, совершаемых с

использованием компьютерной техники: автореф. дис. … канд. юрид. наук: 12.00.08 // Вехов Виталий Борисович. – Волгоград, 1995. − 27 с.

130. Гузеева О.С. Предупреждение размещения информации, способствующей распространению наркотических средств, в российском сегменте сети Интернет (криминологические и уголовно-правовые проблемы): автореф. дис. … канд. юрид. наук: 12.00.08 / Гузеева Ольга Сергеевна. - М., 2008. − 25 с.

131. Емельянова Е.А. Правовые последствия манипулирования информацией на рынках: автореф. дис.... канд. юрид. наук: 12.00.03/ Емельянова Екатерина Анатольевна. – СПб., 2013. − 23 с.

132. Желудков М.А. Развитие системы криминологического обеспечения защиты личности и общества от корыстных преступлений против собственности: автореф. дис. … докт. юрид. наук: 12.00.08 // Желудков Михаил Александрович. – М., 2012. − 47 с.

133. Зотов П.В. Уголовно-правовая и криминологическая характеристика незаконной банковской деятельности: автореф. дис.... канд. юрид. наук: 12.00.08 / Зотов Павел Владимирович. - М., 2007. − 24 с.

134. Иванова Я. Е. Незаконное предпринимательство: вопросы теории и проблемы правоприменения: автореф. дис.... канд. юрид. наук: 12.00.08 / Иванова Яна Евгеньевна. - М., 2010. − 34 с.

135. Карпов В.С. Уголовная ответственность за преступления в сфере компьютерной информации: автореф. дис. ... канд. юрид. наук: 12.00.08 / Карпов Виктор Сергеевич. - Красноярск. 2002− 27 с.

136. Лопатина Т.М. Криминологические и уголовно-правовые основы противодействия компьютерной преступности: автореф. дис… докт. юрид. наук: 12.00.08 / Лопатина Татьяна Михайловна. – М., 2006. − 60 с.

137. Малиев С. О. Электронные деньги и платёжные системы на их основе: автореф. дис... канд. экон. наук.: 08.00.10 / Малиев Сослан Олегович. - СПб., 2008. − 21с.

138. Мильчехина Е. В. Уголовно-правовой и криминологический анализ незаконной банковской деятельности: автореф. дис.... канд. юрид. наук: 12.00.08 / Мильчехина Елена Владимировна. - Екатеринбург, 2010. – 28 с.

139. Нафиков И.И. Принуждение к совершению сделки или отказу от ее совершения: криминологические и уголовно-правовые аспекты: автореф. дис.... канд. юрид. наук: 12.00.08 / Нафиков Ильнур Илдусович. - М., 2012. − 23 с.

140. Челноков В. В. Компьютерная информация как предмет преступления в отечественном уголовном праве: автореф. дис… канд. юрид. наук: 12.00.08 / Челноков Владислав Валерьевич. - Екатеринбург, 2013. − 31 с.

141. Чхвимиани Э.Ж. Уголовно-правовые и криминологические аспекты противодействия вымогательству: по материалам Краснодарского края: автореф. дис.... канд. юрид. наук: 12.00.08 / Чхвимиани Эдуард Жюльенович. - Ростов-н/Д., 2011. − 27 с.

Монографии, учебники, учебные пособия

142. Батурин Ю.М. Право и политика в компьютерном круге: монография / Ю.М. Батурин. − М., 1987. − 112с.

143. Батурин Ю.М. Проблемы компьютерного права: монография / Ю.М. Батурин. −М., Юридическая литература. 1991. − 160 с.

144. Бойцов А.И. Преступления против собственности: учебное пособие / А.И. Бойцов. − СПб., Юридический центр ПРЕСС. 2002. − 775 с.

145. Вехов В.Б. Компьютерные преступления: способы совершения, методики расследования: монография / В.Б. Вехов. − М., 1996. − 182 с.

146. Волеводз А.Г. Противодействие компьютерным преступлениям: правовые основы международного сотрудничества: монография / А.Г. Волеводз. − М., Юрлитинформ, 2001. − 496 с.

147. Волженкин Б.В. Преступления в сфере экономической деятельности по уголовному праву России: монография / Б.В. Волженкин. − Спб., Юридический центр Пресс. 2007. − 765с.

148. Дашян М.С. Право информационных магистралей: вопрос правового регулирования в сети «Интернет»: монография / М.С. Дашян. − М., Волтерс Клувер, 2007. − 248 с.

149. Дворецкий М.Ю., Копырюлин А.Н. Оптимизация уголовной ответственности и проблемы квалификации преступлений в сфере компьютерной информации: монография. / М.Ю.Дворецкий, А.Н. Копырюлин. − Тамбов, ТГУ им. Г.Р. Державина. 2006. − 212 с.

150. Дремлюга Р.И. Интернет-преступность: монография / Р.И. Дремлюга. − Владивосток, Изд. Дальневосточного университета. 2008. − 240 с.

151. Логинов Е.Л. Отмывание денег через Интернет-технологии: Методы использования электронных финансовых технологий для легализации криминальных доходов и уклонения от уплаты налогов: монография / Е.Л. Логинов. − М., ЮНИТИ-ДАНА. 2012. − 208 с.

152. Побегайло А.Э. Киберпреступность: лекция / А.Э. Побегайло. − М., Академия Генеральной прокуратуры Российской Федерации. 2013. − 50 с.

153. Прозументов Л.М., Шеслер А.В. Криминология (общая часть): учебник / Л.М., Прозументов А.В. Шеслер. − Томск, Томский филиал Академии ФСИН России. 2007. − 238 с.

154. 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. – 199 с.

155. Рассолов И.М. Право и «Интернет»: теоретические проблемы / И.М. Рассолов. − 2-е изд., перераб. и доп. − М., Норма. 2009. − 210 с.

156. Яни П.С. Мошенничество и иные преступления против собственности: уголовная ответственность. Книга третья: монография / П.С. Яни. − М., Библиотека журнала «Уголовное право». 2007. − 136 с.

157. Яни П.С. Посягательства на собственность: монография / П.С. Яни. − М., Библиотека российского судьи. 1998. − 65 с.

Статьи

158. Гузеева О.С. Квалификация мошенничества в российском сегменте сети Интернет / О.С. Гузеева // Законность. − 2013. − №3 (941). − С. 21-24.

159. Гузеева О.С. Действие Уголовного кодекса России в отношении интернет-преступлений / О.С. Гузеева // Законы России: опят, анализ, практика. − 2013. − №10. - С. 15-19.

160. Дремлюга Р.И. Международно-правовое регулирование сотрудничества в сфере борьбы с Интернет-преступностью / Р.И. Дремлюга // Библиотека криминалиста.− 2013. − №5(10). – С.339-346.

161. Желудков М.А. Криминологический анализ содержания угрозы в виде рейдерства для общественных отношений собственности / М.А. Желудков // Вестник Тамбовского университета. Серия: Гуманитарные науки. − 2009. – № 3 (71). − С. 268-271.

162. Желудков М.А. Новый взгляд на концепцию объекта защиты от корыстных преступлений против собственности / М.А. Желудков // Вестник Воронежского института МВД России. − 2011. − №1.– С.47-51

163. Желудков М.А. Обоснование реализации системных защитных мер в механизме предупреждения корыстной преступности / М.А. Желудков // Вестник Волгоградской академии МВД России. − 2014. − № 4 (31). – С. 47-51.

164. Желудков М.А. Ююкина М.В. Вопросы повышения эффективности обеспечения безопасности собственности при совершении корыстных преступлений / М.А. Желудков, М.В. Ююкина // Вестник Тамбовского университета. Серия: Гуманитарные Науки. − 2013. − №8(124). – С. 397-401.

165. Желудков М.А., Ююкина М.В. Системные особенности информационного обеспечения защиты объектов собственности от корыстных преступлений против собственности / М.А. Желудков, М.В. Ююкина // Вестник Тамбовского университета. Серия: Гуманитарные Науки. − 2013. − №7(123). – С. 359-363.

166. Киселёв А.К. Киберпреступность – взгляд из Европы / А.К. Киселёв // Библиотека криминалиста.− 2013. − №5(10). − С.309-313.

167. Козаев Н.Ш. Некоторые новеллы уголовного законодательства, направленные на обеспечение экономической безопасности в условиях научно-технического прогресса / Н.Ш. Козаев // Библиотека криминалиста.− 2013. − №5(10). – С.15-21.

168. Коменский Н.А. Компьютерная информация и информационные технологии как средство совершения преступления / Н.А. Коменский // 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.133-139.

169. Кочои С.М. Новые нормы о мошенничестве в УК РФ: особенности и отличия / С.М. Кочои // Криминологический журнал Байкальского государственного университета экономики и права. − 2013. − № 4. – С. 104-110.

170. Лапутин М.М. Уголовная ответственность за неправомерный доступ к компьютерной информации: общая характеристика и некоторые проблемы квалификации / М.М. Лапутин // Библиотека криминалиста.− 2013. − №5(10). – С.23-31.

171. Лопатина Т.М. Проблемы формирования уголовно-правового способа борьбы с компьютерным мошенничеством / Т.М. Лопатина // Библиотека криминалиста.− 2013. − №5(10). – С.32-41.

172. Мошков А.Н. Информационная безопасность России: новые вызовы, угрозы, решения / А.Н. Мошков // Информационная безопасность России: аналитический сборник. 2014. Вып.1. – С.86-87.

173. Мутасова М.А. Мошенничество в информационной сфере / М.А. Мутасова // 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.184-189.

174. Номоконов В.А., Тропина Т.Л. Киберпреступность: прогнозы и проблемы борьбы / В.А. Номоконов, Т.Л. Тропина // Библиотека криминалиста.− 2013.− №5(10). − С.148-159.

175. Нургалиев Р. Электронный патруль / Р. Нургалиев // Правовые вопросы национальной безопасности. - 2009. - № 5-6. - С. 25 - 29

176. 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.

177. Простосердов, М.А. Вымогательство, совершенное в сети Интернет / М.А. Простосердов // Библиотека криминалиста. Научный журнал. – 2013. − №6 − С. 150-152.

178. 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. Выпуск № 3. Под ред. Ю.Е. Пудовочкина и А.В. Бриллиантова. М., РАП. 2013г. – С. 198-209.

179. Простосердов М.А. Легализация (отмывание) денежных средств в киберпространстве / М.А. Простосердов // Российское правосудие. – 2014. - № 9(101). – С. 75 – 80.

180. 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 / Под ред. А.В. Бриллиантова и Ю.Е. Пудовочкина. − М.: РГУП, 2015. – С. 334-351.

181. Простосердов М.А. Проблемы квалификации компьютерных преступлений / М.А. Простосердов // Российское правосудие. – 2012. − № 6 (74) - С. 106 –108.

182. 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.

183. 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).

184. Рябов В.О. Электронные деньги в России. Проблемы использования и регулирования / В.О. Рябов // Креативная экономика.− 2010. − № 9(45). − С. 31-37.

185. Сабадаш В.П. Специальные подразделения и организации по борьбе с Интернт-мошенничеством в различных государствах мира / В.П. Сабадаш // Библиотека криминалиста.− 2013. − №5(10). – С.328-338.

186. Савельев А.И. Правовая природа виртуальных объектов, приобретаемых за реальные деньги в многопользовательских играх / А.И.

Савельев // Вестник гражданского права. − 2014. −N 1. − СПС «КонсультантПлюс».

187. Семёнов К.П., Симонова А.Э. законодательное регулирование и уголовно-правовая защита информационных правоотношений: состояние и перспективы / К.П. Семёнов, А.Э. Симонова // Информационная безопасность регионов. – 2011. −№ 2(9). – С.90-93.

188. Смирнов А.А. Сеть «Интернет» в механизме криминологической детерминации / А.А. Смирнов // Библиотека криминалиста. − 2013. − №5(10). – С.161-173.

189. Суслопаров А.В. Некоторые направления совершенствования законодательства об ответственности за компьютерные преступления с учетом международного опыта / А.В. Суслопаров // 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.105-110.

190. Сухомлинов В.В. Вопрос – Ответ / В.В. Сухомлинов. // Юный техник. − 1989. − №5. – С. 78.

191. Фатьянов А.А.Правовой анализ категории «электронные денежные средства» в российском законодательстве / А.А. Фатьянов // Гражданское общество в России и за рубежом. − 2014. − N 3. − СПС «КонсультантПлюс».

192. Филимонов С.А. Ошибки и затруднения, возникающие при квалификации киберпреступлений / С.А. Филимонов // Библиотека криминалиста.− 2013. − №5(10). – С.48-54.

193. Хилюта В.В. Хищение с использованием компьютерной техники или компьютерное мошенничество? / В.В. Хилюта // Библиотека криминалиста.− 2013. − №5(10). – С.55-65.

Электронные ресурсы

194. Анализ обращений в CERT-GIB за 2013 год... - Group-IB Расследование компьютерных преступлений. [Электронный ресурс]// URL: https://www.facebook.com/GroupIB/posts/640006572733415 (Дата обращения: 27.01.2014).

195. Газета Белла-Италия // [Электронный ресурс] URL: http:// bellaitalia.at.ua/news/svjaz_v_italii/2012-11-05-94 (Дата обращения: 06.01.2013).

196. Дадали А. Электронный банкинг [Электронный ресурс] // URL:http://www.compress.ru/article.aspx?id=10653&iid=434 (Дата обращения: 05.05.2012).

197. Деловая пресса [Электронный ресурс] // URL:http://www.businesspress.ru/newspaper/article_ mId_21961_aId_317463.html (Дата обращения: 02.08.2014).

198. Доклад компании Group-IB «Threat Intelligence Report 2012 – 2013 H1» [Электронный ресурс] // URL: http://report2013.group-ib.ru/ (Дата обращения: 26.04.2012).

199. Доклад компании Norton «Norton Report-2013: Symantec» [Электронный ресурс] // URL:http://www.symantec.com/about/news/resources/ press_kits/detail.jsp?pkid=norton-report-2013 (Дата обращения: 26.04.2014).

200. Дубко М. Международное сотрудничество в сфере уголовно-правовой борьбы с неправомерным завладением компьютерной информацией [Электронный ресурс] // URL:http://www.crime-research.ru/articles/Dubko_0001 (Дата обращения: 27.08.2014).

201. Официальный сайт «Европола». Оценка угрозы организованной преступности в ЕС на 2013 год. [Электронный ресурс] // URL: https://www.europol.europa.eu/sites/default/files/publications/socta2013.pdf (Дата обращения: 26.04.2012).

202. Информационный ресурс «Bizhit». Интернет в России и в мире. [Электронный ресурс] // URL:http://www.bizhit.ru/index/users_count/0-151 (Дата обращения: 02.08.2014).

203. Информационный ресурс «BugTraq.Ru» История компьютерного андеграунда Хакеры 80-х [Электронный ресурс] // URL: http://bugtraq.ru/library/underground/underground4.html (Дата обращения: 1.05.2012).

204. Информационный ресурс «China Space». [Электронный ресурс] //URL: http://www.chinaspace.ru/internet-tolko-po-pasportu/ (Дата обращения: 06.01.2013).

205. Информационный ресурс «Ciec.org». Reno vs. ACLU, 117 S.Ct. 2329 (1997) (casebook at 932-53). [Электронный ресурс] // URL:http//ciec.org/SC_appeal/opinion.shtml. (Дата обращения: 27.05.2012).

206. Информационный ресурс «Group-IB». Русский рынок компьютерных преступлений: состояние и тенденции 2011. [Электронный ресурс] // URL:http://www.group-ib.ru/images/analytics/group-ib_report_2011_rus.pdf (Дата обращения: 26.04.2015).

207. Информационный ресурс «Hi-Tech.Mail.Ru» [Электронный ресурс] // URL: http://hi-tech.mail.ru/bytovaya/polaris-wi-fi.html (Дата обращения: 08.03.2014).

208. Информационный ресурс «Mari Uver». [Электронный ресурс]// URL: http://mariuver.wordpress.com/2011/09/13/brach-aferist/ (Дата обращения: 27.01.2014).

209. Информационный ресурс «Over Betting». Закрыто Интернет казино White Club [Электронный ресурс] // URL: http://www.overbetting.ru/ news/casino/zakryto-internet-kazino-white-club.html (Дата обращения: 24.06.2013).

210. Информационный ресурс «The Wall Street Journal» [Электронный ресурс] // URL: http://blogs.wsj.com/developments/2013/12/17/hamptons-seller-tries-new-pitch-buy-my-house-in-bitcoin/?mod=WSJ_3Up_RealEstate (Дата обращения: 5.04.2015).

211. Информационный ресурс «Барфик». Самые известные хакеры. [Электронный ресурс] // URL:http:// barfik.com/people/samyie-luchshie-hakeryi-v-mire.html (Дата обращения: 26.04.2014).

212. Информационный ресурс «Бизнес ФМ». Электронная торговля отправится в регионы. [Электронный ресурс] // URL: http://www.bfm.ru /news/101235 (Дата обращения: 15.04.2014).

213. Информационный ресурс «Вести.ру» [Электронный ресурс] // URL: http://www.vesti.ru/videos/ show/vid/379888/# (Дата обращения: 26.04.2014).

214. Информационный ресурс «Информационная безопасность». [Электронный ресурс] URL:http://www.itsec.ru/newstext.php?news_id=91024 (Дата обращения: 01.09.2013).

215. Информационный ресурс «Казино 367». Закрыта Голдфишка. [Электронный ресурс] URL: http://casino367.com/news/close-golfishka-2/ (Дата обращения: 24.06.2013).

216. Информационный ресурс «Компьютерная газета». [Электронный ресурс]URL: http://www.nestor.minsk.by/kg/2002/31/kg23101a.html (Дата обращения: 27.05.2012).

217. Информационный ресурс «Налог.ру» [Электронный ресурс] // URL: http://www.nalog.ru/rn77/news/activities_fts/4460907/ (Дата обращения: 08.01.2014).

218. Информационный ресурс «Русский проект». Мобильная связь и компьютерные сети в СССР. [Электронный ресурс] // URL: http://www.rusproject.org/node/72 (Дата обращения: 05.05.2012).

219. Информационный ресурс «Улфек». Компьютерная преступность. [Электронный ресурс] // URL: http://ulfek.ru/osnovy-bezopasnosti-informatsionnykh-tekhnologij/3469-kompyuternaya-prestupnost.html (Дата обращения: 1.05.2012).

220. Информационный ресурс «Хабрахабр» [Электронный ресурс] URL:http://habrahabr.ru/post/102427/ (Дата посещения 21.01.2015).

221. Информационный ресурс «Хакер.ру» [Электронный ресурс] // URL: https://xakep.ru/2002/05/30/ 15400/ (Дата обращения: 26.04.2014).

222. Информационный ресурс «Яндекс.Маркет». Компьютеры // [Электронный ресурс] URL:http://market.yandex.ru/search.xml?&hid=91011 &track=menuleaf&how=dprice&np=1 (Дата посещения 21.01.2015).

223. Информационный ресурс «CERT-GIB». Анализ обращений в CERT-GIB за 2013 год - Group-IB Расследование компьютерных преступлений. [Электронный ресурс] // URL: https://www.facebook.com/GroupIB/posts/640006572733415 (Дата обращения: 27.01.2014).

224. Концепция Стратегии Кибербезопасности Российской Федерации. [Электронный ресурс] //URL:http://www.council.gov.ru/media/files/41d4b3dfbdb25cea8a73.pdf (Дата обращения: 28.04.2012).

225. Официальный сайт «Бизнес ФМ» [Электронный ресурс] // URL: http://bfm.ru/news/303135. URL:http://bfm.ru/news/303004. (Дата обращения: 4.10.2015).

226. Официальный сайт «Итар-тасс» [Электронный ресурс] // URL: http://itar-tass.com/ekonomika/ 783989 (Дата обращения: 5.04.2015).

227. Официальный сайт Парламента Швецарии [Электронный ресурс] // URL: http://www.parlament.ch/e/suche/Pages/geschaefte.aspx?gesch_id= 20134070 (Дата обращения: 5.04.2015).

228. Официальный сайт «Европола». Socta 2013. EU Serious and Organised Crime Threat Assessment. [Электронный ресурс] // URL: https://www.europol.europa.eu/sites/default/files/publications/socta2013.pdf (Дата обращения: 18.04.2014).

229. Официальный сайт «ИТАР-ТАСС» [Электронный ресурс] // URL: http://tasstelecom.ru/news/one/23775 (Дата обращения: 27.05.2012).

230. Информационный ресурс «Икс Медиа». Серый, черный, белый Интернет [Электронный ресурс] // URL: http://www.iksmedia.ru/articles/4808504.html (Дата обращения: 27.05.2012).

231. Официальный сайт Российская газета [Электронный ресурс] // URL: http://www.rg.ru/2013/09/10/internet-moshenniki-site-anons.html (Дата обращения 08.03.2014).

232. Официальный сайт «Kaspersky Lab». [Электронный ресурс] .// URL: http://www.kaspersky.ru/about (Дата обращения: 26.04.2014).

233. Официальный сайт информационного агентства «Russia Today» [Электронный ресурс] // URL: http://rt.com/usa/bitcoin-sec-shavers-texas-231/ (Дата обращения: 5.04.2015).

234. Официальный сайт магазина «Амазон» [Электронный ресурс] // URL: www.amazon.com (Дата обращения: 05.05.2012).

235. Официальный сайт МВД РФ [Электронный ресурс] // URL: https://mvd.ru/upload/site1/import/65afff0dd0.pdf (Дата обращения: 20.01.2015).

236. Официальный сайт МВД РФ [Электронный ресурс] // URL: https://mvd.ru/folder/101762/item/804701/ (Дата обращения: 20.01.2015).

237. Официальный сайт МВД РФ [Электронный ресурс] URL: http://68.mvd.ru/news/item/576876 (Дата обращения: 01.08.2014).

238. Официальный сайт МВД РФ [Электронный ресурс] URL: http://mvd.ru/upload/site1/import/65afff0dd0.pdf (Дата обращения: 06.09.2013).

239. Официальный сайт системы «Биткойн». [Электронный ресурс] // URL: http://bitcoin.org/ru/ (Дата обращения: 27.08.2013).

240. Официальный сайт Следственного Комитета Российской Федерации [Электронный ресурс] URL: http://www.sledcom.ru/actual/372197/ (Дата обращения: 27.02.2014).

241. Официальный сайт Федеральной службы государственной статистики. [Электронный ресурс] // URL:http://www.gks.ru/wps/wcm/connect/ rosstat_main /rosstat/ru/statistics/population/ (Дата обращения: 19.02.2015).

242. Официальный сайт ФНС РФ. [Электронный ресурс] // URL: http://www.nalog.ru/rn68/related_activities/registration_ip_yl/reg_yl/changes/3796283/ (Дата обращения: 26.04.2014).

243. Портал государственных услуг Москвы. [Электронный ресурс] // URL:http://pgu.mos.ru/ru (Дата обращения: 12.09.2014).

244. Рекомендация Комитета министров Совета Европы №89 от 13.09.1989 [Электронный ресурс] // URL: https://wcd.coe.int/ com.instranet.InstraServlet? command=com.instranet. CmdBlob Get&InstranetImage=610660&SecMode=1 &DocId=702280&Usage=2 (Дата обращения: 27.01.2013).

245. Сабадаш В. Проблемы латентности компьютерной преступности. Crime-research.ru [Электронный ресурс] // URL:http://www.crime-research.ru/library/Sabodash0304.html (Дата обращения: 08.03.2014).

246. Свод законодательства США Раздел 18, часть 1, глава 47, §1030 Computer Fraud and Abuse Act (CFAA) [Электронный ресурс] // URL: http://www.law.cornell.edu/uscode/text/18/1030 (Дата обращения: 27.04.2012).

247. Социальная сеть «Classmates». [Электронный ресурс] // URL: http://www.classmates.com/ (Дата обращения: 05.05.2012).

248. Среднесрочный прогноз «Биткойн» от сайта «Matbea», Форум «Биткойн» [Электронный ресурс] // URL: http://blog.matbea.com/194993btc/(Дата обращения: 24.04.2014).

249. Сухаренко А.Н. Современные криминальные вызовы и угрозы информационной безопасности России [Электронный ресурс] // URL: http://sartraccc.ru/Press/special/contr_terror_1_12.pdf (Дата обращения: 5.08.2015).

250. Уголовный кодекс Испании [Электронный ресурс] // URL: http://noticias.juridicas.com/base_datos/Penal/lo10-1995.l2t13.html#a278 (Дата обращения 25.08.2014).

251. Уголовный кодекс Финляндии [Электронный ресурс] // URL: http://www.finlex.fi/en/laki/kaannokset/1889/en18890039.pdf (Дата обращения 25.08.2014).

252. Уголовный кодекс Швейцарии [Электронный ресурс] // URL:http://law.edu.ru/norm/norm.asp?normID=1241950&subID=100098712,100098714,100098872,100099140,100099172#text (Дата обращения 25.08.2014).

253. Уголовный кодекс Австрии [Электронный ресурс] // URL: http://www.gesetze-im-internet.de/stgb/ (Дата обращения 25.07.2015).

254. Уголовный кодекс Белоруссии [Электронный ресурс]// URL:http://etalonline.by/?type=text&regnum=hk9900275#load_text_none_1 (Дата обращения:06.01.2013).

255. Уголовный кодекс Германии с изменениями от 28 декабря 2003 года. [Электронный ресурс] URL: http://lexetius.com/StGB/263a (Дата обращения: 20.01.2013).

256. Уголовный кодекс Дании. [Электронный ресурс] // URL: https://www.retsinformation.dk/Forms/R0710.aspx?id=152827#Kap28 (Дата обращения: 27.01.2013).

257. Уголовный кодекс Италии [Электронный ресурс] // URL:http://www.altalex.com/?idnot=36653 (дата обращения 25.08.2014).

258. Уголовный кодекс Китайской Народной Республики [Электронный ресурс] // URL: http://constitutions.ru/archives/403 (Дата обращения:06.01.2013).

259. Уголовный кодекс Нидерландов [Электронный ресурс] // URL: http://wetten.overheid.nl/BWBR0001854/TweedeBoek/TitelV/Artikel138ab/geldigheidsdatum_29-09-2013 (Дата обращения: 27.01.2013).

260. Уголовный кодекс Республики Корея [Электронный ресурс] // URL: http://www.crime.vl.ru/index.php?p=1324&more=1 (Дата обращения: 06.01.2013).

261. Уголовный кодекс Украины [Электронный ресурс] // URL: http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=2341-14&p=1214905443606898 (Дата обращения:06.01.2013).

262. Уголовный кодекс Эстонии [Электронный ресурс] URL: http://www.hot.ee/almanach/kriminaalseadustik.html (Дата обращения: 27.01.2012).

263. Парламентская библиотека. Государственные стратегии кибербезопасности [Электронный ресурс] // URL: http://www.securitylab.ru/ (Дата обращения: 27.01.2013).

264. Резолюция Генеральной Ассамблеи ООН от 31 января 2002 N 56/261 «Планы действий по осуществлению Венской декларации о преступности и правосудии: ответы на вызовы XXI века» (Принята в г. Нью-Йорке на 93-м пленарном заседании 56-ой сессии Генеральной Ассамблеи ООН) // СПС «КонсультантПлюс».

265. Форум «Ламборджини» [Электронный ресурс] // URL: http://lamborghininewportbeach.blogspot.ru/2013/12/the-bitcoin-saga-continues.html (Дата обращения: 5.04.2015).

266. Черкасов В.Н. Информационные технологии и организованная преступность [Электронный ресурс] URL: http://www.crime-research.ru/library/Cherkas03.html (Дата обращения:20.01.2015).

ПРИЛОЖЕНИЕ №1

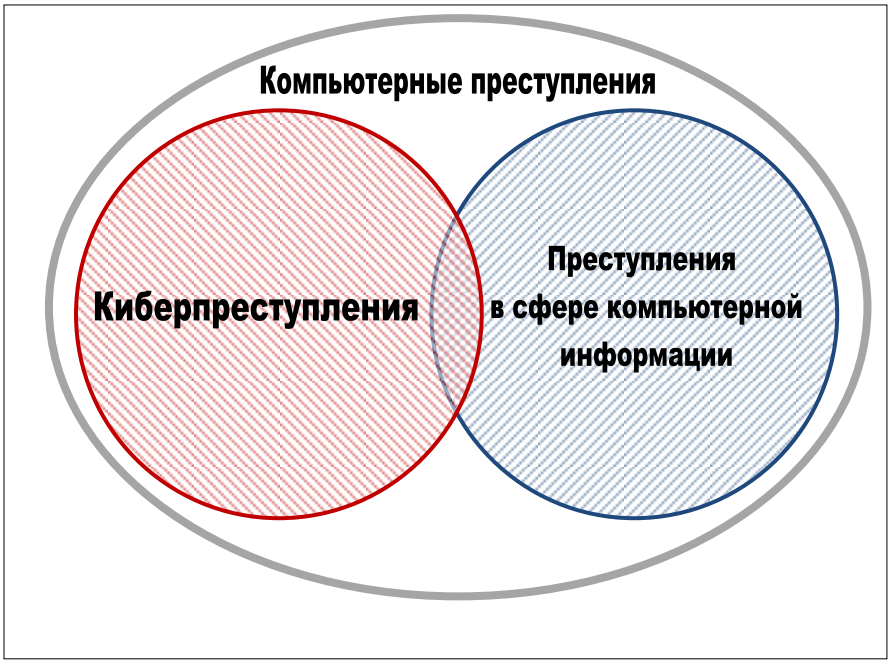

Рисунок 1. - Разграничение понятий «компьютерные преступления», «киберпреступления» и «преступления в сфере компьютерной информации».

На Рисунке 1 видно, что существуют компьютерные преступления:

- совершаемые без использования киберпространства и не являющиеся преступлениями в сфере компьютерной информации, например, совершаемые с использованием средств компьютерной техники (СМС-мошенничество с использованием смартфонов);

- совершаемые без использования киберпространства, но являющиеся преступлениями в сфере компьютерной информации (нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации);

- совершаемые в киберпространстве и не являющиеся преступлениями в сфере компьютерной информации (вымогательство в социальной сети);

- совершаемые в киберпространстве и также являющиеся преступлениями в сфере компьютерной информации (незаконное получение сведений, составляющих коммерческую тайну).

ПРИЛОЖЕНИЕ №2

ОПРОСНЫЙ ЛИСТ

Кафедра уголовного права Российской академии правосудия проводит исследование по вопросу о противодействии экономическим преступлениям, совершенным в киберпространстве. В этой связи просим Вас оказать содействие в проведении исследования и ответить на следующие вопросы (обведите кружком нужный ответ(ы).

Благодарим Вас за помощь!

1. По Вашему мнению, может ли киберпространство являться местом совершения экономических преступлений (преступлений против собственности и преступлений в сфере экономической деятельности)?

a. Да.

b. Нет.

c. Затрудняюсь ответить;

d. Иное (указать, что именно)_______.

2. По Вашему мнению, каковы основные причины и условия существования экономической киберпреступности? (возможно несколько вариантов ответа)

a. Анонимность пользователей киберпространства.

b. Трансграничность киберпространства.

c. Техническое несовершенство киберпространства.

d. Возможность получения сверхприбыли при минимальных затратах в киберпространстве.

e. Отсутствие единых и четких правил поведения в киберпространстве.

f. Наличие субкультуры хакеров.

g. Бездействие правоохранительных органов.

h. Несовершенство уголовного и информационного законодательства.

i. Иное (указать, что именно) _____.

3. По вашему мнению, является ли хищение чужого имущества, совершённое путём ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей (путём ввода вируса в банковскую платёжную систему либо путём перенаправления платежа), составом мошенничества?

a. Да, является составом мошенничества.

b. Нет, данный состав не является мошенничеством, поскольку совершается без обмана и злоупотребления доверием, и является новой, самостоятельной формой хищения.

c. Затрудняюсь ответить.

d. Иное (указать, что именно) _____.

4. По вашему мнению, возможно ли совершение хищения путём обмана или злоупотребления доверием (классическое мошенничество – ст. 159 УК РФ) в киберпространстве?

a. Да, возможно.

b. Нет, хищение в киберпространстве можно совершить **только** путём ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей.

c. Затрудняюсь ответить.

d. Иное (указать, что именно) _____.

5. По Вашему мнению, может ли криптовалюта («Биткойн», Интернет-валюта) являться предметом хищения?

a. Да.

b. Нет.

c. Затрудняюсь ответить.

6. По Вашему мнению, может ли угроза уничтожением, блокированием либо модификацией компьютерной информации (угроза уничтожения коммерческого сайта либо блокирования платёжной системы Сбербанка, угроза DdoS атаки) рассматриваться как способ совершения вымогательства (ст. 163 УК РФ)?

a. Да.

b. Нет.

c. Затрудняюсь ответить.

6.1 . Если да, то каким образом следует отразить это обстоятельство в УК РФ?

a. Выделить в качестве квалифицирующего признака.

b. Выделить в качестве самостоятельного состава.

d. Иное (указать, что именно) _____.

7. По вашему мнению, можно ли в киберпространстве причинить имущественный ущерб путём обмана или злоупотребления доверием (ст. 165 УК РФ)?

a. Да, возможно.

b. Нет, причинение имущественного ущерба в киберпространстве можно совершить только путём ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей.

c. Затрудняюсь ответить.

7.1. Если да, то каким образом следует отразить это обстоятельство в УК РФ?

a. Выделить в качестве квалифицирующего признака.

b. Выделить в качестве самостоятельного состава.

c. Иное (указать, что именно) _____.

8. По вашему мнению, как следует квалифицировать внесение заведомо недостоверных сведений путём ввода или модификации компьютерной

информации через киберпространство в Реестр владельцев ценных бумаг, в систему депозитарного учета?

a. Как фальсификацию Реестра владельцев ценных бумаг или системы депозитарного учёта путём неправомерного доступа (ч.2 ст. 170.1 УК РФ).

b. Как неправомерный доступ к компьютерной информации (ст. 272 УК РФ).

c. Следует квалифицировать по совокупности ч. 2 ст. 170.1 и ст. 272 УК РФ.

d. Иное (указать, что именно) _____.

9. По вашему мнению, как следует квалифицировать осуществление предпринимательской деятельности в киберпространстве (Интернет-торговля, оказание услуг связи, хранения или передачи данных) без регистрации и/или необходимой лицензии, причинившей крупный ущерб?

a. Как незаконное предпринимательство, причинившее крупный ущерб (ч.1 ст. 171 УК РФ).

b. Как неправомерный доступ к компьютерной информации, причинивший крупный ущерб (ч.2 ст. 272 УК РФ).

c. По совокупности ч. 1 ст. 171 УК РФ и ч. 2 ст. 272 УК РФ.

d. Иное (указать, что именно) _____.

10. По вашему мнению, как следует квалифицировать придание правомерного вида безналичным или электронным деньгам либо криптовалюте, приобретённым преступным путём?

a. Как легализацию (отмывание) денежных средств либо иного имущества (ст. 174 УК РФ).

b. Как неправомерный доступ к компьютерной информации, причинивший крупный ущерб (ч.2 ст. 272 УК РФ).

b. По совокупности статей 174 и 272 УК РФ.

c. Иное (указать, что именно) _____.

11. По Вашему мнению, может ли угроза уничтожением, блокированием либо модификацией компьютерной информации (угроза уничтожения коммерческого сайта либо блокирования платёжной системы

Сбербанка, угроза DdoS атаки) рассматриваться как способ принуждения к совершению сделки или к отказу от ее совершения (ст. 179 УК РФ)?

a. Да.

b. Нет.

c. Затрудняюсь ответить.

d. Иное (указать, что именно) _____.

11.1. Если да, то каким образом следует отразить это обстоятельство в УК РФ?

a. Выделить в качестве квалифицирующего признака.

b. Выделить в качестве самостоятельного состава.

c. Иное (указать, что именно) _____.

12. По вашему мнению, как следует квалифицировать использование в киберпространстве чужого товарного знака, причинившее крупный ущерб его правообладателю?

a. Как незаконное использование товарного знака, причинившее крупный ущерб (ч. 1 ст. 180 УК РФ).

b. Как неправомерный доступ к компьютерной информации, причинивший крупный ущерб (ч.2 ст. 272 УК РФ).

c. По совокупности ч. 1 ст. 180 УК РФ и ч. 2 ст. 272 УК РФ.

d. Иное (указать, что именно) _____.

13. По вашему мнению, как следует квалифицировать неправомерный доступ через киберпространство к компьютерному файлу, содержащему коммерческую, налоговую или банковскую тайну?

a. Как незаконное получение сведений, составляющих коммерческую, налоговую или банковскую тайну (ч.1 ст. 183 УК РФ).

b. Как неправомерный доступ к компьютерной информации (ст. 272 УК РФ).

c. По совокупности ч. 1 ст. 183 и ст. 272 УК РФ.

d. Иное (указать, что именно) _____.

14. По Вашему мнению, следует ли признавать использование средств компьютерной техники (специальных устройств либо компьютерных программ) для совершения преступления обстоятельством, повышающим общественную опасность?

a. Да.

b. Нет.

c. Затрудняюсь ответить.

14.1. Если да, то каким образом следует отразить это обстоятельство в УК РФ?

a. Включить в перечень обстоятельств, отягчающих наказание.

b. Выделить в качестве квалифицирующего признака для всех преступлений, совершение которых возможно с использованием средств компьютерной техники.

c. Выделить все преступления, совершаемые с использованием средств компьютерной техники, в самостоятельные составы.

d. Иное (указать, что именно) _____.

15. По Вашему мнению, какие из способов противодействия экономической киберпреступности будут наиболее эффективны? (возможно несколько вариантов ответа)

a. Совершенствование отечественного уголовного и информационного законодательства.

b. Принятие международных конвенций и соглашений.

c. Техническое совершенствование самого киберпространства.

d. Обязательное предоставление всеми пользователями киберпространства реальных данных об имени, фамилии и возрасте.

e. Введение обязательного использования антивирусных программ для всех пользователей киберпространства.

f. Массовое информирование граждан об угрозах в киберпространстве.

g. Иное (указать, что именно) _____.

Благодарим Вас за помощь!

ПРИЛОЖЕНИЕ №3

ТАБЛИЦА РАБОТЫ С СУДЕБНЫМИ ДОКУМЕНТАМИ

№	Наименование документа, наименование суда, дата, номер дела	Статья УК РФ	Пол	Наличие судимости	Семейное положение	Место жительства	Образование	Имеет ли постоянное место работы
1.	Приговор Невельского городского суда Сахалинской области от 14.10.2014 по делу N 1-95/2014	159	М	ДА	Н/А	г.Невельск	Н/А	Н/А
2.	Приговор Ванинского районного суда Хабаровского края от 07.11.2014 по делу N 1-194/14	159	М	НЕТ	Н/А	п. Ванино	Высшее	Ведущий инженер-программист
3.	Приговор Кировского районного суда города Хабаровска от 07.09.2012 по делу N 1-58/2012.	159	МЖ ММЖ ММ	Н/А	Н/А	г.Хабаровск	Н/А	Н/А
4.	Приговор Центрального районного суда города Комсомольск-на-Амуре от 21.05.2012 по делу N 1-625	159	М	НЕТ	Холост	г.Комсо-мольск-на-Амуре	Неполное среднее	Безработный
5.	Приговор Якутского городского суда Республики Саха (Якутия) от 24.11.2011 по делу N 1-1598-11	159	М	НЕТ	Н/А	г.Якутск	Н/А	Н/А
6.	Приговор Фрунзенского районного суда города Владивостока от 05.04.2011 по делу N 1-96/2011	159	ММ	Н/А	Н/А	г.Владивосток	Н/А	Н/А
7.	Приговор Димитровградского городского суда Ульяновской области от 19.12.2014 по делу N 1-433/2014	159	М	НЕТ	Н/А	г.Димитров-град	Среднее специальное	Н/А
8.	Приговор Ульяновского районного суда Ульяновской области от 27.08.2014 по делу N 1-2079/14	159	Ж	НЕТ	Н/А	с.Большое Нагаткино	Н/А	Н/А
9.	Приговор Медведевского районного суда Республики Марий Эл от 10.07.2014 по делу N 1-2-27/2014	159	М	НЕТ	Н/А	п. Оршанка	Н/А	Н/А
10.	Приговор Советского районного суда города Казани от 27.06.2014 N 1-393/14.	159	М	ДА	Н/А	г.Казань	Н/А	Н/А
11.	Приговор Медведевского районного суда Республики Марий Эл от 13.01.2014 по делу N 1-16/2014(1-229/2013)	159	М	ДА	Н/А	пос. Медведево	Н/А	Н/А
12.	Приговор Благовещенского районного суда Республики Башкортостан от 22.10.2013 по делу N 1-104/2013 ст.159	159	М	НЕТ	Холост	г.Благо-вещенск	Высшее	Безработный
13.	Приговор Ленинского районного суда города Нижний Новгород от 20.08.2013 по делу N 1-246/2013	159	М	ДА	Холост	г.Н.Новгород	Неоконченное высшее	Работает
14.	Приговор Ленинского районного суда города Пензы от 13.08.2012 по делу N 1-131/12	159	М	Н/А	Н/А	г.Пенза	Н/А	Н/А
15.	Приговор Автозаводского районного суда города Тольятти от 03.07.2012	159	М	НЕТ	Н/А	г.Тольятти	Н/А	Н/А
16.	Приговор Фрунзенского районного суда города Саратова от 29.02.2012	159	М	НЕТ	холост	г.Саратов	Среднее специальное образование	Работает
17.	Приговор Печорского городского суда Республики Коми от 06.06.2014 по делу N 1-194/2014 ст.159 ч. 2 УК РФ.	159	М	НЕТ	Н/А	г.Печора	Н/А	Н/А
18.	Приговор Вологодского городского суда Вологодской области от 02.09.2013 по делу N 1-471/2013 ст.159 ч. 2 УК РФ.	159	М	ДА	Н/А	г.Вологда	Н/А	Н/А
19.	Приговор Череповецкого городского суда Вологодской области от 21.01.2013 по делу N 1-98/2013(1-1375/2012)	159	М	ДА	Н/А	г.Череповец	Н/А	Н/А
20.	Приговор Московского районного суда города Санкт-Петербурга от 22.08.2011 по делу N 1-472/2011	159	М	НЕТ	Н/А	г.Санкт-Петербург	Н/А	Н/А
21.	Приговор Изобильненского районного суда Ставропольского края от 21.05.2013 по делу N 1-156/2013	159	М	НЕТ	Н/А	г.Изобильный	Н/А	Н/А
22.	Приговор Кисловодского городского суда Ставропольского края от 09.11.2012 по делу N 1-397/12	159	М	Нет	Н/А	г.Кисловодск	Н/А	Н/А

23.	Приговор Кировского районного суда города Омска от 02.12.2014 по делу N 1-759/2014	159	М	НЕТ	Холост	г.Киров	Среднее специальное	Н/А
24.	Приговор Ленинского районного суда города Новосибирска от 28.05.2014 по делу N 1-403/2014	159	М	НЕТ	Холост	г.Новосибирск	Н/А	Работает
25.	Приговор Ленинского районного суда города Барнаула от 26.05.2014 по делу N 1-235/2014	159	М	НЕТ	Н/А	г.Барнаул	Н/А	Н/А
26.	Приговор Советского районного суда города Красноярска от 13.11.2012	159	М	НЕТ	Н/А	г.Красноярск	Н/А	Н/А
27.	Приговор Ленинского районного суда города Нижнего Тагила от 16.01.2014 по делу N 1-93/2014(1-573/2013)	159	М	Н/А	Н/А	г.Нижний Тагил	Н/А	Н/А
28.	Приговор Елецкого районного суда Липецкой области от 15.08.2014 по делу N 1-77/2014.	159	М	НЕТ	Холост	Г.Липецк	Среднее	Работает
29.	Приговор Железнодорожного городского суда Московской области от 21.05.2014 по делу N 1-142/14	159	М	Н/А	Н/А	г.Железнодорожный	Н/А	Н/А
30.	Приговор Октябрьского районного суда города Тамбова от 14.02.2014 по делу N 1-85/14	159	М	НЕТ	Холост	г.Тамбов	Среднее	Безработный
31.	Приговор Орехово-Зуевского городского суда Московской области от 06.09.2013 по делу N 1-500/2013	159	М	НЕТ	Женат	г.Орехово-Зуево	Высшее	Безработный
32.	Приговор Гусь-Хрустального городского суда Владимирской области от 23.05.2013 N 1-40/2013	159	М	НЕТ	Холост	г.Гусь-Хрустальный	Среднее специальное	Безработный
33.	Приговор Ленинского районного суда города Костромы от 10.04.2012 по делу N 1-58/2012	159	М	НЕТ	Н/А	г.Кострома	Н/А	Н/А
34.	Приговор Пушкинского городского суда Московской области от 27.12.2010 по делу N 1-524/10	159	М М	НЕТ НЕТ	Холост Холост	г.Пушкино	Среднее специальное Неоконч.высш.	Безработный Работает
35.	Приговор Ленинского районного суда города Владимира от 15.10.2010 по делу N 1-337/2010	159	М М	НЕТ НЕТ	Н/А	г.Владимир	Н/А	Н/А
36.	Приговор Волжского городского суда Волгоградской области от 23.09.2014 по делу N 1-941/2014	159	М М	Н/А	Н/А	г.Волжский	Н/А	Н/А
37.	Приговор Темрюкского районного суда Краснодарского края от 08.04.2014 по делу N 1-128/2014	159	М	НЕТ	Женат	г.Темрюк	Среднее	Н/А
38.	Приговор Октябрьского районного суда города Краснодара от 27.06.2013 по делу N 1-256/2013	159	Ж	НЕТ	Н/А	г.Краснодар	Н/А	Н/А
39.	Приговор Центрального районного суда города Волгограда от 22.06.2011 по делу N 1-199/2011	159	М	НЕТ	Н/А	г.Волгоград	Н/А	Н/А
40.	Апелляционное определение Московского городского суда от 06.05.2013 по уголовному делу №10-2076	159.6	М	Н/А	Н/А	г.Москва	Н/А	Н/А
41.	Апелляционное определение Московского городского суда от 23.09.2013 по уголовному делу №10-8391	159.6	М	Н/А	Н/А	г.Москва	Н/А	Н/А
42.	Приговор Железнодорожного районного суда города Красноярска от 24.06.2014 по делу N 1-12/2014(1-190/2013;)	159.6	М	Н/А	Н/А	г.Красноярск	Н/А	Н/А
43.	Приговор Пресненского районного суда города Москвы от 29.04.2014 по делу N 1-43/2014 ст. 30 ч. 3, ст. 159.6 ч. 4; ст. 159.6 ч. 4 УК РФ.	159.6	М М М	Нет Нет Нет	Н/А	г.Москва	Высшее Высшее Высшее	Работает Безработный Работает
44.	Приговор Хамовнического районного суда города Москвы от 01.08.2013 по делу N 1-100/2013.	159.6	М Ж	Да Да	Холост Замужем	г.Москва	Высшее Среднее техническое	Безработный Безработный
45.	Приговор Кировского районного суда города Курска от 15.05.2014 N 1-64/9-2014г.	159.6	М	Нет	Н/А	г.Курск	Н/А	Н/А
46.	Приговор Савеловского районного суда города Москвы от 03.06.2013 N 1-226/13	159.6	М М	Н/А	Н/А	г.Москва	Высшее Высшее	Н/А
47.	Приговор Димитровградского городского суда Ульяновской области от 19.12.2014 по делу N 1-433/2014	159.6	М	Нет	Н/А	г.Димитров-град	Н/А	Н/А
48.	Приговор Октябрьского районного суда города Самары от 10.06.2014 N 1-141/14	159.6	М	Нет	Жената	г.Самара	Среднее специальное	Работает

49.	Приговор Советского районного суда города Уфы от 05.05.2014 по делу N 1-209/2014	159.6	М	Нет	Н/А	г.Уфа	Н/А	Безработный
50.	Приговор Самарского районного суда города Самары от 18.04.2014 по делу N 1-34/2014	159.6	М	Н/А	Н/А	г.Самара	Н/А	Н/А
51.	Приговор Комсомольского районного суда города Тольятти от 18.03.2014 по делу N 1-125/2014	159.6	М	Н/А	Н/А	г.Тольятти	Н/А	Н/А
52.	Приговор Красноглинского районного суда города Самары от 06.03.2014 по делу N 1-76/2014	159.6	М	Нет	холост	г.Самара	Неоконченное высшее	Работает
53.	Приговор Промышленного районного суда города Самары от 21.02.2014 по делу N 1-122/2014	159.6	М	Н/А	Н/А	г.Самара	Н/А	Н/А
54.	Приговор Ленинского районного суда города Самары от 12.04.2013 по делу N 1-73/2013 ст.159.6 ч. 3 УК РФ.	159.6	М	Нет	Холост	г.Самара	Среднее	Безработный
55.	Приговор Зеленодольского городского суда Республики Татарстан от 04.06.2013 по делу N 1-218/2013	159.6	М	нет	Н/А	г.Зеленодольск	Н/А	Н/А
56.	Приговор Благодарненского районного суда Ставропольского края от 15.12.2014 по делу N 1-183/14	159.6	М	Нет	Н/А	г.Благодарный	Н/А	Безработный
57.	Приговор Андроповского районного суда Ставропольского края от 31.10.2014 по делу N 1-97/14	159.6	М	нет	Холост	с. Курсавка	Неоконченное высшее	Работает
58.	Приговор Апанасенковского районного суда Ставропольского края от 28.08.2014 по делу N 1-78/2014	159.6	М	Н/А	Н/А	с.Дивное	Н/А	Н/А
59.	Приговор Апанасенковского районного суда Ставропольского края от 11.08.2014 по делу N 1-72/2014	159.6	М	Нет	Женат	с. Дивное	Среднее специальное	Безработный
60.	Приговор Благодарненского районного суда Ставропольского края от 28.07.2014 по делу N 1-108/2014	159.6	М	Нет	Н/А	г.Ставрополь	Н/А	Н/А
61.	Приговор Кизилюртовского городского суда Республики Дагестан от 11.06.2014 по делу N 1-49/2014	159.6	М М	ДА НЕТ	Холост Женат	г.Кизилюрт	Неполное среднее; Среднее	Работает Работает
62.	Приговор Братского городского суда Иркутской области от 12.11.2014 по делу N 1-549/2014	159.6	М	Да	Холост	г.Братск	Н/А	Безработный
63.	Приговор Сургутского городского суда Ханты-Мансийского автономного округа - Югры от 16.12.2014 по делу N 1-1286/2014	159.6	М	Н/А	Н/А	г.Сургут	Н/А	Н/А
64.	Приговор Златоустовского городского суда Челябинской области от 23.06.2014 по делу N 1-260/2014 ст.159.6 ч. 2 УК РФ.	159.6	М	Да	Женат	г.Златоуст	Среднее специальное	Работает
65.	Приговор Талицкого районного суда Свердловской области от 19.06.2014 по делу N 1-92/2014	159.6	М	Н/А	Н/А	г.Талица	Н/А	Н/А
66.	Приговор Талицкого районного суда Свердловской области от 18.02.2014 по делу N 1-30/2014	159.6	М	Н/А	Н/А	г.Талица	Н/А	Н/А
67.	Приговор Зареченского районного суда города Тулы от 16.12.2014 по делу N 1-125/2014	159.6	М	Да	Н/А	г.Тула	Н/А	Н/А
68.	Приговор Хорошевского районного суда города Москвы от 28.11.2014 по делу N 1-585/14	159.6	М	Нет	жената	г.Москва	Высшее	Работает
69.	Приговор Железногорского городского суда Курской области от 21.10.2014 по делу N 1-243/2014	159.6	М	Да	холост	г.Железногорск	Среднее специальное	Безработный
70.	Приговор Конаковского городского суда Тверской области от 24.07.2014 по делу N 1-171/2014	159.6	М	Нет	Холост	г.Конаково	Среднее специальное	Безработный
71.	Приговор Кировского районного суда города Курска от 15.05.2014	159.6	М	Н/А	Н/А	г.Курск	Н/А	Н/А
72.	Приговор Хамовнического районного суда города Москвы от 15.05.2014 по делу N 1-49/2014	159.6	М	Нет	Н/А	г.Москва	Н/А	Работает
73.	Приговор Пресненского районного суда города Москвы от 16.05.2013 по делу N 1-176/2013	159.6	М М	Да Да	Холост Холост	г.Москва	Среднее Среднее специальное	Безработный Безработный
74.	Приговор Подольского городского суда Московской области от 23.04.2013 по	159.6	Ж	Н/А	Н/А	г.Подольск	Н/А	Н/А

	делу N 1-232/13(78648)							
75.	Приговор Индустриального районного суда города Хабаровска от 18.07.2014 по делу N 1-726/2014	160	М	Да	Н/А	г.Хабаровск	Н/А	Н/А
76.	Приговор Октябрьского районного суда города Пензы от 14.06.2012 по делу N 1-166/2012	160	Ж	Нет	Н/А	г.Пенза	Н/А	Н/А
77.	Приговор Выборгского гарнизонного военного суда от 19.02.2010 по делу N 14/10	160	М	Н/А	Н/А	г.Выборг	Н/А	Н/А
78.	Приговор Курского районного суда Ставропольского края от 08.08.2013 по делу N 1-132/2013	160	Ж	Нет	Замужем	ст. Курская	Неоконченное высшее	Безработная
79.	Приговор Мончегорского городского суда Мурманской области от 09.07.2010 по делу N 118-2010	163	М	Нет	Холост	г.Мончегорск	Среднее	Работает
80.	Приговор Советского районного суда города Челябинска от 24.12.2013 по делу N 1-588/2013	163	Ж	Нет	Не замужем	г.Челябинск	Среднее специальное	Работает
81.	Приговор Советского районного суда города Брянска от 14.10.2014 по делу N 1-162(14)	163	М М Ж	Н/А	Н/А	г.Брянск	Н/А	Н/А
82.	Приговор Хорошевского районного суда города Москвы от 01.12.2014 по делу N 1-587/2014г.	163	М	Нет	Холост	г.Москва	Среднее	Безработный
83.	Приговор Октябрьского районного суда Тамбова города от 29.05.2009 по уголовному делу №1-324/09	163	М	Н/А	Н/А	г.Тамбов	Н/А	Н/А
84.	Приговор Мичуринского городского суда Тамбовской области по уголовному делу № 1-563/2004	165	М	Н/А	Н/А	г.Тамбов	Н/А	Н/А
85.	Приговор Новотроицкого городского суда Оренбургской области от 02.02.2012 по делу N 1-09/2012	165	М	Н/А	Н/А	г.Новотроицк	Н/А	Н/А
86.	Приговор Бузулукского районного суда Оренбургской области от 03.12.2010 N 1(1)-208/2010	165	М	Нет	Н/А	г.Бузулук	Н/А	Н/А
87.	Приговор Воткинского районного суда Удмуртской Республики от 05.10.2010 N 1-368(03/1423)	165	М	Нет	Холост	г.Воткинск	Н/А	Н/А
88.	Приговор Волгодонского районного суда Ростовской области от 28.01.2010	165	Ж	Нет	замужем	г.Волгодонск	Высшее	Работает
89.	Приговор Куйбышевского районного суда города Омска от 05.02.2014 по делу N 1-53/2014(1-476/2013)	171.2	М	Н/А	Н/А	г.Омск	Н/А	Н/А
90.	Приговор Приволжского районного суда города Казани от 28.02.2014 по делу N 1-13 2013;1-86 2012	180	М	Н/А	Н/А	г.Казань	Н/А	Н/А
91.	Приговор Первореченского районного суда города Владивостока от 28.04.2011 по делу N 1-240/11	183	М	Нет	Холост	г.Владивосток	Среднее	Работает
92.	Постановление Московского городского суда от 05.12.2013 N 4у/2-9352;	183	М	Н/А	Н/А	г.Москва	Н/А	Н/А
93.	Приговор Автозаводского районного суда г.Тольятти по уголовному делу № 1-828/2004	183	М	Н/А	Н/А	г.Тольятти	Н/А	Н/А
94.	Приговор Сарапульского городского суда Удмуртской Республики от 05.08.2014 по делу N 1-139/14	183	М	Н/А	Н/А	г.Сарапул	Н/А	Н/А
95.	Приговор Юрьянского районного суда Кировской области от 21.04.2011 по делу N 1-52(21333)	183	М	Да	Н/А	п. Юрья	Н/А	Н/А
96.	Приговор Новгородского районного суда Новгородской области от 22.03.2011 по делу N 1-13/11	183	М	Н/А	Н/А	г.Великий Новгород	Н/А	Н/А
97.	Приговор Новозыбковского городского суда Брянской области от 18.07.2011	183	М	Нет	Н/А	г.Новозыбков	Н/А	Н/А
98.	Приговор Гусь-Хрустального городского суда Владимирской области по делу N 1-90/11	183	М	Нет	Холост	г.Гусь-Хрустальный	Среднее специальное	Безработный
99.	Приговор Преображенского районного суда города Москвы от 10.02.2011	183	Ж	Нет	Замужем	г.Москва	Высшее	Работает
100.	Приговор Калужского районного суда Калужской области от 17.05.2010	183	М	Нет	Холост	г.Калуга	Неоконченное высшее	Безработный