На правах рукописи

КОМАРОВ Антон Анатольевич

Криминологические аспекты мошенничества в глобальной сети Интернет

12.00.08 – уголовное право и криминология;
уголовно-исполнительное право

Автореферат
диссертации на соискание ученой степени
кандидата юридических наук

Саратов – 2011

Диссертация выполнена в Государственном образовательном учреждении высшего профессионального образования «Пятигорский государственный технологический университет»

Научный руководитель	кандидат юридических наук, доцент **Данелян Рита Суреновна**
Официальные оппоненты:	доктор юридических наук, профессор, Заслуженный юрист РФ **Гриб Владимир Григорьевич**
	кандидат юридических наук, доцент **Бытко Сергей Юрьевич**
Ведущая организация	ФГАОУ ВПО «Казанский (Приволжский) федеральный университет»(юридический факультет).

Защита состоится « 20 » апреля 2011 г. в 14:00 часов на заседании диссертационного совета Д-212.239.01 при Государственном образовательном учреждении высшего профессионального образования «Саратовская государственная академия права» по адресу: 410056, г. Саратов, ул. Чернышевского, 104. ауд. 102.

С диссертацией можно ознакомиться в библиотеке Государственного образовательного учреждения высшего профессионального образования «Саратовская государственная академия права».

Автореферат разослан «___» _____ 2011 года.

Ученый секретарь
диссертационного совета
кандидат юридических наук, доцент **Е.В. Кобзева**

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы исследования. Сегодня уже никого не удивляет факт быстрой трансформации преступности на основе телекоммуникационных и компьютерных технологий. Об этом свидетельствует как официальная статистика правоохранительных органов, так и многочисленные исследования ученых. Если в 1999 году было зарегистрировано лишь 148 случаев мошенничества (ст. 159 УК РФ), совершенного с использованием компьютерных и телекоммуникационных технологий, то спустя десять лет в суд было передано 2799 уголовных дел. В 2010 году наблюдался значительный прирост мошенничества связанного с использованием глобальной сети Интернет и средств мобильной связи. За 2010 года в связи с данными преступлениями по ст. 159 УК РФ («Мошенничество») было возбуждено 6762 уголовных дел, направлено в суд – 3751.[1] Из всей совокупности преступлений, совершенных с использованием компьютерных технологий (зарегистрировано в 2010 году 11636 преступлений), доля мошенничества составляет – 58 %.[2] Вместе с тем, если сравнить официальные статистические данные прошлых лет, то подобные деяния в структуре компьютерной преступности в 2000 году составляли – 17%; в 2005 – 29%.[3] Увеличение количества мошенничеств, совершаемых посредством компьютерных сетей, свидетельствует о двух долгосрочных социально-негативных тенденциях: преобладании корыстной мотивации при совершении компьютерных преступлений и активном проникновении в Интернет традиционных форм мошенничества, в частности потребительского мошенничества в сфере электронной коммерции. Об этом свидетельствует и практика проведения специализированных научно-практических конференций.

9 декабря 2010 года состоялась первая всероссийская специализированная конференция «Борьба с мошенничеством в сфере высоких технологий. Профилактика и противодействие», организаторами которой выступили Комитет Торгово-промышленной палаты Российской Федерации по безопасности предпринимательской деятельности и негосударственное образовательное учреждение «Академия информационных систем» при поддержке Министерства внутренних дел России и Министерства связи и массовых коммуникаций Российской Федерации. В ходе проведения мероприятия было отмечено, что длительное отсутст-

---

[1] См.: итоги пресс-конференции: «Деятельность ГУВД по Московской области по предотвращению мошеннических действий с использованием сети «Интернет» и средств мобильной связи» / Московский Комсомолец [Электронный ресурс]. – 29.10.2010. – URL: http://www.mk.ru/press-center/press/2010/12/28/213.html (дата обращения: 27.01.2011).

[2] См.: состояние преступности (январь-декабрь 2010 г.) / пресс-центр МВД РФ [Электронный ресурс]. – 04.02.2011. – URL: http://www.mvd.ru/presscenter/statistics/ (дата обращения: 13.02.2011).

[3] На основе: официальных отчетов о состоянии преступности пресс-центра МВД [Электронный ресурс]. – URL: http://www.mvd.ru/presscenter/statistics/; и Сводного отчета о преступлениях, совершенных в сфере телекоммуникаций и компьютерной информации в Российской Федерации за период с 1 января 1997 по 1 января 2005 года.

вие эффективных стратегий противодействия распространению мошенничества в глобальной сети Интернет является ключевой проблемой. Особый акцент был сделан на необходимость дополнительных научных исследований в области предупреждения подобных форм мошенничества.[4]

Практика проведения подобных научно-практических мероприятий показывает, что в сложившихся обстоятельствах правоприменитель испытывает определенные трудности, связанные с малоизученностью, стремительным распространением и дифференциацией такого явления, как компьютерная преступность.

Во многом такая ситуация сложилась благодаря тому, что человечество, совершая все новые и новые открытия, до сих пор не научилось определять и ограничивать сферу их применения. Более того, попытки такого ограничения зачастую неэффективны, а порой и невозможны, ибо большинство технологий рассчитано на массовое употребление вне зависимости от целей использования. Таким образом, преступник, являясь частью социума, обогащает собственный арсенал.

Концептуально наше исследование построено на гипотезе о том, что качественные изменения преступности, произошедшие в современном обществе, обусловлены не только классическими социально-экономическими условиями, но и стремительным вовлечением Российской Федерации в процесс информатизации абсолютно всех сфер деятельности человека. Криминологические аспекты, вынесенные в заглавие работы, отражаются в способе изложения материала «от констатации связи между социальными процессами, явлениями и преступностью к выявлению механизма этой связи, а от него – к прогнозированию преступности и планированию мер борьбы с ней».[5]

Анализ всех протекающих в современном информационном обществе процессов позволяет сделать вывод, что мошенничество так же трансформируется, приобретая специфические черты. В результате чего возникает задача по разработке новых и совершенствованию существующих мер противодействия нетрадиционным формам преступности с учетом ее информационно-трансграничного характера.

Эти обстоятельства послужили причиной выбора темы диссертационного исследования, поскольку свидетельствуют об особой актуальности затрагиваемой проблемы.

Степень разработанности темы исследования. Негативные последствия информатизации общества давно рассматриваются на общефилософском уровне, в том числе и в теории права. Исследования, в свое время проведенные А.Б.

---

[4] См.: Новости: Первая Всероссийская конференция «Борьба с мошенничеством в сфере высоких технологий. Профилактика и противодействие» / AntiFraud – Russia [сайт]. [Электронный ресурс]. – декабрь 2010. – URL: http://antifraudrussia.ru/ (дата обращения: 07.01.2011).

[5] Сахаров А.Б. Общетеоретические проблемы криминологии. Цит. по: Хохряков Г.Ф. Криминология. – М.: Юристъ, 2002. – С. 58.

Венгеровым, В.Н. Монаховым, И.Л. Бачило, В.Б. Наумовым, подготовили почву для выделения в отдельное научное направление информационного права. Преступления в сфере высоких технологий стали предметом интереса практиков: появились многочисленные работы, освещающие криминалистические особенности компьютерной преступности. Весомый вклад в разработку рекомендаций следователям по производству следственных действий при расследовании компьютерных преступлений внесли В.Б. Вехов, А.Г. Волеводз, В.А. Голубев, В.В. Крылов, В.А Мещеряков, и другие ученые. Со временем стали появляться труды уголовно-правового толка. Этим вопросам посвящены исследования П.Б. Гудкова, Л.М. Исаевой, Д.С. Пушкина, Г.В. Семенова, Т.Л. Тропиной, А.Г. Серго, С.Д. Бражника, С.И. Ушакова, С.Г. Спириной и иных ученых.

Глубоких всесторонних исследований, посвященных компьютерной преступности как явлению – следствию социальной трансформации общества, пока единицы. При этом нужно понимать, что компьютерная преступность – разносторонний феномен, состоящий из ряда взаимосвязанных явлений. Используя возможности компьютерных систем и сетей, преступники способны причинять существенный вред не только защищенной законом компьютерной информации, но и экономическим интересам организаций и физических лиц. Среди хищений, совершенных при помощи компьютерных средств, значительную долю занимает мошенничество: быстрое развитие глобальной коммуникационной сети Интернет позволило «легализоваться» в виртуальной реальности многим традиционным мошенническим схемам.

В исследованиях экономической составляющей компьютерной преступности, в том числе мошенничества в Интернет, следует отметить заслуги зарубежных коллег: У. Зибера (Ulrich Sieber), С. Бреннер (Susan W. Brenner), Л. Шелли (Louise I. Shelley). Р. Смита (Russell G. Smith).

Среди отечественных ученых, уделивших достаточное внимание криминологическим аспектам компьютерной преступности и распространению ее в сети Интернет, следует выделить: В.Е. Козлова «Теория и практика борьбы с компьютерной преступностью» (монография – 2002), Д.А. Зыкова «Виктимологические аспекты предупреждения компьютерного мошенничества» (кандидатская дисс. – 2002), Т.П. Кесарееву «Криминологическая характеристика и проблемы предупреждения преступности в российском сегменте сети Интернет» (кандидатская дисс. – 2002), А.А. Жмыхова «Компьютерная преступность за рубежом и ее предупреждение» (кандидатская дисс. – 2003), А.Л. Осипенко «Борьба с преступностью в глобальных компьютерных сетях: Международный опыт» (монография – 2004), Т.М. Лопатину «Криминологические и уголовно-правовые основы противодействия компьютерной преступности» (докторская дисс. – 2006), Д.В. Добровольского «Актуальные проблемы борьбы с компьютерной преступностью» (кандидатская дисс. – 2006), Р.И. Дремлюгу «Интернет-преступность» (монография – 2008).

В целом, российских криминологических исследований, посвященных ча-

стным вопросам компьютерной преступности, пока недостаточно. Это связано с постоянной дифференциацией и усложнением компьютерной преступности.

Объект и предмет исследования. Объектом исследования выступает мошенничество в глобальной сети Интернет, как специфическое противоправное явление, и особые формы социальной реакции на него, складывающиеся в виде общественных отношений.

Предметом же исследования в данном случае будут выступать: а) внутренние характеристики и элементы указанного явления; б) комплекс внешних социальных процессов и явлений, обуславливающий существование мошенничества в глобальной сети Интернет в современном нам обществе; в) способы и приемы воздействия на эти закономерности с целью сокращения социально-негативных последствий.

Цель и задачи исследования. Целью диссертационного исследования является разработка научно обоснованной криминологической концепции мошенничества в глобальной сети Интернет, и выдвижение на этой основе практических предложений по предупреждению указанного явления, складывающихся в единую систему.

Цель исследования предполагает постановку и необходимость решения **следующих задач**:

1. Определение объекта предупредительного воздействия, для чего требуется:

а) разработать криминологическое понятие мошенничества в глобальной сети Интернет;

б) определить место интернет-мошенничества в общей структуре преступности и в структуре компьютерной преступности;

в) провести классификацию и типологизацию мошенничества в глобальной сети Интернет.

2. Выявление особенностей интернет-мошенничества как объекта криминологического воздействия, для чего становится необходимым:

а) спрогнозировать развитие преступности в целом и преступности в глобальной сети Интернет;

б) выделить конкретные криминологически значимые детерминанты преступного поведения мошенников в Интернет;

в) раскрыть роль личности в реализации преступного умысла и способы ее формирования посредством механизма индивидуального преступного поведения, а также объяснить тесную взаимосвязь личности преступника и жертвы интернет-мошенничества.

3. Выработка рекомендаций по предупреждению мошенничества в глобальной сети Интернет, для чего становится необходимым:

а) проанализировать возможность и варианты адаптации существующих организационно-технических мер воздействия на компьютерную преступность с целью предупреждения мошенничества в глобальной сети Интернет;

б) разработать новые формы противодействия с учетом специфики изучаемого явления.

Методология и методика исследования. Методологическую основу исследования составили положения общенаучного диалектического метода познания социальных явлений. Характер поставленных в исследовании задач обусловил использование сравнительно-правового, системно-структурного и статистического метода.

В целях криминологического прогнозирования были использованы методы моделирования, в том числе моделирования социальных процессов на долгосрочную и краткосрочную перспективу. Во втором случае – при помощи экстраполяции существующих статистических данных.

Методика исследования включает в себя также: социологические измерения изучаемого явления при помощи анкетирования активных пользователей Интернет, жертв мошенничества, сотрудников правоохранительных органов; контент-анализ прессы, который позволяет выявить распространенность криминального образа жизни, пораженности правосознания интернет-пользователей – применительно к сфере изучения личностных особенностей лиц, совершивших преступление, при раскрытии механизма индивидуального преступного поведения и прочих индивидуально-психологических аспектов; анализ информационных ресурсов Интернет, которые позволяют выявить внутренние связи интернет-сообщества и распространяющейся в нем преступности, формы их взаимодействия, отношение к этому явлению пользователей Интернет.

Нормативную основу работы составили положения, закрепленные в международных договорах и конвенциях, в отечественных законах и подзаконных актах, касающихся вопросов правового регулирования глобальной сети Интернет и борьбы с компьютерной преступностью.

Теоретическая основа исследования. При разработке отдельных проблем диссертации автор опирался на теоретические разработки и концепции известных ученых в области уголовного права и криминологии: Б.В. Волженкина, А.И. Долговой, И.И. Карпеца, В.Н. Кудрявцева, Н.Ф. Кузнецовой, В.В. Лунеева, В.А. Номоконова, В.Е. Эминова, Г.Ф. Хохрякова и других ученых, которые позволили систематизировать полученные результаты исследования, прочно увязать их с системой криминологического знания. В области специальных криминологических знаний по вопросам компьютерной преступности теоретической базой выступили исследования Ю.М. Батурина, А.М. Жодзишского, В.А. Номоконова, Т.М. Лопатиной.

Эмпирической базой исследования явились данные, содержащиеся в статистических отчетах о преступлениях, совершенных в сфере телекоммуникаций и компьютерной информации ГИАЦ МВД РФ (по Ф. 615 КН.1.) за период с 1997 по 2010 год; в сводных статистических формах деятельности федеральных судов общей юрисдикции и мировых судей (без военных судов) Судебного департамента при Верховном Суде Российской Федерации за 2006-2010 годы; в

аналитических докладах негосударственных организаций: ЗАО «Лаборатория Касперского» (Kaspersky Security Bulletin за период с 2005 по 2010 год); статистические данные, связанные с развитием Интернет в России: базы данных «RUметрика: Цифры в Интернете» [*http://rumetrika.rambler.ru*], бюллетени «Интернет в России» Фонда «Общественное мнение» за период с 2002 по 2011 год [*http://bd.fom.ru*], базы данных «Средства массовой информации: Интернет – Пресс-выпуски» Всероссийского центра изучения общественного мнения [*http://wciom.ru*]; статистические данные зарубежных стран, в частности, сведения официальных отчетов о преступности в сфере высоких технологий и интернет-преступности таких организаций, как: the Internet Crime Complaint Center (США) – (IC3 Annual Report on Internet Crime за период с 2001 по 2010 год [http://www.ic3.gov]), the National White Collar Crime Center (США) – (NW3C Annual Reports за период 2005 – 2010 годы [http://www.nw3c.org/research]), ежегодных отчетов компании McAfee – North America Criminology Report за период с 2005 – 2009 годы (Канада) [http://www.mcafee.com/]).

В целях обеспечения достоверности результатов исследования лично автором было проведено анкетирование 118 сотрудников правоохранительных органов (оперуполномоченных отделов по борьбе с экономическими преступлениями, отделов «К» управлений бюро специальных технических мероприятий МВД РФ; следователей следственных отделов) во всех регионах Северо-Кавказского федерального округа, а также в Краснодарском крае, Ростовской и Волгоградской областях, г. Москве.

В рамках виктимологического анкетирования граждан – активных пользователей Интернет автором было опрошено 547 человек на территории Ставропольского края.

Эмпирическую базу составили материалы 52 уголовных дел, находившихся в производстве районных судов общей юрисдикции регионов Северо-Кавказского федерального округа и Южного федерального округа, Свердловской, Новгородской областей, г. Москвы и Санкт-Петербурга за период с 2005 по 2010 год, а также материалы опубликованной судебной практики.

Проведены обобщение и анализ газетных и журнальных публикаций, посвященных преступности в сети Интернет за период с 2005 по 2011 год.

Научная новизна исследования состоит в том, что на основе всестороннего изучения объекта автором была выдвинута целостная научно обоснованная криминологическая концепция мошенничества в глобальной сети Интернет, как общественно опасного явления, обусловленного комплексом коренных закономерностей общественного развития, в том числе информатизацией и технологизацией общественных отношений. На основе полученного нового знания была разработана и предложена система мер по его предупреждению, учитывающая специфику изучаемого явления.

Дальнейшая конкретизация личного вклада автора в криминологическую науку нашла отражение **в положениях, выносимых на защиту**:

1. Мошенничество в глобальной сети Интернет как явление – это совокупность преступлений, характеризующихся единством способа совершения преступления (использование технологических и коммуникационных возможностей компьютерных систем, подключенных к глобальной сети Интернет, для совершения обмана человека или «обмана» компьютерной системы), а также корыстной мотивацией преступной деятельности.

2. Под обманом компьютерной системы (автоматизированной системы обработки данных – АСУ) следует понимать получение доступа к процессам автоматической обработки данных одним лицом от имени другого с целью активации алгоритмов действия АСУ, результатом которых являются утрата кем-либо имущества, имущественных прав, причинения имущественного ущерба. Все компьютерные мошенничества построены на принципе обмана компьютерной системы (АСУ).

3. Интернет-мошенничество является частью компьютерной преступности. В ее структуре следует выделять преступления в сфере компьютерной информации (глава 28 УК РФ), которые являются общим конструктом, отражающим единый информационно-компьютерный способ совершения компьютерных преступлений. Вместе с тем, указанные составы могут применяться самостоятельно. В зависимости от способов использования компьютерной информации в противоправных целях следует выделять еще два структурных блока компьютерной преступности: а) преступления, в которых электронная информация является орудием или средством совершения другого преступления; б) преступления, где компьютеры используются для «визуализации» информации. Мошенничество в глобальной сети Интернет одновременно относится ко второй и третьей группе компьютерных преступлений. Интернет является инструментом распространения машинно-обрабатываемой информации; компьютер, подключенный к глобальной сети – средством ее «визуализации» или самостоятельной обработки. Поскольку Интернет является лишь одним из возможных способов доставки (распространения) компьютерной информации всю компьютерную преступность нельзя свети к интернет-преступности. Однако интернет-преступность вне компьютерной преступности не существует, что обусловлено технологическими особенностями – Интернет – глобальная компьютерная сеть. Интернет как средство распространения информации с неизбежностью ведет к распространению мошеннических схем связанных с его использованием. Поскольку манипуляция с информацией является сутью преступного обмана.

4. Интернет объединяет (позволяет совершать) лишь часть мошеннических схем, существующих в действительности. Можно утверждать о наличии двух видов интернет-мошенничества: 1) нетрадиционные компьютерозависимые формы (компьютерное мошенничество) зачастую использующие коммуникационные возможности Интернет, являются «компьютерозависимыми» поскольку само преступление (хищение) не мыслимо без модификации, копирования компьютерной информации; 2) традиционные компьютеронезависимые»

формы мошенничества, использующие возможности Интернет для реализации преступного умысла в целях обогащения.

5. Система мер предупреждения указанного явления складывается из совокупности трех уровней предупреждения – общий, специальный, индивидуальный, каждый из которых предусматривает собственные направления предупреждения и конкретные формы реализации.

6. В области общего предупреждения мошенничества в глобальной сети Интернет основными направлениями являются: совершенствование уголовной политики РФ в сфере компьютерной преступности, создание эффективной системы социально-правового контроля над распространением мошенничества в Интернет, криминологическая экспертиза нормативно-правовых актов посвященных развитию и функционированию Интернет в России, международно-правовое регулирование Интернет.

7. Основными формами реализации общего предупреждения должны стать:

а) разработка и принятие концептуального закона о развитии российского сегмента Интернет и включение в указанный закон положения о недопустимости использования информационно-коммуникативных технологий в неправомерных целях;

б) принятие федерального закона о негосударственных субъектах предупреждения и системе мер государственной поддержке такой деятельности;

в) устранение разногласий в понимании компьютерного мошенничества путем расширения понятия обмана как способа совершения мошенничества не только в отношении человека, но и автоматизированных компьютерных систем;

г) внесение изменений в гражданское законодательство с целью обособления процедур заключения сделок, совершаемых в электронной форме.

д) принятие мер по совершенствованию правовых основ деятельности электронных платежных систем для выполнения приоритетной задачи –борьбы с анонимностью пользователей и совершаемых ими транзакций.

8. В области специального предупреждения мошенничества в глобальной сети Интернет основными направлениями являются: организационно-техническое предупреждение и виктимологическая профилактика, реализация которых проводится в два этапа: текущий и последующий.

9. В качестве основных форм специального предупреждения должны выступить:

а) разработка и принятие взвешенную и реализуемую программу государства по внедрению электронной цифровой подписи в гражданский оборот;

б) введение идентификации личности пользователя в случае предоставления ему доступа в Интернет из мест коллективного пользования;

в) присвоение каждому пользователю Интернет электронного сертификата (электронного паспорта), содержащего персональную информацию о своем владельце;

г) создание правовых условий (запрета) в сфере регулирования деятельности интернет-провайдеров, в которых заведение анонимного ящика электронной почты без заключения письменного договора станет невозможно;

д) учреждение всеобъемлющего русскоязычного информационного ресурса, опирающегося на государственную поддержку и способного одновременно решить несколько научно-практических задач.

Апробация результатов исследования. Основные положения и выводы, содержащиеся в работе, обсуждались на межрегиональной научно-практической конференции «Социально-экономические, правовые, экологические и социокультурные проблемы России» (Пятигорск, март 2009 г.), 2-й Международно-практической конференции «Молодежь и наука: реальность и будущее» (г. Невинномысск, марта 2009 г.), 5-й Международной научно-практической конференции «Глобальный научный потенциал» (г. Тамбов, июнь 2009 г.), VIII Всероссийской научно-практической конференции «Тенденции и противоречия развития российского права на современном этапе» (г. Пенза, декабрь 2009 г.), VI общероссийской научно-практической конференции «Современные вопросы государства, права, юридического образования» (г. Тамбов, декабрь 2009 г.).

Отдельные аспекты применения результатов исследования нашли отражение в актах о внедрении результатов диссертационного исследования в учебный процесс юридических факультетов Института экономики и управления (г. Пятигорск), Института управления, бизнеса и права (г. Пятигорск), Пятигорского государственного технологического университета, практическую деятельность Пятигорского филиала Северо-Кавказского отделения Сберегательного банка России.

Результаты исследования опубликованы в 13 научных статьях общим объемом 4,78 п.л. Из них четыре статьи входят в перечень изданий, рекомендуемых ВАК Министерства образования и науки Российской Федерации.

Теоретическая и практическая значимость исследования заключается в возможности использовать содержащиеся в диссертации выводы и предложения в процессе совершенствования законодательства в целях предупреждения мошенничества в глобальной сети Интернет. Часть выводов общего характера может быть применена и к предупреждению компьютерной преступности в Интернет, в целом. Диссертационное исследование может послужить материалом для дальнейших научных изысканий в области компьютерной преступности.

Отдельные аспекты диссертации могут найти свое воплощение и в учебном процессе, при изучении соответствующих тем в рамках учебных дисциплин: «Криминология», «Правовая защита информации», «Информационное право».

Практическая значимость состоит и в том, что сформулированные предложения и выводы могут быть использованы в процессе совершенствования деятельности правоохранительных органов по профилактике мошенничества в

глобальной сети Интернет.

Структура диссертации и ее объем обусловлены комплексом решаемых задач. Диссертация состоит из введения, трех глав (тринадцати параграфов), содержащих последовательное изложение научного исследования, заключения, списка используемых источников и трех приложений.

ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

Во **введении** обоснована актуальность избранной темы, определены объект, предмет, цели и задачи исследования, указаны применяемые методы, теоретическая и эмпирическая база, раскрыта научная новизна работы, теоретическая и практическая значимость полученных результатов, приведены сведения об их апробации, сформулированы основные положения, выносимые на защиту.

Глава первая – «Мошенничество в глобальной сети Интернет как объект криминологических исследований» состоит из трёх параграфов. В первом параграфе «Понятие мошенничества в глобальной сети Интернет» исследуемое явление отграничивается от смежных при помощи четырех основополагающих признаков: способ совершения преступления, мотивация преступной деятельности, последствий совершенного преступления, орудия совершения преступления. Особое внимание уделено терминологическому многообразию и отсутствию единого подхода к определению понятия в криминологической и уголовно-правовой науке. Исследуя различные точки зрения на трансформацию мошенничества, например возможности выделения отдельной самостоятельной группы имущественных обманов, выходящих за рамки хищения, автор приходит к выводу о необходимости криминологического объединения мошенничества и причинения имущественного ущерба путем обмана злоупотребления доверием. Рассматривается и компьютерное мошенничество как один из возможных видов интернет-мошенничества и его качественный признак – отсутствие добровольности при передаче имущества (имущественных прав), как общепризнанного признака мошенничества. Для устранения противоречий в зарубежном и отечественном понимании феномена компьютерного мошенничества, автор формулирует концепцию «обмана компьютерной системы», затрагивая отдельные аспекты делегирования правосубъектности человека компьютерной системе.

В рамках рассмотрения такого признака как мотивация мошенничества в глобальной сети Интернет раскрывается ее основополагающий признак – корысть. Затрагиваются вопросы соотношения мотива, цели и результата преступления. Основной акцент делается на корыстный мотив преступной деятельности. Последствия преступления тесно связываются с информационным характером интернет-мошенничества. Отмечается дуализм обладания похищенным правом, зафиксированным в электронном виде, поскольку законный владелец

зачастую не утрачивает возможности распоряжаться своим имуществом. Данные аспекты электронных хищений в зарубежной литературе нашли отражение в виде нового феномена – «кражи личности» (identity fraud).

Специфическим признаком интернет-мошенничества является использование глобальной компьютерной сети в противоправных целях. Раскрывается вопрос об использовании устройств отличных от компьютерной техники, позволяющих осуществлять доступ в глобальную сеть Интернет, а также механизм причинения имущественного ущерба путем обмана и злоупотребления доверием путем использования Интернет во вполне правомерных целях, но за чужой счет.

Вся совокупность признаков позволила объединить в один объект исследования:

- хищения с использованием компьютерных систем, подключенных к глобальной сети Интернет;
- причинение имущественного ущерба путем обмана и злоупотребления доверием, также с использованием компьютерных систем, подключенных к глобальной сети Интернет;
- «традиционные» мошеннические схемы, которые охватываются диспозицией ст. 159 УК РФ, но обязательным элементом в реализации преступного замысла при этом является использование компьютерных систем, подключенных к глобальной сети Интернет.

Во втором параграфе «Интернет-мошенничество в структуре компьютерной преступности» освещается трансформация преступности на основе нового типа общественных отношений – информационных. Компьютерная преступность постоянно расширяет «сферу деятельности». Проводится исследование эволюции взглядов на компьютерную преступность в отечественной криминологической науке. При этом автор придерживается концепции, в соответствии с которой, необходимо говорить лишь о компьютерных аспектах различного рода преступлений. Ключевым аспектом компьютерной преступности является компьютерная (машинно-обрабатываема) информация. При этом глава 28 УК РФ выступает достаточно устойчивым конструктом, поскольку вменение статей по совокупности в ряде случаев (в трактовке правоприменительной практики Верховным Судом РФ) позволяет избежать внесения не вполне обоснованных изменений в УК, связанных с выделением отдельных видов компьютерной преступности в отдельных составах преступлений или повсеместного внедрения квалифицирующих признаков.

В зависимости от способов и приемов манипуляции компьютерной информацией, все компьютерные преступления подразделяются автором на три блока.

рис 1. Структура компьютерной преступности.

Часть мошенничеств, направленная на обман человека, а не компьютерной системы, требует визуализации. Обман компьютерной системы же проходит опосредованно – вне сознания человека. Применение термина «визуализация» будет оправдано и для иных преступлений, не связанных с мошенничеством (ст.ст. 130, 138, 242, 242.1 УК РФ).

Оборот машинно-обрабатываемой информации (обмен, модификация, копирование и пр.) уже трудно увязать только с компьютерной системой в силу отсутствия единых технических требований к компьютерной системе, т.е. самого понятия. Интернет является инструментом распространения такой информации; компьютер, подключенный к глобальной сети, средством ее «визуализации» или самостоятельной обработки. Интернет как средство распространения информации с неизбежностью ведет к увеличению количества мошеннических схем, связанных с его использованием. Ведь любой преступный обман представляет собой манипуляцию с информацией, которая весьма эффективно распространяется посредством коммуникативных технологий Интернет.

В третьем параграфе «Структура интернет-мошенничества» автор проводит классификацию явления по техногенно-историческому критерию, выделяя две категории интернет-мошенничества: «традиционные компьютеронезависимые» формы мошенничества, использующие возможности Интернет для реализации преступного умысла в целях обогащения и «нетрадиционные компьютерозависимые» формы (компьютерное мошенничество) также зачастую использующие коммуникационные возможности Интернет. Характерной чертой «компьютерозависимых» форм мошенничества является то обстоятельство, что изначально они совершались в реальном пространстве и только в процессе развития информационных отношений были перенесены в «виртуальную реальность». Примеров подобной трансформации преступной деятельности много: например, изготовление поддельных документов, бланков, марок акцизного сбора, специальных марок или знаков соответствия, поддельных денег или ценных бумаг, сначала с помощью простого перерисовывания, несколько позднее с помощью изготовления клише, еще позднее с помощью копировального оборудования, и в последнее время при помощи компьютера и распечатывания на принтере. Поэтому даже весьма радикальные методы, такие как прекращение

функционирования Интернет или даже отказ человечества от компьютерной техники, не способен полностью искоренить мошенничество. «Нетрадиционные компьютерозависимые» формы (компьютерное мошенничество), зачастую использующие коммуникационные возможности Интернет, являются «компьютерозависимыми» поскольку само преступление (хищение) не мыслимо без модификации, копирования компьютерной информации. «Компьютерозависимое» мошенничество является следствием несовершенства информационной безопасности.

Помимо указанной классификации проводится типология по способу совершения отдельных мошеннических схем, все разнообразие которых свести к одному классификационному основанию не представляется возможным. Согласно основным направлениям мошеннической деятельности автор выделяет восемь направлений мошеннической деятельности.

Совмещая указанные виды преступлений и их типы, автор приходит к единой структуре интернет-мошенничества.

Вторая глава – «Криминологическая характеристика мошенничества в глобальной сети Интернет» состоит из пяти параграфов.

Первый параграф «Состояние мошенничества в Интернет» посвящён вопросам изучения состояния и криминологического прогнозирования явления. Интернет-мошенничество, рассматривается как закономерный социальный процесс, обусловленный глобальной информатизацией и рядом иных условий. Выделяется ряд основополагающих тенденций развития компьютерной преступности, связанной с использованием сетевых технологий. Отмечается наличие корреляционных связей между распространением мошенничества в глобальной сети Интернет и ростом числа ее пользователей, стоимостью доступа, развитием предпринимательских отношений (электронной коммерции).

В соответствии с этими тенденциями даётся итоговый прогноз относительно дальнейшего распространения мошенничества в глобальной сети Интернет:

а) появление традиционных мошеннических схем в российском сегменте Интернет обусловлено общими тенденциями развития компьютерной преступности, основными факторами распространения которой являются глобальные процессы информатизации стран и коммерциализации информационных ресурсов;

б) по мере возникновения новых возможностей электронной коммерции будет расти количество преступлений против собственности. Доля традиционных (компьютеронезависимых) мошенничеств в глобальной сети Интернет будет увеличиваться по отношению к компьютерному мошенничеству, латентность которого будет увеличиваться;

в) основным криминогенным фактором на сегодняшний день является рост количества пользователей в российском сегменте Интернет. Однако в связи с постепенным замедлением прироста числа новых пользователей в ближай-

шем будущем на первое место должен выдвинуться фактор коммерциализации: расширения финансовых, банковских услуг, массовое развитие интернет-торговли, сферы предоставления услуг;

г) переход традиционных форм мошенничества в Интернет приведет к снижению выявляемости и раскрываемости деяний, совершенных таким способом;

д) компьютерное мошенничество вскоре полностью перейдет в категорию профессиональной преступности. Для преодоления сложных систем информационной безопасности уже сегодня требуется слаженное усилие специалистов в нескольких областях. Поэтому компьютерные мошенники будут создавать транснациональные организованные преступные группировки;

е) основная масса зарегистрированных компьютерных мошенничеств будет относиться к категории пресеченных на стадии покушения. Их по преимуществу будут совершать лица, только начинающие преступную карьеру. Оконченные преступления будут выявляться намного реже. Финансовые учреждения не склонны афишировать недостатки систем безопасности данных. Профессиональные преступники также успешно смогут избегать уголовной ответственности, скрывая следы преступлений или находясь вне досягаемости правоохранительных органов стран, в которых они совершают преступления.

Второй параграф «Латентность интернет-мошенничества» преследует цель более полно познать изучаемое явление, некоторые вопросы, которые не нашли отражения в официальной статистике. Анализируется возможность применения существующих методов измерения латентности. На основе изучения мнения практических работников была составлена приблизительная картина, оценивающая фактические масштабы латентности интернет-мошенничества и компьютерной преступности. В ходе социологического исследования обобщалось мнение об уровне преступности в сфере высоких технологий, выявляемости мошенничества, соотношении латентности интернет-мошенничества с латентностью уличного мошенничества и мошенничества в сфере экономической деятельности. Другим методом исследования латентности стал метод моделирования путем сравнения уровня преступности двух стран: США и России. В подтверждение автор приводит ряд доводов – причин латентности именно данного вида преступности.

Третий параграф «Криминологические детерминанты мошенничества в глобальной сети Интернет» посвящен анализу отдельных причин и условий мошенничества в Интернет. В авторской концепции весь причинный комплекс разбит на группы: во-первых, по особенностям современных сетевых технологий, предоставляющих возможность успешного ведения преступной деятельности; во-вторых, связанных с отсутствием социально-правового контроля со стороны общества за процессами информатизации; в-третьих, объединяющий недостатки в сфере правового регулирования; в-четвертых, комплекс причин, связанных с недостатками правоохранительной деятельности.

В ходе изучения описанных выше групп детерминант было установлено, что именно анонимность во многом определяет специфику общения пользователей в глобальной сети. Технологии мобильного (беспроводного) Интернет усугубляют ситуацию, поскольку преступник может свободно перемещаться в пространстве, используя различные точки доступа. На условиях анонимности предоставляется доступ во всемирную паутину из мест коллективного доступа: широко распространены компьютерные клубы, интернет-кафе. Анонимность в глобальной сети тесным образом связана со свободой доступа. Доступ к услугам сети Интернет уже не является прерогативой обеспеченных слоев населения. Еще одной специфической особенностью является оперативность действий, производимых в Интернет. Оперативность любых операций распространяется на все пространство Интернет, охватывающее страны и континенты. С помощью современных технологий стало возможным общение и взаимодействие людей из различных уголков планеты. Те же самые технологии обеспечивают для мошенников возможность массового воздействия на своих жертв. С минимальной затратой средств и сил стало возможным тиражирование одного и того же сообщения на много-численных досках объявлений, форумах, в виде почтовых сообщений.

Отсутствие социального контроля порождает долгосрочные социально-негативные тенденции. Интернет представляет собой глобальную компьютерную сеть, основанную на принципе саморегуляции, автономности, самодостаточности. Являясь глобальной формой организации общественных отношений, Интернет обществом вовсе не контролируется. Неурегулированность правом информационных процессов, трудности правоприменения, незащищенность интересов сетевых пользователей приводят к возрастанию правового нигилизма. Это состояние является следствием деформации нравственного сознания. Сегодня в сознании людей идет активная переоценка нравственных приоритетов – особое значение придается материальному успеху и власти как способам занять достойное положение в обществе.

Имеющиеся недостатки в правовом регулировании электронной торговли привели к тому, что потребители вынуждены нести на себе все риски предпринимательства. Предприниматели, потерпевшие ущерб от экономических преступлений, перекладывают потери на покупателей. Не урегулированы вопросы заключения сделок в электронной форме, что не позволяет говорить о полноценной реализации концепции электронного бизнеса не территории Российской Федерации. Правовые недостатки в сфере защиты прав потребителей привели к тому, что покупатели настороженно относятся к возможности покупок через Интернет. Главная проблема заключается не в содержании норм, которые соответствуют общемировым требования, а в том, что контролировать исполнение законодательства в Интернет некому.

Основной показатель эффективности деятельности правоохранительной системы – чувство защищенности прав и законных интересов гражданина. Как

удалось установить в ходе проведенного нами виктимологического опроса, потерпевший сам не стремится обращаться в компетентные органы, потому как не надеется на помощь с их стороны. Однако зарубежная практика показывает успешные примеры деятельности многих общественных организаций по предупреждению мошенничества в Интернет. На сайтах таких организаций потерпевший может узнать о появлении новых мошеннических схем, ознакомиться с советами экспертов по тому, как распознать и избежать мошенничества. Эти процессы ведут к дальнейшей виктимизации населения. В 2003 году из Уголовного кодекса была исключена статья, устанавли-вающая ответственность за обман потребителей (ст. 200 УК), одновременно с этим исчезла статья 182 УК «Заведомо ложная реклама». В 2010 году из Уголовного кодекса была исключена ст. 173 «Лжепредпринимательство». По результатам проведенного автором опроса, абсолютное большинство сотрудников правоохранительных органов оценили данную тенденцию как негативную, выразив уверенность в том, что такой подход законодателя приведет к росту преступлений в сфере потребительского мошенничества.

В ходе изучения мнения сотрудников МВД, чья деятельность непосредственно связана с выявлением и раскрытием, расследованием мошенничества в Интернет установлено, что во многих случаях раскрытие и расследование преступлений связано с определенными трудностями. Например, следствие испытывает больше трудностей, нежели оперативные работники, выявляющие преступления и лиц, их совершивших. Иимеются и некоторые иные особенности. Начальствующий состав отделов БЭП и отделов «К» БСТМ всегда указывает на наличие трудностей в отличие от рядовых сотрудников. Осведомленность зависит от ряда факторов: должности, возраста, опыта работы, специализации, личного опыта пользования Интернет.

Причины, сдерживающие широкое распространение интернет-мошенничества в России, по преимуществу, естественного характера: во-первых, это нестабильное социально-экономическое положение в стране – достаточно низкий уровень доходов населения; во-вторых, существующий, но стремительно сокращающийся «разрыв» в области использования высоких технологий; в-третьих, это имеющийся «языковой барьер», не позволяющий отдельным мошенникам совершать преступления в отношении граждан и организаций иных стран.

Четвертый параграф «Личность интернет-мошенника» раскрывает особенности механизмов индивидуального преступного поведения профессионального и ситуативного мошенника. В целях собственного исследования автор намеренно утрировал существующие концепции типологии личности преступника, каждая из которых насчитывает значительно больше типов личности. Выделение всего лишь двух типов позволило более чётко отграничить один от другого, определить наиболее характерные психологические черты, поведенческие реакции, более наглядно соотнести их с механизмом индивидуального преступ-

ного поведения. Пределы криминологического исследования личности преступников этих двух типов задаются относительно редкими фактами выявления мошенничества в Интернет и привлечения преступников к ответственности, низкой мотивацией сотрудников правоохранительных органов по тщательному и полному установлению личностных особенностей преступников. В сравнении даны сведения о личности интернет-мошенников зарубежных стран, в частности США. Наличие двух основных типов личности интернет-мошенников свидетельствует о необходимости использования различных приемов для предупреждения их преступной деятельности. Так, факторы, формирующие личность ситуативного мошенника, устраняются путем более четкой правовой регламентации использования информационных ресурсов глобальной сети Интернет. Наведение правопорядка в электронной коммерции, в области заключения сделок между физическими лицами, в сфере электронных платежных систем позволит значительно сократить количество правонарушений, совершаемых ситуативными мошенниками.

Для предупреждения преступной деятельности профессиональных мошенников необходимо, прежде всего, развивать международное сотрудничество по борьбе с транснациональной компьютерной преступностью, решать вопросы разграничения юрисдикции двух или нескольких государств, унифицировать национальные уголовно-правовые нормы с международными нормами.

Пятый параграф является логическим следствием предыдущего вопроса, раскрывающим связь: жертва – преступник. В работе все виктимогенные факторы условно разделены на объективные – внешние по отношению к жертве; и субъективные – обусловленные психическими особенностями индивидов. Описаны некоторые особенности жертв интернет-мошенничества, приведены поясняющие диаграммы и приложения. Отмечен и такой факт как инверсия ролей – обстоятельство рассмотрено в качестве одного из факторов становления личности ситуативных мошенников. В рамках исследования автор затрагивает проблему виктимности юридического лица. Анализ виктимогенных факторов позволил сформулировать следующие положения: 1) в России виктимологическому риску подвержены более молодые слои населения в силу их большей приверженности к современным технологиям. В США развитие Интернет опережает другие страны, что отражается на графике, захватывая более старшую возрастную группу. Вместе с тем наблюдается некоторое сходство по уровню риска двух возрастных групп, располагающихся в пределах от 20 – до 40 лет, поскольку именно здесь находятся наиболее трудоактивные и обеспеченные слои населения; 2) более 40 % российских пользователей Интернет становились жертвами мошенников. Остальные не пользуются возможностями дистанционной торговли, поскольку не доверяют интернет-магазинам, либо предпочитают осуществлять покупки традиционным способом. 3) особым виктимогенным потенциалом обладает электронная почта. Распространение спама в российском сегменте Интернет достигло угрожающих размеров – более 75% почтового тра-

фика. При этом значительная доля спама посвящена тематике компьютерного мошенничества. 4) основными виктимологическими рисками для юридических лиц остаются вопросы информационной безопасности.

Третья глава – «Предупреждение мошенничества в глобальной сети Интернет» состоит из пяти параграфов.

Первый параграф «Система мер предупреждения мошенничества в глобальной сети Интернет» раскрывает содержание системы мер, дает краткое описание каждой их них. Автор предлагает выделить и конкретизировать традиционные для криминологии: общесоциальный (общий), специально-криминологический (специальный) и индивидуальный уровни предупреждения преступности применительно к изучаемому явлению. С другой стороны, учитывая специфику интернет-мошенничества, необходимо выделять и основные формы воздействия: виктимологическую профилактику и меры по обеспечению информационной безопасности. Виктимологическая профилактика мошенничества в Интернет направлена, прежде всего, на предупреждение традиционных форм мошенничества в Интернет, а меры по обеспечению информационной безопасности направлены на предупреждение компьютерного мошенничества.

Второй параграф «Общесоциальные меры предупреждения» содержит конкретные предложения по предупреждению мошенничества в глобальной сети Интернет. Был выделен и проанализирован целый ряд компонентов: 1) совершенствование уголовной политики; 2) организация и осуществление социально-правого контроля; 3) организация и правовое регулирование криминологической экспертизы; 4) правовое регулирование Интернет.

Обобщая указанные предложения по устранению условий интернет-мошенничества, можно сделать следующие наиболее важные выводы:

1. В рамках совершенствования реализации уголовной политики необоснованно мало внимания уделяется потребительскому мошенничеству. Законодателем даже избрано направление на декриминализацию таких деяний. Анализируя представленные нами типы мошенничества, можно прийти к выводу, что многие из них как раз связаны с коммерциализацией глобальной сети Интернет. Все это лишь осложняет криминогенную обстановку.

2. Учитывая логику построения отечественного уголовного законодательства, представляется нецелесообразным выделять квалифицированные составы мошенничества в отдельные статьи Уголовного кодекса. Мошенничество исключительно разносторонний феномен, криминализация всех его форм приведет к лишним квалификационным ошибкам. Об отсутствии диссонанса в понимании этого явления свидетельствует и правоприменительная практика в толковании Верховного Суда РФ, предлагающая ныне квалифицировать компьютерное мошенничество по совокупности статей.

В этом отношении показателен и сам институт преступлений в сфере компьютерной информации (глава 28 УК РФ), превращающийся в универсальную конструкцию, определяющую именно компьютерно-информационный спо-

соб совершения практически любого преступления предусмотренного особенной частью УК.

3. Одним из важнейших аспектов компьютерной преступности является причиняемый ей экономический ущерб. При этом часть совершаемых в Интернет мошенничеств не подлежит единому систематическому учету. Отсутствует единая методика определения «цены преступности».

4. Социально-правовой контроль как самый эффективный инструмент предупреждения требует легализации. Необходимо принятие федерального закона о негосударственных субъектах предупреждения и системе мер государственной поддержки такой деятельности.

5. Обращая внимание на потенциал Интернет (как СМИ) в целях предупреждения правонарушений, государственные органы мало внимания уделяют реализации этой составляющей.

6. На сегодняшний день существуют две основные проблемы глобального регулирования Интернет: инертность международных организаций по ликвидации анонимности в глобальной сети и разграничение юрисдикции государств при реализации национальных программ по борьбе с правонарушениями в Интернет.

7. В условиях глобализации законодатели различных стран призывают к более решительным мерам по борьбе с компьютерной преступностью. Внедрение профилактических мер в различных странах приводит к постепенному усилению контроля со стороны правоохранительных органов за деятельностью отдельных лиц во «всемирной паутине». На национальном уровне наблюдается постепенная тенденция к изоляции отдельных сегментов сети Интернет с целью более полного контроля над ними. В этом отношении Россия пока не занимает последовательной позиции, хотя изоляция российского сегмента Интернет дала бы положительный эффект.

В третьем параграфе «Криминологическая экспертиза в системе мер предупреждения мошенничества в глобальной сети Интернет» автор с позиции криминологической экспертизы проводит анализ нескольких актуальных законопроектов. И основе этого формулирует ряд научных предложений по правовому регулированию общественных отношений на национальном уровне в целях предупреждения мошенничества в глобальной сети Интернет. Так предлагается принятие концептуального закона «О развитии российского сегмента Интернет», который должен прояснить многие ключевые понятия в сфере организации доступа в глобальную сеть, определить статус субъектов, предоставляющих такие услуги, политику российского государства по отношению к Интернет. В качестве продолжения последовательной политики государства в области регулирования Интернет необходим нормативно-правовой акт, регламентирующий отношения в сфере электронной торговли. Российскому сегменту глобальной сети Интернет необходимо принятие закона, который бы регулировал отношения по заключению сделок не только в сфере предпринимательства, но и

сделок, заключаемых физическими лицами между собой. Одним из важнейших требований остается проблема регулирования деятельности прочих некредитных финансовых организаций, производящих расчеты между пользователями в Интернет, так называемых электронных платежных систем. Концепция закона «Об электронной цифровой подписи» имеет существенные недостатки в целях предупреждения преступности. Одной из важнейших мер должна стать взвешенная и реализуемая программа государства по внедрению ЭЦП. Необходимо упростить порядок сертификации и выдачи ключей ЭЦП пользователям-физическим лицам, унифицировав этот момент с моментом заключения договора с провайдером об оказании услуг по доступу в Интернет. Выход из сложившейся ситуации можно найти только с помощью государственной поддержки. Сформулирован также ряд иных предложений.

Четвертый параграф «Специально-криминологическое предупреждение мошенничества в глобальной сети Интернет» последовательно раскрывает основные формы предупредительного воздействия: организационно-технические мероприятия по обеспечению информационной безопасности и виктимологическую профилактику. Основной задачей организационно-технических мер предупреждения мошенничества в глобальной сети Интернет является борьба с анонимностью совершаемых интернет-пользователями действий. Одним из возможных решений является введение идентификации пользователей Интернет. Проводится анализ технических средств, позволяющих решить подобную задачу.

Виктимологическая профилактика мошенничества в глобальной сети Интернет также складывается из ряда мероприятий. Выявленные в ходе исследования виктимогенные факторы позволили выделить основные направления виктимологической профилактики мошенничества в Интернет: а) одним из основных аспектов виктимологической профилактики является повышение эффективности информационной безопасности, совершенствование программно-технических средств защиты компьютерной информации; б) особое внимание стоит уделять распространению спама по электронной почте; в) использовать Интернет в качестве информационного ресурса для предупреждения мошенничества в Интернет.

В рамках выделенных направлений автор предлагает ряд специфичных мер реагирования: организовать полноценное взаимодействие правоохранительных органов, негосударственных субъектов предупреждения и граждан при помощи государственной поддержки; создать единый информационный портал по борьбе с мошенничеством в глобальной сети интернет способный одновременно решать ряд научно-практических задач; обратить особое внимание на принципы формирования кадровой политики юридическими лицами, возможность страхования рисков мошенничества.

В зависимости от перспективы все предлагаемые меры автор разделяет на два этапа: текущий и последующий.

Для сокращения интернет-мошенничества на текущем этапе необходимо одновременно оказывать воздействие в трех направлениях:

1) борьба с анонимностью интернет-пользователей: в местах коллективного доступа, владельцев электронных почтовых ящиков, владельцев счетов электронных платежных систем;

2) правовое регулирование экономических отношений в глобальной сети Интернет, что позволяет устранить экономическую основу мошенничества: вопросы электронной формы сделки по гражданскому законодательству, вопросы регулирования деятельности и ответственности ЭПС, интернет-аукционов, участников дистанционной торговли.

3) организация полноценного взаимодействия правоохранительных органов, негосударственных субъектов предупреждения и граждан в целях реализации положений виктимологической профилактики.

Технология интернет-паспорта является наиболее перспективной технологией (для реализации «последующего этапа»), существенно сокращающей возможности распространения мошенничества в глобальной сети Интернет. Однако без устранения указанных нами недостатков целей предупреждения мошенничества она достичь в полной мере не сможет. Таким образом, необходимо финансировать отечественные научно-технические исследования в этой сфере и развивать международное сотрудничество. Ибо подобная технология не должна быть монополизирована какой-либо отдельной страной, что угрожает национальной безопасности России.

Пятый параграф «Индивидуальное предупреждение ряда типичных мошеннических схем» содержит совокупность практических рекомендаций, которая может быть применена на практике для предупреждения различных мошеннических схем, типология которых приводится в первой главе диссертационного исследования.

Среди них особо выделяются: мошенничество на интернет-аукционах, мошенничества связанные с электронными платежными системами, пластиковыми банковскими картами, используемыми при расчетах через Интернет (кардинг и фишинг).

В **заключении** сформулированы научно обоснованные положения, отражающие основные достижения диссертационного исследования, совокупность которых условно можно разделить на две группы: закономерности мошенничества в Интернет как криминологически значимого явления; ряд рекомендаций, касающихся предупреждения этого явления на территории Российской Федерации, точнее в российском сегменте глобальной сети Интернет.

Основные положения диссертации отражены в следующих работах автора:

- статьи в журналах, включенных в Перечень ведущих рецензируемых научных журналов и изданий, рекомендованных ВАК Министерства образования и науки РФ:

1. Комаров, А.А. Причинение имущественного ущерба путем обмана и злоупотребления доверием в контексте компьютерного мошенничества / А.А. Комаров // Российский криминологический взгляд. – Ставрополь, 2008. – №2. – Стр. 258-261. (4 стр. / 0,24 п.л.).
2. Комаров, А.А. Об уголовной политике России в области противодействия преступной деятельности в Интернет и рекомендациях криминологической науки / А.А. Комаров // Право и политика. – М., 2008. – №11. – Стр. 2674 – 2679. (6 стр./0,75 п.л.).
3. Комаров, А.А. Специфика мошенничества в Интернет / А.А. Комаров // Современное право. – М., 2009. – №1. Стр. 91 – 93. (3 стр. / 0,37 п.л.).
4. Комаров, А.А. Криминологическая экспертиза некоторых законопроектов, связанных с Интернет / А.А. Комаров // Современное право. – М., 2009. – №6. – Стр. 109 – 114. (5 стр. / 0,62 п.л.)

- статьи в иных изданиях:

5. Комаров, А.А. Интернет как преступная среда. Взгляд на проблему / А.А. Комаров // Научные концепции повышения жизненного уровня населения на современном этапе развития России: сб. науч. трудов / филиал РГСУ в г. Кисловодске; под ред. Л.Г. Коломойцевой. – Кисловодск, 2005. – С. 333-338. (6 стр. / 0,38 п.л.).
6. Комаров, А.А. Информационная безопасность как составляющая профилактики компьютерного мошенничества / А.А. Комаров // Трибуна молодых учёных: сб. науч. тр. / Пятигорский государственный технологический университет, кафедра уголовного права и процесса; под ред. Е.Н. Зайцевой. – Пятигорск, 2005. – С. 51-55. (5 стр. / 0,19 п.л.).
7. Комаров, А.А. Мошенник и Интернет. Суждение о личности / А.А. Комаров // Неделя уголовного права и процесса: сб. науч. тр. / Пятигорский государственный технологический университет, кафедра уголовного права и процесса; под ред. А.В. Симонян. – Пятигорск, 2006. – С. 64-69. (6 стр. / 0,22 п.л.).
8. Комаров, А.А. Криминологические детерминанты мошенничества в сети Интернет / А.А. Комаров // Актуальные проблемы правовой науки, теории и практики: сб. науч. тр. / Пятигорский государственный технологический университет, кафедра уголовного права и процесса; под ред. Н.В. Исако-

ва. – Пятигорск, 2007. – С. 65-73. (9стр. / 0,42 п.л.).
9. Комаров, А.А. Борьба с преступностью в глобальной сети Интернет: международный опыт и законодательство России / А.А. Комаров // Политика и общество. – М.: 2008. – №5 (47). – Стр. 29-34. (6 стр. / 0,46 п.л.).
10. Комаров, А.А. Мошенничество в глобальной сети Интернет, как одна из основных угроз становлению информационного общества в России / А.А. Комаров // Право и безопасность. – М., 2008. – №3. – Стр. 23 – 27. (5 стр. / 0,58 п.л.).
11. Комаров, А.А. Правовое регулирование мер предупреждения мошенничества в глобальной сети Интернет / А.А. Комаров // Глобальный научный потенциал. Сборник материалов 5-й международной научно-практической конференции: 16-17 июня 2009 – Тамбов, 2009. – Стр. 3 – 5. (2 стр. / 0,14 п.л.)
12. Комаров, А.А. Виктимологические аспекты интернет-мошенничества / А.А. Комаров // Тенденции и противоречия развития российского права на современном этапе: сб. науч. тр. – Пенза: Приволжский Дом знаний, 2009. – Стр. 156 – 158 (3 стр. / 0,21 п.л.).
13. Комаров, А.А. Проблема предупреждения мошенничества в глобальной сети Интернет / А.А. Комаров // Современные вопросы государства, права, юридического образования: сб. науч. тр. / Тамбовский государственный университет им. Г.Р. Державина. – Тамбов: издательский дом ТГУ им. Г.Р. Державина, 2010. – Стр. 262 – 265. (4 стр. / 0,28 п.л.).