

Министерство образования и науки РФ
Федеральное государственное бюджетное образовательное
учреждение высшего образования
«Пензенский государственный университет»

Юридический факультет

Кафедра «Уголовное право»
(наименование)

Направление подготовки

40.04.01
(код

«Юриспруденция»
и наименование)

Магистерская программа

Уголовное право
(наименование)

МАГИСТЕРСКАЯ ДИССЕРТАЦИЯ

на тему:

«Интернет-преступность: уголовно-правовая и криминологическая
характеристика»

Студент 15ююм3
номер группы


подпись, дата

Альмяшев Камиль Рафаэлевич
фамилия, имя, отчество полностью

Научный руководитель


подпись, дата

О.В. Романовская
фамилия, инициалы

Консультанты:

по _____
наименование раздела, звание, должность

подпись, дата

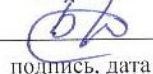
фамилия, инициалы

по _____
наименование раздела, звание, должность

подпись, дата

фамилия, инициалы

Нормоконтролер: к.ю.н., доцент
должность


подпись, дата

О.В. Безрукова
фамилия, инициалы

Рецензент: Сидорова Ольга Владимировна
С.К. РР по Пензенской обл.
должность


подпись, дата

Казаров Д.Ю.
фамилия, инициалы

Работа допущена к защите в (протокол заседания кафедры от 06.06 2017 г. № 1)

Заведующий кафедрой «Уголовное право»
название


подпись, дата

Г.Б. Романовский
фамилия, инициалы

Работа защищена с оценкой отл. (Протокол от 16 июля 2017 г. № 25)

Секретарь ГЭК


подпись, дата

Анатолий Е.Р.
фамилия, инициалы

Пенза 2017 г.

ПЕНЗЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
Юридический факультет
Направление «Юриспруденция»

УТВЕРЖДАЮ
Зав. кафедрой «Уголовное право»

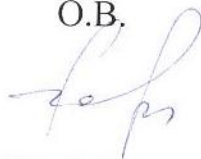
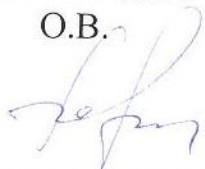
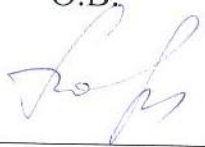
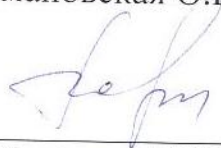
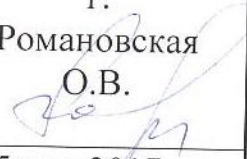
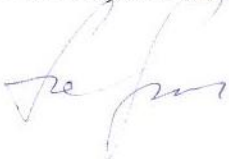
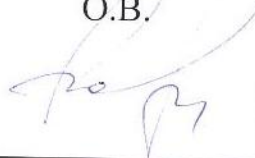
Г.Б. Романовский
(инициалы и фамилия)
 2017 г.

ЗАДАНИЕ

на выпускную квалификационную работу студента группы № 15ююм3
Альмяшева Камиля Рафаэлевича
(фамилия, имя, отчество)

1. **Тема работы:** «Интернет-преступность: уголовно-правовая и криминологическая характеристика»
2. **Научный руководитель:** профессор д.ю.н. О.В. Романовская
3. **Дата выдачи задания:** 25 ноября 2015 года
4. **Срок сдачи студентом законченной работы:** 29 мая 2017 года
5. **Перечень подлежащих разработке вопросов:**
 - 5.1 Понятие и уголовно-правовая характеристика интернет-преступности.
 - 5.2 Понятие интернет-преступности и история ее развития.
 - 5.3. Свойства интернет-преступности.
 - 5.4 Типология интернет-преступлений.
 - 5.5 Криминологическая характеристика интернет-преступности.
 - 5.6 Интернет-преступность в России. Криминологический анализ наиболее проблемных видов интернет-преступлений.
 - 5.7 Личность интернет-преступника и его жертвы.
 - 5.8 Меры предупреждения и международный опыт борьбы с интернет-преступностью.

6. Консультанты по работе, с указанием относящихся к ним разделов работы

Раздел	Консультант	Подпись, дата	
		Задание выдал	Выполненное задание принял
Введение		3 декабря 2015 г. Романовская О.В. 	16 января 2016 г. Романовская О.В. 
Понятие и уголовно-правовая характеристика интернет-преступности		16 января 2016 г. Романовская О.В. 	24 марта 2016 г. Романовская О.В. 
Криминологическая характеристика интернет-преступности		24 марта 2016 г. Романовская О.В. 	30 июня 2016 г. Романовская О.В. 
Меры предупреждения и международный опыт борьбы с интернет-преступностью		30 июня 2016 г. Романовская О.В. 	18 января 2017 г. Романовская О.В. 
Заключение		18 января 2017 Романовская О.В. 	5 мая 2017 г. Романовская О.В. 

СОДЕРЖАНИЕ

ВВЕДЕНИЕ.....	6
1 ПОНЯТИЕ И УГОЛОВНО-ПРАВОВАЯ ХАРАКТЕРИСТИКА ИНТЕРНЕТ-ПРЕСТУПНОСТИ.....	10
1.1 Понятие интернет-преступности и история ее развития.....	10
1.2 Свойства интернет-преступности.....	19
1.3 Типология интернет-преступлений.....	27
2 КРИМИНОЛОГИЧЕСКАЯ ХАРАКТЕРИСТИКА ИНТЕРНЕТ- ПРЕСТУПНОСТИ.....	51
2.1 Интернет-преступность в России. Криминологический анализ наиболее проблемных видов интернет-преступлений.....	51
2.2 Личность интернет-преступника и его жертвы.....	60
2.3 Меры предупреждения и международный опыт борьбы с интернет- преступностью.....	68
ЗАКЛЮЧЕНИЕ.....	75
СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ.....	77

ВВЕДЕНИЕ

Данная выпускная квалификационная работа посвящена теме «Интернет-преступность: уголовно-правовая и криминологическая характеристика». В условиях повсеместной интернетизации она, несомненно, является актуальной для современного уголовного права.

Стремительное внедрение цифровых технологий во все сферы человеческой жизни предопределило возникновение новых общественных отношений. Наибольшую значимость и распространенность имеет технология Интернет, которая сделала коммуникации дешевыми и беспрепятственными, открыла новые горизонты для всего мирового сообщества и дала человеку безграничные возможности в области распространения информации.

Всего несколько лет назад, интернет-преступления совершались в России, ввиду своей привилегированности, крайне редко, а интернет-преступность как негативное социальное явление, представляло реальную угрозу лишь в обозримом будущем. Но уже сейчас доля сетевой преступности в структуре общероссийской, существенно увеличилась. Это можно наблюдать на примере статистических данных о совершенных преступлениях в сфере компьютерной информации, которые показывают, что за последние десять лет в России количество зарегистрированных преступлений в сфере компьютерной информации увеличилось с 4050 до более 10000 преступлений в год. Хотя в последние годы наблюдается снижение регистрируемых преступлений. Это напрямую связано с ростом применения более совершенных компьютерных технологий для совершения широкого круга преступлений и сокрытия их следов.

Интернет стал средой распространения и развития сайтов, пропагандирующих и продающих наркотические вещества, публикующие

порнографические материалы (в том числе и с участием несовершеннолетних), а также ресурсы с откровенно расистской, националистской, террористической, экстремистской направленности.

Высокая социальная опасность преступлений в Глобальной сети является следствием их транснационального характера. Последствия подобных преступных деяний могут охватывать неограниченный круг лиц в самых разных уголках мира. При этом количество пользователей всемирной сети продолжает стремительно увеличиваться, а значит, вред, причиняемый интернет-преступниками будет только увеличиваться.

Интернет-преступность находится на стыке трех научных дисциплин: криминологии, уголовного и информационного права. И сегодня как никогда требуется подробное и всестороннее изучение интернет-преступности как негативного социального явления, так и отдельных видов сетевых преступлений, разработка и наиболее эффективных меры предупреждения и борьбы, совместная работа с правоохранительными органами других стран.

Актуальность данной выпускной квалификационной работы обусловлена с одной стороны, тем, что Интернет присутствует во всех сферах жизни современного общества, и с другой стороны, ее недостаточной разработанностью. Рассмотрение вопросов связанных с данной темой носит как теоретическую, так и практическую значимость.

Объектом данного исследования является анализ интернет-преступности как негативного социального явления, составов преступлений и их уголовно-правовой и криминологической характеристики.

Предметом исследования является рассмотрение отдельных вопросов, сформулированных в качестве задач данного исследования, в том числе путём сравнения с нормами международного права.

Целью работы является выявление наиболее спорных моментов и особенностей характеристики современной российской интернет-

преступности, ее криминологическая характеристика, разработка системы различного мер профилактики и противодействия

В рамках достижения поставленной цели были поставлены следующие задачи:

- 1) Изучить теоретические аспекты и выявить природу интернет-преступности, ее актуальности проблемы;
- 2) Назвать и раскрыть свойства интернет-преступности;
- 3) Привести типологию интернет-преступлений;
- 4) Указать криминологические особенности интернет-преступности в современной России;
- 5) Привести криминологическую характеристику наиболее актуальных и проблемных преступлений, совершаемых с помощью Интернета;
- 6) Раскрыть личность интернет-преступника и указать основные виктимологические проблемы интернет-преступности;
- 7) Рассказать о международном опыте борьбы с интернет-преступностью;
- 8) Указать способы предупреждения и борьбы с российской интернет-преступностью.

Работа имеет традиционную структуру и включает в себя введение, основную часть, состоящую из 2 глав, заключение и список использованных источников информации.

Во введении обоснована актуальность выбора темы, поставлены цель и задачи исследования, охарактеризованы методы исследования и источники информации.

Первая глава «Понятие и уголовно-правовая характеристика интернет-преступности» раскрывает понятие Интернета, интернет-преступности и интернет-преступления, а также исторические аспекты эволюции интернет-преступности. Обуславливается актуальность вопросов, напрямую связанных

с проблематикой правового понимания интернет-преступности в системе российского уголовного права. Раскрываются свойства интернет-преступности, а также дается типология интернет-преступлений.

Вторая глава «Криминологическая характеристика интернет-преступности» рассказывает о состоянии интернет-преступности в современной России и дает криминологическую характеристику наиболее проблемным и актуальным с правовой точки зрения интернет-преступлениям. Раскрываются особенности личности интернет-преступника, а также указываются виктимологические проблемы интернет-преступности, международный опыт борьбы с интернет-преступностью, указываются меры по предупреждению и борьбе.

В заключении указываются основные понятия и характеристики интернет-преступности, проблемы связанные с противодействием интернет-преступности и пути их решения, подводятся итоги дипломной работы,

Таким образом, актуальность данной проблемы для мирового сообщества и России в частности определила выбор темы работы, круг вопросов и логическую схему ее построения.

Теоретической и методологической основой проведения исследования явились законодательные акты и нормативные документы по теме работы.

Источниками для написания работы по теме «Интернет-преступность: уголовно-правовая и криминологическая характеристика» послужили базовая учебная литература, теоретические труды известных авторов в рассматриваемой области, результаты практических исследований, статьи и обзоры в специализированных и периодических изданиях.

1 ПОНЯТИЕ И УГОЛОВНО-ПРАВОВАЯ ХАРАКТЕРИСТИКА ИНТЕРНЕТ–ПРЕСТУПНОСТИ

1.1 Понятие интернет-преступности и история ее развития

Прежде чем перейти к рассмотрению проблем связанных с совершением преступлений в сети Интернет, для начала следует сформулировать базовый набор понятий и определений. Основным понятием в данной области является собственно «сеть Интернет».

Интернет на данном этапе развития человеческого общества можно смело назвать новым пространством человеческого самовыражения; международным виртуальным пространством, не имеющим чётких географических границ, децентрализованное пространство, которым полностью не владеет и не управляет ни одна из мировых держав. Такой подход к определению понятия сети Интернет в большей степени подчеркивает ту социальную значимость, которой глобальная сеть имеет для международного сообщества и современного человека. Но в то же время данное определение не раскрывает понятие сети Интернет с точки зрения особенных характеристик и свойств, в том числе и правовых.

Данное определение, имеет скорее технический и структурный характер, не отражая при этом принципиальных отличий Интернета от других технологий связи и компьютерных сетей.

Помимо транснациональности и глобальности некоторые авторы также обращают своё внимание на то, что по своей сути Интернет это «сеть в сети», то есть включает в себя большое число глобальных сетей - доменов, подчиняющихся определенным правилам. Физически они находятся на территории определенного государства, и их владельцы обязаны соблюдать законы, действующие в той или иной стране.

Интернет представляет собой объединение множества компьютерных сетей, на основе протокола IP и протокола маршрутизации пакетов данных (ТСР). В результате такого объединения сетей образуется глобальное информационное пространство (виртуально пространство или киберпространство), которое связывает компьютеры, системы и сети ЭВМ по всему миру. Несмотря на то, что Интернет имеет конкретное физическое воплощение в виде компьютеров, линий связи, серверов, Всемирная паутина это, прежде всего протокол, посредством которого унифицируется обмен данными в цифровом представлении между компьютерами и компьютерными сетями. Данная особенность позволяет компьютерам, вне зависимости от компании – производителя и индивидуальных технических характеристик, обмениваться между собой различной информацией и пакетами данных в электронном виде, так как правила передачи задокументированы и единообразны.

Таким образом, мы имеем дело с двоякой природой глобальной сети. С одной стороны Интернет - это множество компьютеров, соединенных в единую сеть, он имеет материальное воплощение в виде объединения ЭВМ. С другой стороны называть Интернет соединением компьютеров ошибочно, ведь всемирная паутина – это, прежде всего, набор абстрактных принципов и задокументированных протоколов, а уже потом реализованная на их основе глобальная система взаимодействия компьютеров.

Говоря о значении понятия «Интернет», следует отметить, что до недавнего времени российский законодатель по-разному толковал значение данного термина. Федеральный закон «Об информации, информационных технологиях и о защите информации» содержал в себе такое понятие, как «информационно-телекоммуникационная сеть», под которой подразумевается технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с

использованием средств вычислительной техники.¹ Но что конкретно входит в эту сеть не разъяснялось. В свою очередь, Федеральный закон «О рекламе» уже оперировал понятием информационно-телекоммуникационная сеть «Интернет». Эти данные были достаточно противоречивы и не давали точного определения сети Интернет.²

В 2011 году с принятием Федерального закона «О внесении изменений в отдельные законодательные акты Российской Федерации в связи с принятием Федерального закона «Об информации, информационных технологиях и о защите информации» глобальная паутина стала официально именоваться «информационно-телекоммуникационная сеть «Интернет».³ Говоря о содержании понятия «Интернет» и о его значении для российского законодателя, следует отметить, что Интернет главным образом является средством массовой коммуникации и представляет собой глобальное объединение компьютерных сетей и информационных ресурсов, принадлежащих множеству различных людей и организаций, средством массовой информации (главным образом это информационные ресурсы), а также информационным электронным архивом, предназначенным для хранения и передачи информации. Кроме того, за нарушение правил пользования Интернетом наступает ответственность, в том числе и уголовная.⁴

Нормативно правовое регулирование Интернета на территории Российской Федерации осуществляется рядом законодательных актов. Но их количество и качество, к сожалению, не отвечает тем требованиям, которые нужны не только для ведения эффективной борьбы с динамично

¹ Федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 05.04.2013) «Об информации, информационных технологиях и о защите информации» // СПС Консультант Плюс. - 2017.

² Максуров А.А. Интернет как новое правовое пространство. // Право и экономика. – 2010. - №3. – С. 39.

³ Федеральный закон от 11.07.2011 № 200-ФЗ (ред. от 02.05.2012) «О внесении изменений в отдельные законодательные акты Российской Федерации в связи с принятием Федерального закона «Об информации, информационных технологиях и о защите информации» // СПС «Консультант Плюс» - 2017.

⁴ Максуров, А. А. Интернет как новое правовое пространство. // Право и экономика. – 2010. – № 3. – С. 38 – 44.

развивающейся интернет-преступностью, но и правового регулирования интернет-отрасли в целом.

Так, Федеральный закон «О средствах массовой информации» под средством массовой информации понимается периодическое печатное издание, радио-, теле-, видеопрограмма, кинохроникальная программа, иная форма периодического распространения массовой информации. Нельзя отнести весь Интернет к средствам массовой информации, но некоторые его участки - информационные ресурсы таковыми являются, и действие вышеуказанного закона на них распространяется.¹

В отношении большинства правонарушений совершаемых в Интернете применяются нормы гражданского права. Чаще всего Гражданский кодекс РФ регулирует вопросы, связанные с причинением вреда доброму имени и деловой репутации; в отношении авторских и смежных прав на обнародованные, либо необнародованные произведения, находящиеся в какой-либо объективной форме; в связи с недобросовестной конкуренцией.

Немаловажную роль в регулировании правовых отношений связанных с сетью Интернет играет Закон «Об информации, информационных технологиях и о защите информации», который содержит в себе не только определение информационно-телекоммуникационной сети, но и раскрывает значение понятий: «электронное сообщение», «электронный документ», «оператор информационной системы», «сайт в сети «Интернет», «страница сайта в сети «Интернет», «доменное имя», «сетевой адрес», «владелец сайта в сети «Интернет», «провайдер хостинга».²

Административное право также имеет место при квалификации некоторых правонарушений, совершаемых с помощью всемирной паутины. Кодекс об административных правонарушениях содержит норму,

¹ Федеральный закон от 27.12.1991 № 2124-1 (ред. от 05.04.2013) «О средствах массовой информации» // СПС Консультант Плюс - 2017.

² Федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 05.04.2013) «Об информации, информационных технологиях и о защите информации» // СПС Консультант Плюс. - 2017.

предусматривающую ответственность за нарушение требований к организации доступа к информации о деятельности государственных органов и органов местного самоуправления и ее размещению в сети «Интернет».¹

Но для данного исследования наибольшее значение имеет взаимодействие сети Интернет и российского уголовного права. Наиболее ярким примером является Глава 28 Уголовного кодекса РФ, в которой законодатель впервые установил уголовную ответственность за совершение преступлений в сфере компьютерной информации. Но Интернет по своей сути может служить инструментом и средой совершения различных преступлений, имеющих объектом своего посягательства не только компьютерную информацию. О них будет рассказано подробнее.

В связи с такой многоликостью Интернета и информации, объединенной с его помощью в глобальное информационное пространство, встает вопрос, какое место может занимать Интернет в преступлении.

Интернет-преступность явление относительно новое и молодое и должна рассматриваться без отрыва от сети Интернет. Ведь именно благодаря таким особенностям глобальной сети как, анонимность, технические особенности применения, высокая скорость, трансграничность и дешевизна преступления совершенные с помощью Интернета выделяются на фоне традиционных преступлений. С исторической точки зрения можно выделить несколько этапов развития и становления интернет-преступности.

Первый этап связан с возникновением компьютерной сети Интернет в 60-е гг. XX века, когда сетевой преступности не существовало как явления.

Второй этап связан со становлением интернет-преступности и появлением первых интернет-преступников (хакеров). Наблюдается рост числа преступлений, совершаемых в сети, но эти противоправные деяния

¹ Кодекс Российской Федерации об административных правонарушениях от 30.12.2001 № 195-ФЗ (ред. от 07.05.2013) // СПС «Консультант Плюс» - 2017.

совершаются лишь узким кругом специалистов и пока не обладают таким признаком как «трансграничность».

На третьем этапе Интернет начинает использоваться в качестве средства и орудия совершения традиционных преступлений, а также на стадии приготовления к преступлению. С дальнейшим распространением Интернета в мире, возникают отдельные организованные национальные группы хакеров. Можно уже говорить о возникновении профессиональной интернет-преступности.

Четвертый этап развития характеризуется глобальностью, транснациональностью, появляется кибертерроризм. Зачастую Интернет используется в политических целях.

Уже сейчас с определенной долей уверенности можно прогнозировать наступление нового этапа в развитии интернет-преступности, который ожидает нас в ближайшем будущем. Учитывая современные темпы роста и развития Интернета, увеличение его влияние на общество, экономику, политику, интернет-преступность будет преобладать над остальными видами, и причинять огромный вред общественным и государственным интересам, влиять на политические процессы.

В зависимости от того как разнятся уровни развития высоких технологий, цифровых инфраструктур, распространения технической грамотности среди населения в различных странах мира, по-разному происходит и становление интернет-преступности. Чем больше государство уделяет внимание развитию информационных технологий, внедрению Интернета в повседневную жизнь своих граждан, тем быстрее и активнее происходит эволюция преступности. Нельзя при этом установить какие-либо временные рамки, у каждой страны, вставшей на путь информационно-технического прогресса, интернет-преступность проходила свои этапы развития в различные годы. Что касается России, то преступления в сети Интернет стали совершаться сравнительно недавно. Причиной тому

послужило достаточно позднее полноценное подключение и повсеместное распространение Интернета. Но, не смотря на это, за последние 10-15 лет интернет-преступность в России прошла первые три этапа развития. Для сравнения, в США у интернет-преступников на это ушло порядка 30 лет.

Преступления, совершаемые с помощью сети Интернет в России пока не достигли показателей США, стран Европейского союза, а также некоторых азиатских государств, но российская интернет-преступность уже успела за столь короткий срок полностью интегрироваться в мировую интернет-преступность, не смотря на достаточно низкий уровень интернетизации среди населения. Это произошло за счёт того, что в нашей стране самые высокие показатели некоторых видов интернет-преступности, в таких как: нарушение авторских и смежных прав, рассылка спама, распространение порнографии (в том числе детской).

Говоря о положении интернет-преступности среди других видов преступлений, многие авторы отождествляют ее с киберпреступностью, исходя из того, что преступления совершаются не в физическом мире, а в киберпространстве - виртуальной реальности. Такое определение интернет-преступности не совсем верно. Более того, сравнение интернет-преступности с компьютерной, не позволяет полностью охарактеризовать все криминальные проявления, связанные с использованием компьютерных сетей. Её скорее следует приравнивать к преступлениям, совершаемым с помощью компьютерных сетей, так как Интернет по своей сути является разновидностью компьютерной сети.

Преступления, совершенные с помощью компьютерных сетей, по мнению И.Г. Чекунова следует отнести к информационным преступлениям, наравне с киберпреступлениями, представляющими из себя совокупность преступлений, совершаемых в киберпространстве с помощью или посредством компьютерных систем или компьютерных сетей, а также иных средств доступа к киберпространству, в рамках компьютерных систем или

сетей, а также против компьютерных систем, компьютерных сетей и компьютерных данных.¹ Автор также отмечает, что толкование понятия «киберпреступность» шире чем «преступления в сфере компьютерной информации».

На мой взгляд, отнесение интернет-преступлений к разряду информационных достаточно спорно, ведь основой этой классификации преступлений является объект преступного посягательства – информация. Не во всех преступлениях, совершаемых в сети, преступный умысел направлен именно на завладение или распространение информации. Интернет уже стал воплощением реальной жизни в виртуальной плоскости, и на сегодняшний день большинство преступлений предусмотренных Уголовным кодексом находят своё отражение в Интернете и объектом выступают различные виды правоотношений не обязательно связанных с информационной сферой. Интернет-преступность тесно взаимосвязана с информационной, данный факт отрицать нельзя. Но эта связь зачастую прослеживается лишь на подготовительной стадии преступления, когда злоумышленнику требуется для совершения преступного деяния та или иная информация, либо он совершает информационное преступление с целью облегчить совершение другого правонарушения. Интернет-преступления являются частью киберпреступлений (компьютерных преступлений), при условии выделения данного вида преступлений по средству их совершения. Ведь любое интернет-преступление – это преступление компьютерное, но не наоборот.

Интернет-преступления выделяются на фоне информационных именно способом своего совершения, использование компьютерных сетей в качестве орудия или средства для достижения преступных результатов является их отличительной чертой, и характеризуют объективную сторону совершаемых преступлений.

¹ Чекунов И.Г. Киберпреступность: понятие и классификация // Российский следователь. – 2012. - №2. – С. 39.

В целом же понятие интернет-преступлений как элемента преступлений совершенных с использованием компьютерных сетей можно определить в виде совокупности запрещенных уголовным законодательством деяний, способ совершения которых предполагает обязательное использование таких сетей в качестве орудия или средства.¹ А российской криминологии интернет-преступностью называется социальное негативное явление в виде совокупности преступлений и их системы, которые совершены посредством или с помощью сети Интернет с территории Российской Федерации, либо с территории других государств, но направленных против интересов Российской Федерации.

Так или иначе, единообразной точки зрения на этот вопрос пока не существует, можно лишь надеяться, что с развитием российского законодательства и принятием международного опыта в области Интернета и сетевых преступлений, появится единая уголовно-правовая и криминологическая модель, указывающая их точное положение.

1.2 Свойства интернет-преступности

Для наилучшего понимания отличительных особенностей интернет-преступности, для начала следует раскрыть понятие среды, в которой данные преступления совершаются, так как свойства интернет-пространства непосредственно влияют на характеристики сетевых преступлений.

На сегодняшний день интернет представляет собой не только обширную компьютерную сеть, но и значительную часть международной информационно-коммуникационной технологии, которая активно развивается в современных условиях в совершенно новую, не имеющую аналогов информационную индустрию. Интернет формирует новое

¹ Чекунов И.Г. Киберпреступность: понятие и классификация // Российский следователь. – 2012. - №2. – С. 40.

пространство: экономическое, социальное, политическое, информационное, предпринимательское и все они неразрывно связаны с оборотом информации. Таким образом, можно сказать, что глобальная сеть Интернет это не только объединение компьютерных сетей, но и социальная структура, объединяющая людей по всему миру, от простых интернет - пользователей, до распространителей информации, провайдеров. Он может использоваться не только простыми гражданами, но и организациями, а также государственными структурами. Для определения этой новой среды зарубежные специалисты используют термин «киберпространство». Впервые этот термин был использован писателем-фантастом Уильямом Гибсоном, который использовал его для обозначения пространства, образуемого компьютерными сетями. В научной действительности данный термин позволяет осознать Интернет как новую форму пространства, которая не отвечает характеристикам материального мира, но в тоже время дающую возможность осуществлять в ней действия имеющие последствия для реального мира.

Киберпространство это сложное явление, которое должно рассматриваться в единстве двух основных его характеристик: социальной и технической. Социальная сторона понятия выражается в том, что киберпространство является совокупностью общественных отношений. Они возникают в процессе использования сети Интернет, а также других сетей, которые входят в состав киберпространства. Данные правоотношения возникают в процессе информационного обмена. И соответственно объектом данных отношений выступает информация, обращающаяся в мировой паутине. Техническая сторона вопроса заключается в характеристике киберпространства как сложного объекта – совокупности технических и программных средств, информационных ресурсов и инфраструктуры.

Когда речь идет о киберпространстве, имеется ввиду именно пространство, а не территория. Понятие «территории» в современной

научной доктрине зачастую имеет связь с государственными географическими границами, которые играют наиважнейшую роль в таких понятиях, как суверенность и государственная целостность. В соответствии с нормами международного права под государственной территорией понимается часть земного шара, которая принадлежит определенному государству и в пределах которой оно осуществляет свое территориальное верховенство; а в состав государственной территории входят: суша, воды, находящиеся под сушей и водами недр, воздушное пространство над сушей и водами. В действующем российском законодательстве имеется несколько определений пространства, так под воздушным пространством Российской Федерации понимается воздушное пространство над территорией Российской Федерации, в том числе воздушное пространство над внутренними водами и территориальным морем; космическое же пространство определяется как расположенное за пределами земной атмосферы пространство.¹

В целом же пространство можно определить как вмещилище, структуру, служащую средой, в которой происходят различные процессы (например, физические) и явления, которую человек в силах субъективно ощутить. Исходя из всего этого, можно сделать вывод, что киберпространство нельзя рассматривать с точки зрения территориального принципа (в буквальном понимании), но правовое понятие пространства, как некой среды обладающей специфическими качествами, здесь вполне применимо. Таким образом, под киберпространством понимается сфера социальной деятельности непосредственно связанная с оборотом информации в Интернете и других информационно-коммуникационных сетях, это уникальная по своим свойствам среда, не расположенная в

¹ Уголовное право. Особенная часть: учебник / Отв. ред. И. Я. Козаченко, Г. П. Новоселов. - 4-е изд., изм. и доп. - М.: Норма, 2008. - С. 81 - 82.

географическом пространстве, но доступная практически любому человеку вне зависимости от места его нахождения посредством доступа в Интернет.

По мнению И.М. Рассолова киберпространство может быть рассмотрено в нескольких плоскостях:

- киберпространство представляет собой глобальное объединение компьютерных сетей и информационных ресурсов, не имеющее при этом четко определенного владельца, служащее для интерактивной коммуникации индивидуумов, организаций и государственных структур;
- киберпространство открывает новые горизонты для человеческого самовыражения и общения, единое международное пространство, не имеющее четких географических границ;
- это децентрализованное пространство, которым полностью не владеет и не управляет ни одно государство;
- киберпространство разнородно, подразумевает свободу действий и высказываний.

Наряду с этими характеристиками М.С. Дашян предлагает также выделить принципы, на которых строится функционирование сети. К ним относятся:

- принцип конвергенции, означающий смешение традиционных явлений и процессов, переход их в новое состояние (ярким примером являются электронные библиотеки и правовые системы);
- принцип иерархичности отражает структурную взаимосвязь сетей, составляющих структуру Интернета;
- принцип децентрализации предполагает высокий уровень независимости компьютерных сетей от властных полномочий

органов государственной власти, предполагает самостоятельное регулирование процессов, связанных с функционированием сети;

- принцип экстерриториальности означает, что Интернет образует и является частью нового киберпространства, находящегося вне пределов реального мира, но имеющего тесную с ним связь.
- принцип демократичности тесно связан с социальной составляющей Интернета и означает возможность добровольного и равноправного участия в деятельности сети всех индивидуумов вне зависимости от их расы, национальности, места жительства, пола, имущественного положения и уровня образования.¹

Исходя из всех этих характеристик, определяющих свойства, как киберпространства, так и его части - Интернета, нельзя не отметить, что они тесно взаимосвязаны, а зачастую являются причиной возникновения такого отрицательного социального явления как преступность. Более того признаки отличающие Интернет находят свое отражение в свойствах интернет-преступности.

Благодаря глобальной и межгосударственной природе Интернета одно и тоже преступное деяние, совершенное с помощью глобальной сети подпадает под юрисдикцию нескольких государств. В реальном мире человек физически не может находиться в двух местах одновременно, но сеть, связывающая миллионы компьютеров по всему миру, сделала это реальностью. Преступник, находясь на территории одного государства, может с помощью своего компьютера совершать преступление в другом уголке земного шара. Злоумышленника и его жертву могут разделять тысячи километров, ведь одним из свойств интернет-преступности является ее удаленность.

Не меньшие сложности возникают и при определении субъекта преступления, совершенного с использованием сети. Механизмы действия

¹ Рассолов, И. М. Право и Интернет: теоретические проблемы – 2-е изд., доп. – М.: Норма, 2009. – С. 56.

Интернета таковы, что позволяют совершать различные виды преступлений, не разглашая при этом личные данные, либо выдавая себя за другого человека. Такая анонимность касается не только личности самого преступника, но и его местонахождения. Так или иначе, это зависит от уровня знаний и навыков самого интернет-преступника. В данном случае речь идет об анонимности сетевой преступности. Но помимо этого существуют такие ситуации, когда компьютерная система, распространяющая вирус по сети, сама является носителем вируса, распространение происходит автоматически. Установить личность преступника, когда он отвечает только за запуск зараженного файла в сети и проследить его по всей цепочки, зачастую состоящей из тысячи компьютеров, представляется маловероятным. Это дает ещё один отличительный признак интернет-преступности – ее неперсонофицированность.

Специфика интернет-преступности такова, что для совершения преступления требуется определенный уровень и набор знаний. Пользователь с базовым уровнем владения компьютером вряд ли сумеет осуществить задуманное, но в определенных случаях, умение и опыт могут заменить уже готовые программы, находящиеся в свободном интернет - доступе. Но низкий уровень владения компьютером и непонимание принципов работы Интернета прямо пропорциональны общественной опасности совершенного преступления и, если можно так выразиться, его качеству. Поэтому стоит всё-таки говорить о сугубо интеллектуальном характере интернет-преступности. Это подтверждает и тот факт, что некоторые из интернет-преступников (речь идет о такой группе как хакеры) намеренно демонстрируют свои умственные способности посредством совершения киберпреступлений, считая, что они интеллектуально превосходят не только отдельно взятых компьютерных специалистов различных компаний и организаций, но представителей государственных

служб в той же отрасли. Поэтому интеллектуальный фактор играет большую роль при совершении интернет-преступлений.

Большинство видов преступлений требует от субъекта не только определенных знаний, но и профессиональной принадлежности, достижения возраста уголовной ответственности. Но если совершение «традиционных» видов преступлений сопровождается такими особенностями, то повсеместная интернетизация привела к тому, что возможность совершать преступления получили, к сожалению, получило огромное количество людей, ограниченных в своих социальных или физических возможностях. Ведь основным фактором совершения интернет-преступлений является интеллект и свободное владение компьютером. Именно поэтому чаще всего киберпреступления совершаются несовершеннолетними гражданами. Интернет сделал преступления доступными для людей с невысокими социальными или возрастными возможностями. Теперь для совершения преступления достаточно лишь иметь доступ к Интернету, не задумываясь об орудиях преступления и возможных свидетелях.

Высокий уровень латентности является еще одним свойством Интернет-преступности. Различные ученые называют несколько причин этого явления. На мой взгляд, наиболее очевидной является нежелание самой жертвы обратиться в правоохранительные органы. Зачастую, ущерб от интернет-преступления кажется минимальным по сравнению со временем, нужным для проведения необходимых следственных действий. При этом никаких гарантий, что виновное лицо будет найдено и наказано, нет. Такое поведение связано, несомненно, с правовой неграмотностью и непониманием всех принципов и методик расследования киберпреступлений. Большинство наших сограждан далеки от проблематики компьютерных преступлений и не придает им значения, до тех пор, пока интернет-преступники не причинят им значительный ущерб, тем самым вынудив обратиться за помощью в органы правопорядка. Среди причин высокой латентности интернет-преступности

можно отметить нежелание отдельных пользователей и организаций предоставлять правоохрнительным органам доступ к конфиденциальным данным, тем самым затрудняя дальнейшее расследование преступления. Кроме того латентности способствует постоянное появление новых способов совершения киберпреступлений, различных программ облегчающих совершение таких противоправных деяний. Точно оценить уровень латентности интернет-преступности сложно, препятствием служит само разнообразие преступлений, имеющих различные объекты преступного посягательства и объединенные лишь средством совершения. Также преступления сами по себе не являются очевидными, преступник прилагает все усилия, чтобы скрыть свою личность. Деяние может иметь как длящийся характер, так разовый и одномоментный характер, кроме того преступник может совершать одновременно несколько преступных деяний, посягая на различные объекты.

С повсеместным распространением Интернета в России стремительно увеличивается рост преступлений совершаемых в Интернете. Можно уже говорить о широкой распространенности данного негативного явления.

Отличительной особенностью интернет-преступности, безусловно, является ее транснациональность и трансграничность. Всемирная паутина является идеальным средством для быстрого и относительно безопасного совершения самых различных преступлений. Свойства Интернета таковы, что дают преимущества не только преступникам-одиночкам, но и целым преступным группам, помогая последним добиваться своих преступных целей. При этом члены преступной группы могут проживать в разных странах и даже не знать друг друга по имени, общаясь исключительно с помощью сети Интернет.

Характеризуя объективную сторону данного вида преступлений, следует отметить, что Интернет в зависимости от ситуации становится средством или орудием совершения преступления, но способом совершения

преступного деяния Интернет назвать нельзя. О сети Интернет как о средстве совершения преступного деяния можно говорить тогда, когда она была непосредственно использована преступником для достижения преступного результата. Но при этом компьютерная сеть имеет непосредственную связь со способом совершения преступления в тех случаях, когда она используется в качестве средства их совершения.¹

Но Интернет может рассматриваться не только как средство совершения преступления, но и как орудие. Сущность этих двух понятий не зависит от характера преступлений, но определяется их ролью в совершенных преступлениях. Средства и орудия выступают теми предметами, с помощью которых оказывается преступное влияние на охраняемые уголовным законом общественные отношения. Сеть Интернет рассматривается в качестве средства совершения преступления, в случае если она была использована для облегчения совершения преступного деяния. Тогда как орудием Интернет можно назвать лишь в случае, когда с его помощью совершается преступление. Примером такой ситуации, когда Интернет выступает орудием преступления, может служить интернет-мошенничество, тогда как в случае кражи информации с целью шантажа, Интернет уже выступает средством совершения преступления.

Использовать Интернет преступник может не только при непосредственном совершении преступления, но на его подготовительном этапе. Так, зачастую с помощью сети осуществляется приискание средств и орудий для дальнейшего совершения преступлений уже не связанного с использованием Интернета. Данные случаи не подпадают по категорию интернет-преступлений, так как такого рода преступления предусматривают использование всемирной паутины не раньше, чем на стадии покушения

¹ Чекунов И.Г. Киберпреступность: понятие и классификация // Российский следователь. – 2012. - №2. – С. 43

Стоит также отметить, что при совершении самого общественно опасного деяния посредством Интернета, изменяются и его характеристики. За счет того, что глобальная сеть обладает уникальными возможностями, изменяется качество преступления, что не может не отразиться на степени его общественной опасности.

1.3 Типология интернет-преступлений

Говоря о типологии интернет-преступлений нельзя не обратить внимание на классификацию предложенную И.Г. Чекуновым. Основной особенностью ее конечно является отнесение преступлений совершаемых с помощью компьютерной сети к разряду информационных преступлений. Так или иначе, он выделяет две категории информационных преступлений, отличающихся от других наличием специфического объекта (как основного, так и дополнительного) и способом совершения преступления, предполагающим использование компьютерной сети в качестве средства или орудия преступления. При этом автор учитывает нормы российского уголовного права и вносит в свою классификацию «традиционные» преступления.

Первую категорию составляют преступления так или иначе связанные с незаконным получением, распространением и собиранием конфиденциальной информации, поэтому по большей части это преступления 28 главы Уголовного кодекса («Преступления в сфере компьютерной информации»). Но в эту, же группу входят преступные деяния, в которых в качестве основного или дополнительного объекта выступают общественные отношения в сфере охраны тех или иных сведений. А значит к ним следует отнести преступления против конституционных прав и свобод человека и гражданина, против семьи и несовершеннолетних, в

сфере экономической деятельности, против основ конституционного строя и безопасности государства, а также против порядка управления.

Во вторую категорию можно отнести достаточно широкий круг преступлений, в том числе и преступления против жизни и здоровья граждан.

По мнению А.Ю. Карамнова преступления, совершаемые в сети Интернет и не имеющих непосредственного отношения к ст. 272,273,274 Уголовного кодекса РФ, можно разделить на две группы. К первой относятся те преступления, которые совершаются с непосредственным использованием Интернета и его возможностей. Сюда можно отнести интернет-мошенничество, кибертерроризм, киберсквоттерство с целью вымогательства, криминализированный спам и другие. Вторая группа включает в себя преступления, при совершении которых Интернет использовался как средство, упрощающее злоумышленникам процесс достижения их преступных целей, например, торговля наркотическими веществами, шантаж, распространение порнографических материалов (в том числе и с участием несовершеннолетних), разжигание межнациональной розни.¹

Кроме того, законодатель просто не поспевает за развитием Интернета и поэтому большое количество деяний остается некриминализированным. Наиболее ярким примером является спам, статус которого в современном российском уголовном праве пока не определен.

Использование сети Интернет при совершении преступлений является квалифицирующим признаком многих преступных деяний. Но в большинстве статей Уголовного кодекса законодатель не указывает в диспозиции возможности совершения того или иного преступления посредством всемирной паутины. Тем не менее, на современном этапе

¹ Карамнов, А. Ю. Проблемы квалификации в отношении преступлений, совершенных в глобальной сети Интернет. // Российская академия юридических наук. Научные труды. Выпуск 11. Т. 2. – М., 2011. – С. 667.

развития, данный способ совершения преступных деяний всё чаще используется злоумышленниками.

1. Преступления против жизни и здоровья

На первый взгляд кажется невозможным совершить преступление против жизни или здоровья человека с помощью Интернета. Ещё недавно так и было, но с развитием глобальной сети ситуация изменилась.

В научной литературе достаточно широко известен случай первого официально зарегистрированного факта убийства, посредством сети Интернет, который произошел в феврале 1998 г. в США. Тогда тяжело раненый свидетель преступления был спрятан в закрытом госпитале на территории военной базы. Преступники смогли тогда подключиться к кардиостимулятору и к аппарату искусственной вентиляции легких и изменить режим их работы, что привело к смерти пациента.

Нельзя отрицать, что с развитием высоких технологий, а также с увеличением в нашей жизни количества электронных устройств имеющих доступ в Интернет, возможностей для совершения преступлений только увеличиваются. Способы причинения вреда здоровью и даже лишение жизни посредством Интернета разнообразны и в обозримом будущем их скорее всего только прибавится. Так возможны не только подключения к кардиостимуляторам, системам обеспечения жизнедеятельности, но и к компьютерным системам, установленным в автотранспорте, на борту самолетов или скоростных поездов.

И даже в тех случаях, когда посредством сети не удастся совершить преступление против жизни и здоровья напрямую, преступник всегда сможет воспользоваться широкими возможностями Интернета на подготовительном этапе, для поиска способа и орудия, организации, пособничества и подстрекательства.

Но существует статья, предусматривающая ответственность за угрозу убийством или причинение тяжкого вреда здоровью (ст.119 Уголовного

кодекса РФ). Способы совершения данного преступления различны, но нас больше всего интересует осуществляемый путем передачи сообщений об угрозе убийством или причинением тяжкого вреда здоровью в сети Интернет через социальные сети, электронную почту, систему быстрых сообщений и т.д.

Так, в начале января 2011 г. студент Российской международной академии туризма гр. А. посылал на электронную почту прокурору г. Москвы Юрию Семину письма с угрозами в грубой форме; в послании автор обещал зарезать жертву и его родственников, а расчлененное тело прислать в полицию. По данному факту было возбуждено уголовное дело по ст. 119 УК РФ.¹

Активное развитие социальной составляющей Интернета привело к возникновению такого явления как «культ» самоубийств. Во многом его появлению предшествовал рост зависимости людей от Интернета, мнения интернет-сообщества, особенно это оказало влияние на лиц с неустойчивой психикой и несовершеннолетних. Ст. 110 Уголовного кодекса РФ предусматривает уголовную ответственность за доведение до самоубийства. Это преступление является очень серьезным и, несомненно, заслуживает справедливого наказания, но, к сожалению, данное преступление не всегда выявляется, а доказывание вины по уголовным делам представляется достаточно проблематичным. На сегодняшний день в сети Интернет существует большое количество так называемых «клубов самоубийц», содержащих подробные инструкции и рекомендации для тех, кто решил уйти из жизни. Такие сайты укрепляют в сознании людей понятие нормальности самоубийств, что недопустимо.

На общероссийском уровне доля лиц осужденных к отбытию наказания за совершение данного преступления, как и количество возбужденных дел

¹ Пирожок Е.Д. Способ преступления как наиболее важный элемент криминалистической характеристики угрозы убийством или причинением тяжкого вреда здоровью. // Юрист. – 2013. – С. 14.

невелики. Но, тем не менее, в 2012 году в Российской Федерации уже имел место приговор за доведение до самоубийства посредством использования Интернета.

Анна Семененко – первый в России пользователь, которого осудили по статье «доведение до самоубийства». Девушка онлайн мстила своему бывшему молодому человеку за то, что расстались. Лазаревский районный суд Сочи приговорил обвиняемую к одному году и девяти месяцам лишения свободы. Отбывать наказание 31-летняя Анна Семененко будет в колонии-поселении.¹ Проверка по факту его смерти проводилась достаточно долго. После анализа собранных материалов пришли к выводу, что молодой человек был доведен до самоубийства, и возбудили уголовное дело. Зарегистрировавшись под вымышленными именами в соцсети, женщина начала рассылать сообщения о будто бы нетрадиционной сексуальной ориентации бывшего сожителя. О самоубийстве Голубова она узнала из тех же социальных сетей. Теперь уверяет, что не хотела этого, а просто пыталась заставить его переживать и нервничать. И не могла подумать, что парень «окажется таким мнительным...»²

На фоне роста числа самоубийств в России появление нового способа совершения этого преступления, удручает. Это, несомненно, должно вызвать реакцию законодателя на эту проблему. Наиболее целесообразным представляется дополнение ст. 110 Уголовного кодекса РФ квалифицирующим признаком, так как доведение до самоубийства обладает большей общественной опасностью. Стоит также отметить создание «Единого реестра доменных имен, указателей страниц сайтов в информационно-телекоммуникационной сети «Интернет» и сетевых адресов, позволяющих идентифицировать сайты в информационно-телекоммуникационной сети «Интернет», содержащие информацию,

¹ Официальный сайт 1 канала. Режим доступа: <http://www.1tv.ru/news/social/202707>

² Официальный сайт Российской газеты. Режим доступа: <http://www.rg.ru/2011/12/22/reg-ufo/prigovor-anons.html>

распространение которой в Российской Федерации запрещено», который помогает бороться с информацией популяризирующей самоубийства.¹

Следует отметить, что Интернет по своим свойствам позволяет преступнику охватить своим преступным замыслом неограниченно большой круг людей по всему миру. Кроме того глобальная сеть дает чувство уверенности в собственной безнаказанности, своеобразную психологическую защиту, что не может не создавать проблемы для привлечения интернет-преступников к ответственности. Но, на мой взгляд, говорить о широком распространении совершения преступлений против жизни и здоровья посредством Интернета, говорить пока рано.

2. Преступления против свободы, чести и достоинства личности

Безграничные возможности в доставке информации и распространении информации, анонимность и широкая аудитория сделало Интернет по сути универсальным средством массовой информации. Но отсутствие наблюдения и контроля со стороны органов государственной власти привело к «гипертрофированности» свободы слова. Каждый интернет-пользователь считает своим законным правом высказаться, не задумываясь при этом о последствиях своих слов. Очень часто тем или иным способом появляется информация, в социальных сетях, форумах, блогах, потенциально опасная, содержащая оскорбительные и клеветнические сведения.

Объективную сторону ст. 128.1 «Клевета» составляет распространение заведомо ложных сведений, порочащих честь и достоинство другого лица или подрывающих его репутацию, совершенных в любой форме: устно, письменно или в виде изображения. Интернет дает преступнику просто уникальную возможность распространить данную информацию, причем масштаб распространения сопоставим только с теми же данными обнародованными с помощью средств массовой информации. Интернет ничем не уступает телевидению, радио или газетам, он превосходит их в

¹ РЕЕСТР???

скорости, в количестве аудитории. Возможность опубликования клеветнических сведений анонимно затрудняет поиск виновного лица, можно только предполагать какой эффект будет иметь клевета распространенная через социальные сети. Интернет-преступники часто не ограничиваются одними лишь ложными сведениями в письменной форме, в сети публикуются сфабрикованные клеветнические аудио - и видеоматериалы.

Сведения, распространяемые через Интернет, становятся достоянием широкого круга лиц, что говорит о весьма высокой общественной опасности клеветы и оскорбления, осуществленных таким способом.¹ Введение нового квалифицирующего признака в эту статью необходимо, так как вред, нанесенный репутации жертвы преступлением, совершенным посредством Интернета больше, нежели в других, указанных законодателем, случаях.

3. Преступления против конституционных прав и свобод человека и гражданина

Интернет прочно проник во все сферы нашей жизни. Люди уже настолько привыкли к нему, что доверяют социальным сетям и блогам конфиденциальную информацию, тем самым провоцируя совершение в отношении них преступлений. Кроме того, данные хранящиеся на компьютерах жертв, переписка по электронной почте также становится предметом преступного посягательства. Преступления, предусмотренные ст. 137 и 138 Уголовного кодекса РФ («Нарушение неприкосновенности частной жизни» и «Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений») получили новый, более быстрый и выгодный, способ совершения.

Объективная сторона преступления предусмотренного ст. 137 Уголовного кодекса РФ содержит в себе два тождественных действия:

- Собираение сведений означает, что виновный тайно или открыто, знакомится с документами, письмами и другими источниками информации в

¹: Королева М.М. Клевета и оскорбление в сети Интернет // Законность – 2010. - № 7. - С.52.

доме потерпевшего, на его работе или у его близких родственников. Характерной деталью является то, что документы (письменные или печатные), виновным не изымаются, а остаются на месте их хранения, то есть используется лишь содержание документов. Интернет как ничто другое подходит для осуществления данного преступления.

- Распространение сведений о частной жизни потерпевшего означает сообщение их хотя бы одному лицу, заинтересованному или незаинтересованному в получении таких сведений. Осуществляется распространение различными способами: устно, письменно. Но диспозиция статьи выделяет: публичное выступление, публичная демонстрация произведения (кинофильма, видеоролика), через средства массовой информации. Интернет в качестве средства совершения преступления прямо законодателем не указан, но такой вариант развития событий возможен.¹

Повсеместная интеграция компьютерной сети (в том числе и на мобильных телефонах) помогает перехватить сообщения любого вида. Преступник, проникая в компьютер потерпевшего, начинает контролировать все коммуникации своей жертвы.

Россия является одним из мировых лидеров по количеству совершаемых преступлений, связанных с нарушением авторских и смежных прав. Уголовный кодекс РФ содержит в себе ст. 146, предусматривающую ответственность за это преступление. Простота распространения информации по сети, малая степень контроля со стороны государственных органов стали благодатной почвой для процветания интернет-пиратства. Но в данном случае нельзя винить одних только интернет-пиратов. Спрос рождает предложение, а значит простые граждане, ежедневно скачивающие с интернет-ресурсов нелегальный контент виноваты не меньше.

¹ Уголовное право. Особенная часть: учебник / отв. ред. И. Я. Козаченко, Г. П. Новоселов. – 4-е изд., изм. и доп. – М.: Норма, 2008. – С. 177 – 178.

Эта статья впервые вводит в понятие «интеллектуальной собственности» - охраняемые законом результаты творческой деятельности человека в любой сфере, независимо от назначения и достоинства произведения. В законе это называется объектами авторского права, которое распространяется как на обнародованные произведения, так и на необнародованные, но существующие в какой-либо объективной форме: письменной, устной, аудио-, видеозаписи, объемно-пространственной (скульптура, картина и т.д.).¹

Единственным требованием для распространения с помощью Интернета является его электронный формат. Товар должен быть оцифрован. Неизменно популярными для скачивания и распространения в сети остаются кинофильмы, музыкальные произведения, тексты книг и компьютерные программы. Интернет-пиратство распространилось так сильно, что говорить об установлении контроля над громадным количеством непрерывно скачиваемых и загружаемых файлов, пока говорить не приходится. Именно поэтому большинство файлов скачивается в обход отчисления авторам денежных средств, а в случае крупного и особо крупного ущерба автору или иному правообладателю, наступает ответственность по ст. 146 Уголовного кодекса РФ.

Но для того чтобы распространять нелегальный контент совершенно не обязательно выкладывать его в Интернет. Уже достаточно давно существуют специальные торрент-трекеры для файлообмена, где пользователи предлагают документы для обмена. В некоторых странах Европы, например, в Швеции, торрент-трекеры были приравнены к пиратским сайтам, однако в России привлечь владельцев торрент-трекеров к ответственности крайне затруднительно, так как на трекерах файлы не хранятся, а наше

¹ Уголовное право. Особенная часть: учебник / отв. ред. И. Я. Козаченко, Г. П. Новоселов. – 4-е изд., изм. и доп. – М.: Норма, 2008. –С.189.

законодательство предусматривает наказание за распространение нелегальной продукции.¹

Нарушение авторских и смежных прав в сети Интернет включает в себе большую опасность, так как незаконно сделанные копии распространяются интернет-пиратами по всему миру, причиняя серьезный экономический вред. Не стоит забывать, что кроме авторов и иных правообладателей, в создании кинофильма, может также принимать участие государство, а соответственно рассчитывать на часть прибыли полученной от продаж. Но из-за активной деятельности интернет-пиратов, государство несет убытки, как это часто происходит с отечественным кинематографом. Из вышесказанного следует сделать вывод о необходимости введения квалифицирующего признака «совершенное посредством информационно-коммуникационной сети (в том числе Интернета)».

4. Преступления против семьи и несовершеннолетних

Дети наравне со взрослыми имеют доступ к Интернету, при помощи которого ребенок или подросток может быть вовлечен в совершение преступных деяний. Ответственность за вовлечение несовершеннолетних в совершение преступления предусматривается ст. 150 Уголовного кодекса РФ. Объективную сторону данного преступного деяния образует совершение преступником действия, направленного на вовлечение несовершеннолетнего гражданина в преступление путем обещаний, обмана, угроз (кроме применения насилия) или иным способом оказывающего на него воздействия. Все эти альтернативные действия могут осуществляться преступником не только при непосредственном, но и при удаленном контакте. Действуя через Интернет, преступник сохраняет свою анонимность, снижает риск раскрытия своей личности, а так же значительно облегчает себе задачу, прежде всего в поиске несовершеннолетнего.

¹ Вилинов, А. Практика регулирования отношений, связанных с незаконным использованием объектов авторского и смежных прав в сети Интернет, в США, России и ряде стран // Интеллектуальная собственность : Авторское право и смежные права. – 2010. – № 12. – С. 54.

Интернет позволяет виновному найти и установить контакт с психологически неустойчивым несовершеннолетним лицом, не знающим о возможной противоправности предлагаемых к совершению действий, либо наоборот желающих принять участие в совершении преступления.

Как бы то ни было, опытный киберпреступник без особого труда заинтересует и привлечет несовершеннолетнего к совершению преступления, продемонстрировав возможности, предоставляемые взломом интернет-сайта или программы.

Кроме того, Интернет может стать подспорьем в вовлечении несовершеннолетнего в совершение антиобщественных действий, ответственность за которые предусмотрена ст. 151 Уголовного кодекса РФ. В сети достаточно легко наткнуться на пропаганду или одобрения употребления спиртных напитков, психотропных веществ, что может привести к возникновению у несовершеннолетних совершить данные действия.

Опубликование в Интернете материалов подобного содержания позволяет достигать неограниченно большой аудитории, и попытки вовлечения в антиобщественные или преступные действия, несомненно, оказывают значительный вред. И чем популярнее ресурс, разместивший у себя такую информацию, тем больше шансов, что призывы подобного рода дойдут до своих целей. Для предотвращения совершения подобных преступлений действий только со стороны правоохранительных органов недостаточно. Необходима помощь общественности, в том числе родителей.

5. Преступления против собственности

Одним из самых распространенных преступлений во всемирной сети несомненно является интернет-мошенничество. Такая популярность хищения чужого имущества путем обмана или злоупотребления доверием с помощью Интернета объясняется достаточно просто. Интернет не только дает злоумышленнику анонимность, но и возможность выдать себя за совершенно

другого человека, тем самым изменив возраст, социальный статус и другие личные данные. Эти действия дают значительное преимущество интернет-преступнику по сравнению с обычным мошенником. Кроме того, Интернет открывает бесконечное множество способов и возможностей получить денежные средства обманным путем. Сеть облегчает поиск жертв, зачастую они сами находят злоумышленника, отвечая на электронные сообщения разосланные последним, позволяет ввести в заблуждение, осуществить незаконную финансовую операцию. Интернет может быть использован практически на всех стадиях большинства преступлений против собственности, за исключением сопряженных с насилием.

В 2012 году в Уголовный кодекс РФ была введена ст. 159.6 предусматривающая ответственность за совершение мошенничества в сфере компьютерной информации, то есть хищения чужого имущества или приобретения 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.¹

Н.Л. Коликов в своей статье приводит определение интернет-мошенничества данное А.А.Комаровым – 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» системы), а также корыстной мотивацией преступной деятельности.²

Интернет во многом облегчил совершение преступлений, и мошенничество не исключение. Глобальная сеть дает практически 100-

¹ «Уголовный кодекс Российской Федерации» (ред. от 05.04.2013) // СПС Консультант Плюс. - 2017.

² Коликов, Н. Л. Профессиональная компьютерная преступность и мошенничество. // Вестник Южно-Уральского государственного университета. – 2011. – Выпуск 28. – № 40. – С. 62.

процентную конфиденциальность преступника. Анонимность в сети имеет тесную связь со свободой доступа в Интернет, а специфика работы Интернета обеспечивает оперативность действий: за считанные мгновения сообщения достигают своих жертв, осуществляются электронные платежи в пользу злоумышленников.

Неиссякаемым источником заработка для интернет-мошенников являются социальные сети. Это связано с огромным числом пользователей и тем фактом, что администрация такого рода сетей не несет ответственность за содержание материалов, размещаемых на пользовательских страницах, а значит и за их сохранность и никак не защищает своих пользователей от возможных преступных посягательств. А интернет-мошенники тем временем, чуть ли не ежедневно находят новые схемы обмана, в результате которых жертва сама отдает преступникам свои денежные средства.

О.С. Гузеева приводит примеры наиболее распространенные схемы интернет-мошенничества:

1) схема «увеличить и сбросить» (Pump&dump) - вид рыночной манипуляции, заключающейся в извлечении прибыли за счет продажи ценных бумаг, спрос на которые был искусственно сформирован. Первоначально создается повышенный спрос на определенные ценные бумаги, затем осуществляется их продажа по завышенным ценам. После совершения подобных манипуляций цена на рынке возвращается к своему исходному уровню, а рядовые инвесторы оказываются в убытке;

2) схема финансовой пирамиды (Pyramid Schemes) при инвестировании денежных средств с использованием интернет-технологии полностью повторяет классическую финансовую пирамиду. Инвестор получает прибыль исключительно за счет вовлечения в игру новых инвесторов;

3) схема «надежного» вложения капитала (The «Risk - free» Fraud) или «инвестиционная схема» заключается в распространении через Интернет инвестиционных предложений с низким уровнем риска и высоким уровнем

прибыли. Например, вложение в якобы высоколиквидные ценные бумаги неизвестных компаний;

4) «экзотические» предложения (Exotic Offerings), например, распространение через Интернет предложения акций коста-риканской кокосовой плантации, имеющей контракт с сетью американских универмагов и гарантирующей получение сверхдоходов;

5) мошенничества с использованием банков (Prime Bank Fraud) заключаются в том, что мошенники, прикрываясь именами и гарантиями известных и респектабельных финансовых учреждений, предлагают инвесторам вложение денег в ничем не обеспеченные обязательства с нереальными размерами доходности;

6) фишинг (Fishing) - вид интернет-мошенничества, цель которого - получить данные, содержащиеся на пластиковой карте. Злоумышленники рассылают электронные письма от имени банков или платежных систем. Пользователю предлагается зайти на сайт, который является точной копией настоящего сайта банка. Для дальнейшей возможности использовать пластиковую карту владельца просят указать пин-код и личные данные, содержащиеся на карте. Впоследствии эти данные используются для изготовления поддельной пластиковой карты и обналичивания денежных средств;

7) интернет-попрошайничество. В Интернете могут появиться объявления, например, от благотворительной организации с просьбой о материальной помощи больным детям. Злоумышленники создают сайт-дублер, который является точной копией настоящего, и меняют реквизиты для перечисления денег;

8) аукционы и розничная торговля в режиме онлайн. Отличительная черта этого вида мошенничества - низкая цена на определенный товар и отсутствие фактического адреса или телефона продавца. В этом случае

предлагается подделка, некачественный товар либо деньги покупателей просто присваиваются, а товар не доставляется.¹

6. Преступления в сфере экономической деятельности

Интернет обеспечил простую и дешевую платформу для создания интернет-сайтов, как следствие открыть свое дело в сети не составляет труда. В интернете стали день ото дня открываться новые интернет-магазины, сайты по оказанию интернет-услуг и т.д. отсутствие контроля со стороны государственных органов зачастую приводит к тому, что преступники начинают осуществлять предпринимательскую деятельность, не имея на то соответствующего разрешения. Об оплате налогов и говорить не приходится. При этом данная незаконная деятельность ведется не только в сфере предпринимательства (ст. 171 Уголовного кодекса РФ), но и в сфере банковской деятельности (ст. 172 171 Уголовного кодекса РФ).

Объективную сторону преступления в сфере банковской деятельности могут составлять осуществление банковских операций без регистрации и без специального разрешения (лицензии), когда таковые являются обязательными, с помощью систем оборота денежных средств в Интернете (PayPal, WebMoney и др.). В Интернете существует огромное количество сайтов, предлагающих свои посреднические услуги в финансовых операциях без каких-либо специальных разрешительных документов или регистрации. Очень популярны обменные пункты, позволяющие вывезти денежные средства за границу без оформления документов и уведомления соответствующих органов, или обменять валюту. Такое положение вещей, когда контроль со стороны государственных органов снижен, провоцирует совершение новых преступлений, например легализацию денежных средств, приобретенных преступным путем (ст. 174, 174.1 Уголовного кодекса РФ), организация и проведение азартных игр в Интернете (ст. 192.1 Уголовного

¹ Гузеева, О. Квалификация мошенничества в российском сегменте сети интернет // Законность. – 2013. – № 3. – С. 22.

кодекса РФ), невозвращение средств в иностранной валюте из-за рубежа (ст. 193 Уголовного кодекса РФ), не говоря уже об уклонении от уплаты налогов (ст. 198, 199 Уголовного кодекса РФ).¹

Интернет дает возможность совершать финансовые операции в считанные мгновения, не оставляя при этом не только бумажных, но и электронных следов, чем и пользуются интернет-преступники. Часто возникают проблемы с определением с идентификацией личности преступника и отслеживанием компьютера, с которого производились незаконные операции с денежными средствами.

Злоумышленники могут также использовать Интернет для совмещения двух различных видов преступлений. Нередки случаи оплаты порнографического материала за рубежом с помощью системы виртуальных платежей PayPal. Таким образом, всемирная паутина позволяет интернет-преступнику, совершающему преступные деяния предусмотренные Главой 22 Уголовного кодекса РФ, игнорировать государственные границы.

Ст. 185.3 Уголовного кодекса РФ предусматривает ответственность за манипулирование рынком. Объективная сторона данного преступления предусматривает умышленное распространение виновным лицом заведомо ложных сведений с помощью средств массовой информации, в том числе и электронных, информационно-коммуникационных сетей (Интернета), если в результате незаконных действий цена, спрос, предложение или объем торгов финансовыми инструментами, иностранной валютой и (или) товарами отклонились от уровня или поддерживались на уровне, существенно отличающемся от того уровня, который сформировался бы без учета указанных выше незаконных действий.

7. Преступления против общественной безопасности

¹ Комментарий к Уголовному кодексу Российской Федерации / Отв. ред. В.М. Лебедев. – М.: Юрайт-Издат, 2010. – С. 67.

Интернет уже проник во все сферы общественной жизни, но с его появлением возникла одна из наиболее опасных разновидностей киберпреступности - кибертерроризм.

В Интернете терроризм развивается стремительно, поскольку сеть - это идеальная среда для его развития и распространения. Отсутствие цензуры приводит к распространению информации, изображений, угроз или сообщений независимо от их законности или потенциального воздействия на человеческое сознание.

Кибертеррористы используют открытость Интернета для своих целей: дискредитации правительств и государств, размещения сайтов террористической направленности, порчи и разрушения ключевых систем (путем внесения в них фальсифицированных данных или постоянного вывода этих систем из строя). Это в свою очередь порождает страх или тревогу среди населения, и является дополнением к традиционному виду терроризма. Данные преступные деяния предусмотрены ст. 205, 205.1, 205.2 Уголовного кодекса РФ.

Ежегодно МВД России выявляется около 150 ресурсов, содержащих материалы террористической и экстремистской направленности. Больше всего подобных сайтов было обнаружено в российском сегменте сети, их оказалось более 70. Мониторингом интернет-пространства круглосуточно занимаются специализированные подразделения МВД России, в соответствии с законодательством закрываются сайты с негативным контентом, а лиц, размещающих на них информацию, привлекают к уголовной ответственности. Однако около 15% закрытых сайтов появилось вновь под другими именами на хостинговых ресурсах как российских, так и зарубежных провайдеров. Чаще всего сайты, вытесненные из российского сегмента сети, мигрируют в другие страны. Поэтому повышение уровня международного сотрудничества в данной сфере представляется весьма актуальным. Во многом положительные результаты противодействия

международной компьютерной преступности достигнуты благодаря постоянно проводимой МВД России работе по развитию взаимодействия с правоохранительными органами государств - участников СНГ.¹

Тем не менее, Интернет создает для террористических организаций ряд преимуществ в отношении вербовки, финансирования террористической деятельности, дезинформирования о планируемых актах терроризма, так и непосредственно для совершения самих террористических актов. Основные характеристики всемирной паутины как глобальность, анонимность, трансграничность делают его не только удобным, но и доступным инструментом в руках террористов. При этом не имеет значение, о каком терроризме идет речь, о внутригосударственном или международном.

Интернет может применяться для совершения таких преступлений как: организация массовых беспорядков (ст. 212 Уголовного кодекса РФ); незаконные операции (в данном случае приобретение) оружия, его основных частей, боеприпасов, взрывчатых веществ и взрывных устройств (ст. 222 Уголовного кодекса РФ).

Глобальная сеть может послужить средством распространения информации, необходимой для незаконного изготовления оружия (ст. 223 Уголовного кодекса РФ).

Использование Интернета при совершении преступных деяний многократно увеличивает их общественную опасность. Что касается преступлений связанных с террористической деятельностью, то использование сети может привести к непоправимым последствиям.

8. Преступления против здоровья населения и общественной нравственности.

¹ Паненков А.А. Предложения по оптимизации борьбы с использованием сети Интернет в террористических целях // Правовые вопросы связи. – 2011. – №2. – С. 17.

При совершении преступлений, предусмотренных Главой 25 Уголовного кодекса РФ, также возможно применение сети Интернет для достижения преступных целей.

Пропаганда наркомании стала неотъемлемой частью сети Интернет. Огромное количество сайтов публикуют на своих страницах технологию изготовления наркотических препаратов в домашних и промышленных условиях, инструкции по употреблению или просто предлагают купить наркотические вещества через Интернет.

Ст. 230 Уголовного кодекса РФ предусматривает ответственность за склонение к потреблению наркотических средств, психотропных веществ и их аналогов.¹ Представляется целесообразным ввести квалифицирующий признак, прямо указывающий на возможность совершения данного преступления посредством сети «Интернет».

Но не только популяризация наркомании является опасной для здоровья населения и общественной нравственности. Большой резонанс в обществе вызывают преступления связанные с проблемой педофилии. Особое внимание следует уделить преступлениям ей сопутствующим: изготовлению и обороту материалов или предметов с порнографическими изображениями несовершеннолетних (ст. 242.1 Уголовного кодекса РФ) и использование несовершеннолетнего в целях изготовления порнографических материалов или предметов (ст. 242.2 Уголовного кодекса РФ), совершенным с использованием Интернета.

Порнобизнес получил широкое распространение в сети, и является одним из самых прибыльных видов преступной деятельности. Всемирная паутина позволяет злоумышленникам размещать рекламу, распространять порнографические материалы, принимать электронные платежи, а также значительно облегчает поиск «исполнителей» и координацию преступной группы.

¹ Уголовный кодекс Российской Федерации (ред. от 17.04.2017) // СПС Консультант Плюс. - 2017.

Сеть точно также используется и при незаконном изготовлении и обороте порнографических материалов или предметов (ст. 242 Уголовного кодекса РФ).

В октябре 2012 года был принят документ, регулирующий деятельность «Единый реестр доменных имен, указателей страниц сайтов в информационно-телекоммуникационной сети «Интернет» и сетевых адресов, позволяющих идентифицировать сайты в информационно-телекоммуникационной сети «Интернет», содержащие информацию, распространение которой в Российской Федерации запрещено» или как его окрестили в народе – «Черный список сайтов».

Основной функцией Реестра является выявление и пресечение (путем блокировки) сайтов, содержащих запрещенный контент, а именно:

- материалов с порнографическими изображениями несовершеннолетних и (или) объявлений о привлечении несовершеннолетних в качестве исполнителей для участия в зрелищных мероприятиях порнографического характера, распространяемых посредством сети «Интернет»;

- информации о способах, методах разработки, изготовления и использования наркотических средств, психотропных веществ и их прекурсоров, местах приобретения таких средств, веществ и их прекурсоров, о способах и местах культивирования наркосодержащих растений и о способах совершения самоубийства и призывов к совершению самоубийства, размещенной в продукции средств массовой информации, распространяемой посредством сети «Интернет».¹

9. Преступления в сфере компьютерной информации

¹ Постановление Правительства Российской Федерации от 26.10.2012 № 1101 «О единой автоматизированной информационной системе «Единый реестр доменных имен, указателей страниц сайтов в информационно-телекоммуникационной сети «Интернет» и сетевых адресов, позволяющих идентифицировать сайты в информационно-телекоммуникационной сети «Интернет», содержащие информацию, распространение которой в Российской Федерации запрещено» // СПС Консультант плюс. – 2017.

Составы, предусмотренные Главой 28 Уголовного кодекса, являются новеллой в российском уголовном праве и обеспечивают защиту общественных отношений в сфере компьютерной информации. Неправомерный доступ к компьютерной информации (ст. 272 Уголовного кодекса РФ) может совершаться и без глобальной сети, но появление Интернета вывело преступление на новый уровень, значительно облегчив злоумышленнику его совершение. При этом, «жертвой» преступления может стать любой компьютер, от простого пользовательского, до находящегося в собственности государственного органа.

Создание, использование и распространение вредоносных программ (ст. 273 Уголовного кодекса РФ) тоже стало возможным только с появлением компьютеров, но, как и преступление предусмотренной ст. 272 Уголовного кодекса РФ, наибольший вред оно наносит именно посредством Интернета. Под вредоносной программой (вирусом) следует понимать программу преднамеренно и без санкции соответствующих лиц изменяющую хранящиеся на компьютере данные и программы.¹

Более чёткие критерии, по которым программы могут быть отнесены к категории вредоносных программ, до настоящего времени нигде конкретно не оговорены. Соответственно, для того, чтобы утверждение о вредоносности программы имело юридическую силу, необходимо проведение программно-технической экспертизы с соблюдением всех установленных действующим законодательством формальностей.

Но наибольшей опасностью являются вирусы способные к самораспространению и самовоспроизводству. Такого рода вредоносные программы могут быть использованы при совершении различного рода преступных деяний, предусмотренных ст. 105, 128.1, 137, 138, 205, 281 Уголовного кодекса РФ.

¹ Козаченко И.Я, Новоселов Г.П. Уголовное право. Особенная часть: учебник. – М.: Норма, 2008. –С. 743.

Использование вредоносных программ может причинить вред как обществу так и государству, поэтому в ст. 272 и 273 Уголовного кодекса РФ следует дополнить квалифицирующим признаком «совершенное посредством информационно–телекоммуникационной сети Интернет».

Объективная сторона преступления предусмотренного ст.274 Уголовного кодекса РФ характеризуется нарушением правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации либо информационно-телекоммуникационных сетей и окончного оборудования, а также правил доступа к информационно-телекоммуникационным сетям.¹ К такому виду нарушений можно отнести: несоблюдение общих средств защиты информации, а также нарушение режима эксплуатации.²

10. Преступления против конституционного строя и безопасности государства

Интернет дал преступникам возможность нелегально заполучить не только конфиденциальную информацию частных лиц и организаций, но и сведения, составляющие государственную тайну. С появлением Интернета значительно возросла общественная опасность преступлений, предусмотренных Главой 29 Уголовного кодекса РФ. Непосредственно с помощью Интернета могут совершаться: государственная измена (ст. 275 Уголовного кодекса РФ), шпионаж (ст. 276 Уголовного кодекса РФ), публичные призывы к осуществлению экстремистской деятельности (ст. 280 Уголовного кодекса РФ), диверсия (ст. 281 Уголовного кодекса РФ), возбуждение ненависти либо вражды, а равно унижение человеческого достоинства (ст. 282 Уголовного кодекса РФ), разглашение государственной тайны (ст. 283 Уголовного кодекса РФ), утрата документов содержащих государственную тайну (ст. 284 Уголовного кодекса РФ). Целесообразно

¹ «Уголовный кодекс Российской Федерации» (ред. от 17.04.2017) // СПС Консультант Плюс - 2017.

² Лебедев М.В. Комментарий к Уголовному кодексу Российской Федерации – М.: Юрайт-Издат, 2010. – С. 456.

дополнить эти статьи, указав, что данные преступные действия могут быть совершены посредством использования информационно-коммуникационных сетей. При совершении остальных преступных деяний предусмотренных этой главой, Интернет может быть использован преступниками на подготовительной стадии.

Таким образом, из всего вышеперечисленного можно сделать следующие выводы:

- Интернет-преступность явление распространенное и разнообразное, охватывающие практически все Главы Особенной части Уголовного кодекса РФ;
- Интернет благодаря своим характеристикам, значительно увеличивает общественную опасность совершаемых преступлений;
- Он может быть использован как для непосредственного совершения преступления, так и на стадии подготовки;
- Интернет может быть использован не только для облегчения реализации задуманного преступного деяния, но и для сокрытия следов уже совершенного преступления;
- Возрастает общественная опасность самого преступника, т.к. использование при совершении преступлений Интернета, вызывает у злоумышленника чувство безнаказанности;
- Глобальная сеть предоставляет преступникам возможность избежать заслуженного наказания и общественного порицания.

Так же следует отметить необходимость включения в некоторые составы квалифицирующего признака «совершенное с помощью сети Интернет», о которых было сказано выше. При условии, если Интернет не только увеличивает степень общественной опасности, но и является типичным способом совершения данного вида преступления. На мой взгляд, данное изменение наиболее необходимо в ст. 110, 128.1, 137, 138, 146, 150, 151, 174, 174.1, 205.1, 205.2, 230, 242, 272, 273, 280 Уголовного кодекса РФ.

Подводя итог, нужно отметить, что законодателю не стоит игнорировать интернет-преступность и уделить данным преступлениям больше внимания, а также постараться усовершенствовать нормативно-правовую базу в вопросах регулирования отношений, возникающих в сети Интернет.

2 КРИМИНАЛИСТИЧЕСКАЯ ХАРАКТЕРИСТИКА ИНТЕРНЕТ-ПРЕСТУПНОСТИ

2.1 Интернет-преступность в России. Криминологический анализ наиболее проблемных видов интернет-преступлений

Главное значение в анализе того или иного вида преступности, является ее состояние, структура и тенденции развития. Интернет-преступность не является исключением.

При изучении данного вопроса, нужно учесть следующие факторы:

1. Высокая латентность;
2. Отсутствие данных статистики по интернет-преступности, так как в Российской Федерации официально ведется только статистика преступлений в сфере компьютерной информации.

Именно на данные последней приходится опираться при анализе состояния интернет-преступности в России. Безусловно, эти сведения крайне малы, а по мнению некоторых ученых, не отражают реальную картину событий. С этим сложно не согласиться, но не стоит забывать, что статистические данные не устраивают ученых вне зависимости от видовой принадлежности преступления. Кроме того, количественные характеристики могут дать общее представление о тенденции развития интернет-преступности в современной России.

Также стоит отметить, что преступления предусмотренные Главой 28 Уголовного кодекса РФ, могут совершаться и без применения сети Интернет, поэтому присутствует определенная погрешность. Но глобальная сеть применяется при совершении данных преступлений чаще всего, поэтому статистические данные могут быть использованы для оценки свойств российской интернет-преступности.

Таблица 1

Динамика преступлений, совершенных в сфере телекоммуникаций и компьютерной информации, зарегистрированных в Российской Федерации, и число интернет-пользователей за период 2009-2012 гг.

	2009	2010	2011	2012
Абсолютный показатель	17 535	12 698	7 974	10 227
Темп прироста, к АППГ (%)	-	27,6	37,2	28,3
Число интернет-пользователей (млн. чел.)	53,5	59,7	60,4	68,0

Мы можем проследить тенденцию снижения общего количества зарегистрированных преступлений, в период с 2009 по 2011 гг. По мнению автора эти данные не могут адекватно отразить складывающуюся на тот промежуток времени ситуацию. Подобные процессы могут быть объяснены как проводимой реформой в органах внутренних дел, которая привела к ослаблению контроля учетно-регистрационной дисциплины, так и снижением активности правоохранительных органов по выявлению преступлений данного вида., поскольку факторы влияющие на совершение компьютерных преступлений не уменьшились, а только еще больше увеличились. Также необходимо отметить, что рост преступлений в 2012 году напрямую связан с увеличением числа интернет-пользователей до 68 млн. по сравнению с 2011 годом (60,4 млн.).

Автор также полагает, что сокращение количества преступлений в 2009-2011 гг. носит искусственный характер, о чем свидетельствует

наглядное сравнение динамики зарегистрированных преступлений в сфере компьютерной информации и число интернет-пользователей за вышеуказанный период.

Как уже отмечалось ранее одной из важных особенностей российской интернет-преступности является высокая степень ее латентности. По оценкам экспертов, она составляет более 90%. Но не стоит, на мой взгляд, утверждать, что это проблема исключительно Российской Федерации. Отнюдь, нет, не менее высокий процент латентности можно наблюдать в странах Европы (Великобритания – 85%, ФРГ – 75 %) и США – 80%, в которых, тем не менее, давно ведут активную борьбу с интернет-преступниками. Это не говорит о бесполезности противодействия киберпреступлениям, вопрос скорее в эффективности мер борьбы, о которых будет рассказано позднее.

Причинами латентности можно назвать:

- не обращение жертв интернет-преступлений в органы правопорядка;
- высокий уровень профессионализма интернет-преступников.

Такое положение дел, несомненно, ухудшает общее состояние интернет-преступности.

Не стоит забывать тот факт, что сумма ущерба, наносимого преступлениями в сфере компьютерной информации значительна по отношению к другим составам преступлений Уголовного кодекса РФ.

По неполным оценкам экспертов, мировая преступность данного профиля приносит ущерб в 200 млрд. долларов ежегодно. Компьютерный преступник, ни чем, по сути, не рискуя, может получить 1 млн. В России же средний ущерб, причиняемый потерпевшему одним совершенным в отношении него компьютерным преступлением, может достигать 1,7 млн. рублей.

В России самые богатые хакеры, по сравнению с другими государствами.оборот рынка компьютерной преступности достигает 1 млрд.

долларов в год. Востребованному и обладающему высокими навыками хакеру, его преступная деятельность приносит от 30 и более млн. рублей в год. При этом самыми прибыльными считаются рассылка спама, кража конфиденциальной информации и Ddos атаки, призванные блокировать работу интернет-сайтов. В 2012 году правоохрнительными органами были выявлены 889 преступлений, предусмотренных ст. 273, тогда как в 2011 – 693 преступления. Это свидетельствует, на мой взгляд, о быстром развитии профессиональной и организованной компьютерной преступности в России.¹

Говоря о состоянии интернет-преступности в России нельзя не затронуть наиболее проблемные и актуальные преступления, с которыми уже сейчас нужно активно бороться, иначе последствия могут быть еще хуже

1. Наркопреступность

Проблема наркомании с возникновением и повсеместным распространением Интернета приобрела глобальный характер и угрожающий масштаб. И если в XX веке преступления такого вида требовали борьбы исключительно на национальном уровне, то сейчас это уже преступность международного характера, развитию которой поспособствовал в том числе и Интернет. А значит бороться с данной преступностью, следует на государственном уровне.

На мой взгляд можно выделить два аспекта, отличающих наркопреступность в сети Интернет.

Во-первых это пересечение активно развивающихся банковских и финансовых технологий, и преступного наркотрафика. Интернет стал удобным пространством для осуществления сделок по купле – продаже наркотических средств, психотропных веществ и их аналогов. Сеть позволяет лицам, заинтересованным в их распространении быстро и анонимно устанавливать контакты между производителями и сбытчиками готовой

Чирков Д.К., Саркисян А.Ж. Преступность в сфере высоких технологий: тенденции и перспективы // Национальная безопасность. - 2013. - № 2. -С. 165.

наркотической продукции, договариваясь о сроках, поставках, культивации, технологии производства, транспортировке. Эта переписка, обмен информации зачастую ведутся в зашифрованном виде.

Оплата производится с помощью электронных платежных систем, чаще всего находящихся за пределами Российской Федерации, что в значительной степени затрудняет выявление данных фактов и дальнейшее пресечение преступного деяния.

Во-вторых, Интернет стал витриной магазина и простейшим инструментом привлечения клиентуры, в руках преступников. Наиболее удобным способом поиска информации о продаже или изготовлении наркотических средств, конечно, являются интернет-поисковики, с помощью которых любой желающий может найти нужную ему информацию. И не смотря на появление «Единого реестра доменных имен, указателей страниц сайтов в информационно-телекоммуникационной сети «Интернет» и сетевых адресов, позволяющих идентифицировать сайты в информационно-телекоммуникационной сети «Интернет», содержащие информацию, распространение которой в Российской Федерации запрещено», количество интернет-ресурсов, предоставляющих подобную информацию, достаточно велико. По моему мнению, социальные сети играют немаловажную роль в распространении наркотических средств и психотропных веществ. Социальная сеть «Вконтакте» наиболее яркий тому пример. Ее аудитория включает в себя большое число подростков, и они попадают в группу риска. Особой популярностью среди молодежи пользуются так называемые «легкие наркотики», хотя законодатель не делит наркотические вещества по такому признаку, так как они в любом случае оказывают негативное влияние на организм.

Большую роль для выявления сайтов с запрещенным контентом играет реакция простых интернет-пользователей, а также социальный контроль со стороны родителей. Чем чаще они будут обращать внимание на появление

информации подобного рода, и сообщать в правоохранительные органы, тем оперативнее будут действовать последние.

Но, к сожалению, нельзя исключить возможность нахождения, например, инструкции по изготовлению наркотического средства в домашних условиях через иностранный сайт, вне юрисдикции Российской Федерации, поэтому не следует забывать и о международном сотрудничестве против распространения сетевой наркопреступности.

Отсутствие уголовной ответственности за рекламу, пропагандировании наркомании не может положительно сказать на общей картине состояния наркопреступности в России. Данные деяния несут в себе большую общественную опасность и применение норм административного права не достаточно. Противодействие наркотизму и распространению наркопреступности является одним из наиболее важных направлений российской уголовной политики, поэтому сетевая наркопреступность не должна оставаться вне поля зрения общества и государства.

2. Сетевая террористическая деятельность

Кибертерроризм использует открытость Интернета для дискредитации правительств и государств, размещения сайтов террористической направленности, порчи и разрушения ключевых систем путем внесения в них фальсифицированных данных или постоянного вывода этих систем из рабочего состояния, что порождает страх или тревогу, и является своего рода дополнением к традиционному виду терроризма.¹

В условиях глобализации И.А. Щуклин выделяет следующие криминогенные факторы, способствующие активизации международного терроризма (в том числе и в сети Интернет):

1. Сама политика глобализации, конечной целью которой является создание однополярного мира;

¹ Паненков А.А. Предложения по оптимизации борьбы с использованием сети Интернет в террористических целях. // Правовые вопросы связи. – 2011. – №2. – С. 16.

2. Модернизация и открытость национальных экономик вместе с глобализацией финансовых рынков;

3. Интенсификация процесса глобальной информатизации путем создания всемирных коммуникаций, одной из которых является сеть Интернет;

4. Глобализация в культуре и религии.

Интенсивная информатизация и повсеместное внедрение высоких технологий в способы управления технико-логическими процессами, в том числе и техногенно-опасными, дает основание ожидать рост возможных террористических действий, направленных на вывод из строя информационной инфраструктуры.¹ Россию данная проблема также не обошла стороной.

Интернет-терроризм по своей структуре неоднороден и его можно условно разделить на два взаимодополняющих направления террористической деятельности:

- совершение террористических актов непосредственно через Интернет;

- осуществление деятельности, сопутствующей терроризму.

1. Но для российского сегмента интернет-терроризма наиболее характерным является второй вид. Всемирная сеть служит для размещения информации, ориентированную на широкий круг интернет-пользователей. Это не только реклама террористических организаций, открытое оправдание их действий и идеологии, но и устрашение, оскорбление населения и органов государственной власти. Распространяя подобные сведения террористы пытаются влиять на общественное мнение, дискредитируя власть и запугивая граждан.

¹Шуклин И.А. Криминальная глобализация в сфере высоких технологий и международный терроризм. // Известия Юго-западного государственного Университета. - 2012. - № 1 -5. - С. 130.

Но подобного рода сопутствующая терроризму деятельность не всегда связана с распространением информации в Интернете. Так, с помощью сети, террористы могут осуществлять вербовку в террористические организации, коммуникацию среди различных террористических группировок, сбор сведений для дальнейшего их применения в своей деятельности, а так же распространение и сбор денежных средств.

Не смотря на то, что объективно оценить соотношение терроризма во всемирной паутине и реальном мире проблематично, совершенно очевидно какое преимущество Интернет дает террористическим организациям, увеличивая в разы общественную опасность совершаемых ими действий..

Паненков А.А. выделяет некоторые актуальные меры борьбы с кибертерроризмом:

1. Совершенствование технических способов фильтрации и блокировки сайтов террористического толка;

5. Совершенствование законодательства по сокращению сроков с момента обнаружения террористического сайта в сети Интернет до вынесения решения судом о признании информационных материалов, размещенных на этом сайте, экстремистскими и ограничении доступа к ним. Применение опыта других стран в борьбе с сетевым терроризмом;

3. Шире использовать возможности прокуратуры по предъявлению исков о возложении на провайдеров обязанности устанавливать фильтры, запрещающие доступ к сетевым ресурсам террористических и экстремистских организаций;

4. Заключение международных соглашений по блокированию или закрытию сайтов, распространяющих информационные материалы террористического характера.¹

3. *Спам*

¹Паненков А.А. Предложения по оптимизации борьбы с использованием сети Интернет в террористических целях. // Правовые вопросы связи. – 2011. – №2. – С. 16.

Интернет привел к появлению большого количества новых разновидностей общественно опасных деяний, некоторые из которых некриминализованы ввиду некоторых обстоятельств. Таковым является спам, то есть массовая рассылка нежелательных сообщений посредством электронной почты или других средств пересылки электронных сообщений. На первый взгляд общественная опасность данного интернет-явления не кажется столь уж значительной. Она не так очевидна для отдельно взятого получателя, спам-сообщение может нанести небольшой материальный ущерб.

И не смотря на то, что спам в России нельзя отнести к уголовно-наказуемым деяниям, спам неотделим от понятия интернет-преступности. Спам-рассылка приносит существенный доход в карман хакеров, игнорирующих права человека. Никому не нужные, содержащие порой информацию, способную нанести моральный вред, нежелательные сообщения, зачастую превышают своим количеством действительно необходимые получателю. Навязчивая реклама распространяется не только через электронную почту, но и через смс-сообщения, что так же, на мой взгляд, требует регламентации.

В США, а также во многих странах Европы, приняты и активно применяются законы против спама. И неплохо было бы применить данные нормы к российским реалиям. Спам обладает относительной распространенностью и типичностью, может нанести материальный и моральный ущерб. И пусть вред рассылки для одного получателя невелик, но негативное влияние на общество и экономику игнорировать никак нельзя.

2.2 Личность интернет-преступника и его жертвы

Для эффективной борьбы с преступлениями, совершаемыми в сети Интернет, необходимо учитывать такой немаловажный факт, как личность преступника.

Поведение человека детерминируется совокупностью нескольких факторов воздействия:

- общественной средой;
- непосредственным окружением;
- внутренним миром человека.

Но основным уровнем, определяющим поведение личности, остается макросоциальный уровень, так как в рамках общесоциальной среды устанавливаются отношения различного рода (политические, культурные, экономические, нравственные и др.), которые, в свою очередь, оказывают влияние на формирование и развитие личности, действуя как непосредственно, так и опосредованно.

Но даже если влияние общесоциальной среды было в целом положительным, все равно остается возможность проявления у человека антисоциального поведения. Его источником может послужить непосредственное ближнее окружение индивидуума, но такого рода поведение может быть уже заложено в особенностях личностных характеристик.

В научной литературе можно найти большое количество классификаций личности преступника, составленных в зависимости от определенных признаков. Это может быть вид преступления, возраст, пол, роль преступника в совершенном преступлении и т.д. при этом, лица совершившие различные виды преступлений (воры, насильники, мошенники), имеют и свои собственные, отличные от других, особенности характеристики их личности.

Говоря о личности интернет-преступника, сложно создать единую картину признаков, отличающих данную категорию правонарушителей. Это связано с тем, что Интернет может использоваться при совершении преступлений различного рода, от направленных против личности до посягающих на государственную власть. В связи с такой неоднородностью интернет-преступности, можно лишь сказать, что в данном случае они будут сочетать в себе признаки, присущие различным группам преступников. Соответственно нельзя будет составить обобщенный криминологический портрет интернет-преступника. Но, тем не менее, наибольший интерес для данного исследования будут представлять самые яркие представители интернет-преступников: компьютерные преступники и интернет-мошенники.

В процессе изучения личности компьютерного преступника, рассмотрению подлежат такие социально-демографические признаки как:

- пол;
- возраст;
- наличие судимостей;
- социальная среда проживания;
- мотивация;
- отношение к содеянному.

Не смотря на то, что соотношение мужчин и женщин пользовательской интернет-аудитории практически равное, большинство компьютерных преступников – это мужчины. Они чаще всего имеют высшее либо неоконченное высшее техническое образование (55%), а также иное высшее или неоконченное высшее образование (24%). Среди которых преобладают лица в возрасте от 18 до 25 лет (52%), а также от 30 до 45 лет (17 %). Компьютерные преступники в обычной жизни чаще всего работают в компьютерной сфере (обслуживание, программирование), постоянное место работы имеет не каждый, предпочитая фриланс. Многие проживают вместе со своими родителями.

Можно с уверенностью сказать, что интернет-преступность молодеет, и большое число совершаемых в сети преступлений приходится на несовершеннолетних правонарушителей. Это указывает на необходимость разработки программы по принятию профилактических мер в вопросах высокотехнологичных преступлений, направленной в первую очередь на молодежь и подростков.

Интерес несовершеннолетних к таким видам преступлений объяснить достаточно легко. Во многих современных российских семьях дети начинают осваивать компьютер достаточно рано, они изучают информатику в школах, либо занимаются самостоятельным обучением. Низкий уровень правовой культуры, влияние более продвинутых сверстников, любопытство и толкают несовершеннолетних лиц на совершение преступлений данного вида.

Эти лица никогда не были судимы и в целом ведут законопослушный образ жизни, но при этом имеют некоторые асоциальные установки, ведут замкнутый образ жизни. Но они чаще всего признают свою вину и не отрицают причастность к преступлению. Некоторые возмещают материальный ущерб, причиненный их противоправными действиями.

Вряд ли описываемой тип преступника можно назвать профессиональным. Они практически не пытаются скрыть следы совершенного преступления, используют свой домашний компьютер и совершают достаточно простые с технической точки действия, зачастую облегчая себе задачу скачанными из Интернета программами. Их мотивация чаще всего корыстная, но происходит не столько из финансовой необеспеченности, сколько из внутренних побуждений, таких как любопытство, тяга к исследованиям. Их заниженная самооценка требует доказательства собственного интеллектуального превосходства. К тому же, эти лица, чаще всего находятся в материальной зависимости от своих родителей и им требуется доказать самим себе собственную значимость, желание приобщиться к популярной хакерской субкультуре.

Но существуют и профессиональные компьютерные преступники, владеющими высокими IT-навыками. Их социальный портрет в целом схож с вышеописанной группой, разницу составляет уровень знаний, интеллектуальная претенциозность и преступная мотивация. К тому же деятельность хакеров не лишена романтизма, разрекламированная средствами массовой информации, послужившая тематикой для книг и фильмов, она неизменно привлекает к себе внимание юных умов, желающих приобщиться к этой культуре.

Интернет оказывает сильное влияние на простых пользователей, что касается личности преступников, то происходит размытие некоторых моральных принципов и «деформация» восприятия. Анонимность, становится причиной чувства вседозволенности. Хакер получает своеобразное удовольствие от мысли о «силе», которой он наделен, а количество взломанных компьютеров и степень проченного ущерба служат своеобразной меркой их способностей. Все эти успехи на хакерском поприще обратно пропорциональны достижениям в реальной жизни, это не что иное, как способ самоутвердиться за счет других людей в ущерб последним.

Корыстный мотив также нельзя исключать. В данном случае хакинг служит существенным источником дохода компьютерного преступника, который в отличие от непрофессионала, совершает преступления еще и на заказ. Личная заинтересованность не является в таком случае обязательной.

Сообщество профессиональных компьютерных преступников достаточно замкнутое и важную роль тут играет авторитет в среде себе подобных и некоторая степень известности. Некоторые фигуры среди этого специфического социума являются «культовыми» и становятся объектами подражания. Отличается высокой степенью сплоченности. Хакеры склонны помогать друг другу, объединяться в группы для совершения кибератак.

Многие компьютерные преступники оправдывают свою противозаконную деятельность борьбой за свободу информации, против

бюрократии и крупных IT-компаний, которые по их мнению монополизировали рынок. Действительно, свод хакерских ценностей существует, но даже если лицо преследует в процессе своей деятельности определенные цели опираясь на подобного рода идеологию, это не делает содеянное законным, и, ни в коем случае не умаляет общественно-опасных последствий. Какой бы ни была мотивация, преступление всегда остается преступлением.

Существуют и другие виды интернет-преступников, которые также как и хакеры действуют в сфере компьютерной информации. Это так называемые вирусописатели – авторы вредоносных программ. Вирус это компьютерная программа, чаще всего деструктивного характера. Можно выделить следующие их виды:

- поражающие всю систему;
- поражающие отдельные системные функции;
- затрудняющие работу системы;
- нейтрального действия;
- позитивно ориентированные.

Лица, создающие и распространяющие вирусы первых трех категорий асоциально настроенные личности, преследующие различные цели, от желания получить финансовое вознаграждения до желания получить признание в обществе себе подобных. Как и в культуре хакеров, социальная среда вирусописателей также имеет огромное значение, особенно в случае, когда преступник хочет, что называется, сделать себе имя. И если хакеры используют все возможности современных компьютерных программ для сохранения своей анонимности и уничтожения доказательств, вирусописатель, имеющий деструктивные наклонности, наоборот, ищет всеобщего признания, выходящего за рамки интернет-сообщества. Но даже если вирусописатель не преследует цель уничтожения и повреждения компьютерных данных, он не становится менее опасным. Такого рода

преступники могут лишь создавать вредоносные программы не запуская их сеть, но, не прекращая активно пропагандировать свои идеи среди интернет-сообщества. Его идеи могут быть воплощены в жизнь другим компьютерным преступником и применены на практике.

Подводя итог, следует указать, что личность интернет-преступника неоднородна и нужно учитывать обстоятельства совершения интернет-преступления. Но можно ориентироваться на социальный портрет компьютерного преступника: это чаще всего молодой мужчина, имеющие определенную склонность к асоциальности, но в целом старающийся не выделяться, проживающий вместе с родителями, материально от них зависим. Он разбирается в компьютерных технологиях, работает, часто по специальности, преступления совершает со своего домашнего компьютера. Может разделять некоторые моральные ценности субкультуры хакеров, но в большинстве им движет желание заработать денежные средства.

На мой взгляд, это интересная тема для научного исследования, которую требуется развивать и дальше. К сожалению личность компьютерного преступника охарактеризовать достаточно трудно, и на эту тему существует не так много научных исследований. Следует вести борьбу с популяризацией данного вида преступной деятельности у молодежи, повышая правовую грамотность и сознательность подростков, нейтрализуя негативное воздействие хакерской субкультуры, помогающей росту распространению и интернет-преступности в целом.

Но не только личность преступника и его намерение совершить преступное деяние является определяющим для возникновения преступной ситуации. Немаловажную роль здесь играет личность потерпевшего и его поведение до, во время и после преступного посягательства. Речь идет о виктимности, то есть повышенная способность человека в силу ряда

духовных, физических, социальных качеств, при определенных объективных обстоятельствах становиться «мишенью» для преступных посягательств.¹

Проблема виктимности жертвы интернет-преступности также важна для изучения, как и при совершении традиционных видов преступлений.

Как уже отмечалось ранее, интернет-преступность неоднородна, поэтому связанная с ней напрямую виктимность потерпевшего, варьируется в зависимости от подвида преступного деяния, совершенного с помощью всемирной паутины.

Можно выделить следующие виды жертв интернет-преступлений:

- физические лица;
- коммерческие организации;
- органы государственной власти;
- предприятия связи и интернет-провайдеры;
- банковские организации;
- иностранные физические и юридические лица.

Свойства Интернета таковы, что жертва преступником часто не выбирается специально. Некоторые программы взлома запрограммированы искать незащищенные компьютерные системы имеющие доступ к сети Интернет, и делают они это не персонифицировано. Злоумышленник может не знать ни места расположения компьютера в географическом плане, ни тем более имя его владельца. А благодаря анонимности жертвы преступлений не располагают данными о личности преступника.

Основными виктимогенными факторами для интернет-пользователей, по моему мнению, выступают небрежность и технологическая неграмотность. Небрежность со стороны пользователя в вопросах защиты своей собственной информации, несомненно, провоцирует и стимулирует не только совершение одного конкретного преступного деяния, но и является фактором роста общего количества преступлений совершаемых через

¹ Малков В.Д. Криминология: Учебник для вузов. – М.: Издательство: ЮстицИнформ, 2011. – С. 324.

Интернет. Но зачастую потерпевший просто не обладает нужными навыками, необходимыми для обеспечения компьютерной системы необходимыми средствами защиты. Значительная часть жертв просто не может обнаружить факт совершенного в отношении нее интернет-преступления, им либо не хватает для этого соответствующих навыков, либо преступник не оставляет за собой следов, что является одной из причин высокой латентности данной группы преступлений. Нежелание жертв сообщать о фактах совершения преступления также не способствует снижению уровня интернет-преступности, а наоборот провоцирует злоумышленников, чувствующих свою безнаказанность, на совершение новых противоправных действий.

Одно из самых популярных интернет-преступлений это, конечно же, мошенничество. Виктимологические риски интернет-мошенничества рассмотрел в своей статье А.А. Комаров. Проведя сравнительное исследование на основе статистических данных собственного эмпирического исследования, он пришел к выводу, что в целевой группе россиян в возрасте от 30 до 40 лет сосредоточены две необходимые виктимогенные посылки – высокий уровень благосостояния и необходимый уровень технической грамотности. Автор также отмечает значимость таких социальных процессов как уровень административных и иных правонарушений, аморальных явлений, наркомании, пьянства, дезадаптации взрослых и детей является виктимогенным фактором, так как доступ к высоко технологическим средствам в современных условиях получили все социально-неблагополучные слои населения нашей страны. Указанные группы могут выступать в роли активных субъектов преступной деятельности, так и жертв интернет-мошенничества. В данном случае имеет место быть так называемая инверсия ролей, когда жертва преступления превращается в преступника и таким образом следствие становится причиной совершения преступления.

А.А. Комаров также отмечает, что группа наиболее подверженная виктимологическому риску в современной России, это молодые слои

населения, в силу их большей приверженности к современным высоким технологиям.

Из всего вышесказанного можно сделать вывод: для криминологической характеристики интернет-преступности важна не только личность самого преступника, но и его жертвы. Причем поведение последней зачастую лишь усугубляет ситуацию. Поэтому, по моему мнению, для эффективной борьбы с интернет-преступностью нужно не только выявлять самих преступников, но и активно работать с населением, разъясняя базовые принципы защиты своих компьютеров от преступных посягательств, а также объяснить, что преступление в киберпространстве не менее серьезно и опасно чем противоправное деяние, совершенное в реальном мире.

2.3 Меры предупреждения и международный опыт борьбы с интернет-преступностью

Основной задачей данного криминологического исследования является выработка мер противодействия и предупреждения интернет преступности. Следует выделить следующие их группы: правовые, организационные, экономические, технические и идеологические.

Правовые меры борьбы с данным видом преступности, на мой взгляд, играют решающую роль. Они должны включать в себя не только разработку и принятие норма, пресекающих совершение преступных деяний, но и оказывающих профилактические меры. Необходимо расширение круга нормативно-правовых актов регламентирующих интернет-отношения и выражающие четкую позицию российского законодателя в отношении правового статуса сети Интернет, закрепление в российских законах международных стандартов безопасности и применение их на практике. Совершенствование норм уголовного и административного

законодательства, а именно введение новых составов и квалифицирующих признаков. Данная мера обусловлена тем, что:

- Интернет в значительной степени повышает общественную опасность преступного деяния;
- Деформация личности преступника, вызванная анонимностью и безнаказанностью;
- Удаленность и трансграничность значительно уменьшают шансы на поимку преступника, поэтому требуется регламентация в области международного сотрудничества;
- Интернет-преступность явление распространенное и разнообразное, охватывающие практически все Главы Особенной части Уголовного кодекса РФ;
- Может быть использован как для непосредственного совершения преступления, так и на стадии подготовки;
- Интернет может быть использован не только для облегчения реализации задуманного преступного деяния, но и для сокрытия следов уже совершенного преступления;

Так же следует отметить необходимость включения в некоторые составы квалифицирующего признака «совершенное с помощью сети Интернет», о которых было сказано выше. При условии, если Интернет не только увеличивает степень общественной опасности, но и является типичным способом совершения данного вида преступления. На мой взгляд, данное изменение наиболее необходимо в ст. 110, 128.1, 137, 138, 146, 150, 151, 174, 174.1, 205.1, 205.2, 230, 242, 272, 273, 280 Уголовного кодекса РФ.

Организационные меры призваны решить проблему регулирования и надзора за отношениями, возникающими в сети Интернет. По моему мнению, государственные органы, организации и гражданское общество должны действовать сообща, при этом ключевое значение играет личностный контроль со стороны интернет-пользователя. Но только при обеспечении

защиты его прав со стороны государства. Отраслевые структуры так же помочь в регулировании данной сферы, но не стоит забывать, что большинство IT-специалистов могут самостоятельно защитить себя от нежелательной и вредной информации и воспрепятствовать совершению противоправного деяния в отношении себя, тогда как обыкновенные интернет-пользователи такими навыками не обладают, а значит должны обращаться за помощью к государству. На данный момент создание единой структуры, которая контролировала бы распространение информации в Интернете просто необходимо. Потому что интернет-преступлениям, контроль, за которым осуществляют правоохранительные органы, сопутствует распространение данных, содействующих преступлениям. Но ресурсы государства ограничены, и сотрудники органов просто не могут уследить за всем противозаконным контентом, появляющимся в сети ежедневно. В данном случае наблюдение за появлением подобного рода информации должно быть отдано администраторам и интернет-ресурсов и интернет-провайдерам.

Экономические меры состоят главным образом в привлечении компьютерных специалистов в информационно-технический сектор экономики. Но к сожалению, сейчас у государства нет практически никаких шансов, для того чтобы сделать интернет-преступность невыгодной. Ведь большинство злоумышленников совершают преступления в сети исходя из корыстного мотива. Развитие отрасли технического, компьютерного и программного обеспечения, учитывая кадровый потенциал нашей страны, финансовая поддержка со стороны государства, оказание мер по поддержке информационных технологий, инвестирование в новую отрасль могли бы в значительной степени решить данную проблему. Но не стоит забывать о том, что большой процент интернет-преступлений это нарушение авторских и смежных прав. На своем опыте могу сказать, что главным отпугивающим фактором против покупки легального контента является его цена, особенно

если речь идет о зарубежной продукции. Не обязательно что бы все было дешево, но можно вести ценовую политику в разумных пределах и возникало желание скачать продукт с торрент-трекера. Появление альтернативного обеспечения или программ, российского производства так же поспособствовало бы снижению цен на продукты интеллектуального труда.

Технические меры можно разделить на два вида: аппаратные и программные. Первые предполагают защиту непосредственно технических устройств передачи данных от физических воздействия. Вторые используются уже для защиты информации и соединения с Интернетом. Даже базовая защита персонального компьютера может предотвратить преступное посягательство, главное ей не пренебрегать. Но даже самый хороший антивирус к сожалению не в силах защитить от проникновения вредоносной программы, разновидностей которых с каждым днем появляется все больше.

Кроме этого существует возможность ограничения доступа на ресурсы, содержащие противозаконную информацию. Это может быть фильтрация запросов к поисковым службам или специальные программы, например «Родительский контроль», призванный защитить несовершеннолетних от вредоносной информации.

Мерами *идеологической* профилактики в первую очередь является выработка негативной оценки деятельности интернет-преступников у населения, посредством средств массовой информации и используя тот же Интернет, для разъяснения основных аспектов поведения в сети. В том числе и в случае столкновения с правонарушителями. «Группой риска» можно считать студентов технологических специальностей, с ними следует проводить занятия по формированию правового сознания. При этом следует выработать единую программу, идеологическую линию, противоречащую мировоззрению интернет-преступности. Ни один правовой запрет не может работать эффективно, пока не будет, подготовлена идеологическая база.

Кроме применения вышеназванных мер внутри страны, не стоит забывать о международном сотрудничестве по борьбе с интернет-преступностью. А.Б. Попов в своей статье отмечает направления реализации нормативно-правового сотрудничества на мировом уровне, путем применения:

- универсальных международных договоров (Конвенция ООН против транснациональной организованной преступности)
- многосторонних соглашений по борьбе с отдельными преступлениями (Европейская конвенция о киберпреступности);
- региональных многосторонних соглашений (Соглашение СНГ в борьбе с преступлениями в сфере компьютерной информации);
- решений ООН и других межправительственных органов;
- двусторонних соглашений государств

Также автор выделяет формы международного сотрудничества в области интернет-преступности, которые предпринимаются со стороны государств для достижения поставленных целей и задач. Это:

- 1) профилактика и пресечение преступлений, в отношении которых заключены специальные соглашения между государствами;
- 2) передача лиц, осужденных к лишению свободы для отбывания наказания в государства их гражданства или постоянного места жительства;
- 3) выдача преступников другому государству или международному органу для уголовного преследования;
- 4) совместное изучение причин и других проблем преступности;
- 5) обмен опытом работы полицейских и других органов путем проведения международных семинаров и пресс-конференций;
- 6) обмен оперативной правовой информацией и др.

Приоритетной задачей международного взаимодействия в сфере предупреждения и пресечения совершения интернет-преступлений, является унификация национального уголовного законодательства государств,

принимающих участие в международном сотрудничестве. В данном случае речь идет о борьбе с киберпреступностью, методики которой не отличаются от способов борьбы с интернет-преступностью в целом, так как на первый план выходит именно сеть Интернет ее особенности.

Наибольшую значимость в области международного взаимодействия имеет Международная «Конвенция о киберпреступности», принятая 23 октября 2001 года. 15 ноября 2005 года Президентом Российской Федерации было подписано распоряжение «О подписании Конвенции о киберпреступности», в котором глава государства дал соответствующие указания Министерству иностранных дел РФ, но тем не менее, Россия вплоть до настоящего времени, так и не подписала данную конвенцию.

Главной причиной препятствующей принять конвенцию, является то обстоятельство, что в уголовном законодательстве РФ не предусмотрена ответственность юридического лица за совершение преступлений, в то время как данное положение прописано в тексте Конвенции и применяется в ряде зарубежных стран.

Конвенция предусматривает в качестве субъектов преступлений только физических, но и юридических лиц. Положения Конвенции указывают, что «государства-участники принимают законодательные и иные меры, необходимые для обеспечения возможности привлечения юридических лиц к ответственности за преступление, которое совершается в их пользу любым физическим лицом, действующим индивидуально или как часть одного из органов соответствующего юридического лица, если такое физическое лицо имеет право представлять данное юридическое лицо, принимать от его имени решения либо осуществлять внутри него контроль».

Позиция законодателя в данном случае вполне понятна, но традиционные представления о территориальной юрисдикции, об административных границах применительно к киберпространству во многом вообще теряют смысл. И роль национального законодательства неизбежно

снижается, а значение международного права выходит на первый план.

Однако в данном случае речь идет не столько о ратификации принятых международно-правовых актов, сколько об учете рекомендаций различных международных организаций, анализа и обобщения существующих пробелов в специальном законодательстве зарубежных стран в работе отечественных законодателей.¹

И все же, несмотря на принятие различных документов на межгосударственном уровне, параллельно следует вести борьбу с интернет-преступностью на уровне национальном, постоянно совершенствуя законодательную базу и правоприменительные методики. Усилия на межнациональном и внутригосударственном уровне должны дополнять друг друга, обеспечивая координацию по борьбе с интернет-преступностью

¹Алавердов, О. С. Международное сотрудничество в области борьбы с Интернет-преступностью // Общество и право. – 2010. – № 3. – С. 166.

ЗАКЛЮЧЕНИЕ

В данной работе была проанализирована и изучена тема «Интернет-преступность: уголовно-правовая и криминологическая характеристика».

Современное развитие технологии Интернет и социальных отношений, возникших благодаря ей, характеризуется непрерывным ростом преступлений и других общественно опасных деяний, совершенных посредством всемирной сети, что подтверждено официальной статистикой и научными исследованиями как в России, так и за границей. Учитывая эту глобальную негативную тенденцию в области правовой борьбы с преступностью в Интернет, необходимы решительные меры криминологического и уголовно правового характера по противодействию и профилактике данного вида преступлений.

Принимая во внимание всепроникающее внедрение Интернета во все сферы общественной жизни, представляется, что проблема преступности в Глобальной сети, являясь одной из главных составляющих Информационной безопасности РФ, относится к актуальным, своевременным, имеющим теоретическое и практическое значение.

В данной работе проведен обширный анализ Интернет-преступности.

Во-первых, сформулировано понятие интернет-преступления и интернет-преступности, проанализированы уголовно-правовые, криминологические признаки и характеристики, исторические аспекты интернет-преступности.

В данной работе выявлены основные факторы виктимности потерпевших от интернет-преступлений и предложены меры виктимологической профилактики интернет-преступлений; проведен анализ общественного мнения разных групп населения в их отношении к проблеме преступности в Интернет. Выявлено, что общество считает государственный

контроль информации в Интернет, осуществляемый в настоящее время, недостаточным и требует его ужесточения.

В работе достаточно подробно исследованы: состояние, структура и динамика компьютерной и Интернет-преступности, а также наиболее опасных её подвидов. Проведен анализ криминогенности сети Интернет. Дана правовая и криминологическая оценка общественно опасной деятельности в Интернет, которая не криминализована; выявлена необходимость и условия для установления уголовной ответственности за нежелательную рассылку электронных сообщений (спам).

Также выявлены детерминанты роста и развития Интернет-преступности; в качестве специфических причин выделены: особые свойства сети Интернет как технического, социального, правового явления; неразвитость сектора информационных технологий в российской экономике; негативное влияние субкультуры хакеров; пробелы и недочеты в российском уголовном и ином законодательстве.

Разработаны меры предупреждения Интернет-преступности организационного, идеологического, технического и правового характера. Среди других шагов по противодействию данному виду общественно опасных деяний необходимо выделить: нейтрализацию негативного влияния субкультуры хакеров, развитие отрасли информационных технологий, модернизацию законодательства РФ в сфере компьютерных технологий.

Современному этапу исследований преступной природы Интернет свойственно постепенное накопление и анализ практической информации. Несмотря на обширное количество специалистов, занимающихся проблемой компьютерной преступности и проблемой компьютерного права, многие вопросы, касающиеся уголовно-правовой и криминологической характеристики Интернет-преступности остаются все еще недостаточно исследованными.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

Нормативно-правовые акты

1. Конституция Российской Федерации (с учетом поправок, внесенных Законами РФ о поправках к Конституции РФ от 30.12.2008 № 6-ФКЗ, от 30.12.2008 № 7-ФКЗ, от 05.02.2014 № 2-ФКЗ, от 21.07.2014 № 11-ФКЗ) // Собрание законодательства РФ. - 04.08.2014. - № 31. - Ст. 4398.
2. Уголовный кодекс Российской Федерации от 13.06.1996 (ред. от 17.04.2017) // Собрание законодательства РФ. - 17.06.1994. - № 25. - Ст. 2654.
3. Кодекс Российской Федерации об административных правонарушениях от 30.12.2001 № 195-ФЗ (ред. от 17.04.2017) // СПС Консультант Плюс. - 2017.
4. Федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 19.12.2016) «О средствах массовой информации» // СПС Консультант Плюс - 2017.
5. Федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 19.12.2016) «Об информации, информационных технологиях и о защите информации» // СПС Консультант Плюс. - 2017.
6. Постановление Правительства Российской Федерации от 26.10.2012 № 1101 «О единой автоматизированной информационной системе «Единый реестр доменных имен, указателей страниц сайтов в информационно-телекоммуникационной сети «Интернет» и сетевых адресов, позволяющих идентифицировать сайты в информационно-телекоммуникационной сети «Интернет», содержащие информацию, распространение которой в Российской Федерации запрещено» // СПС Консультант Плюс. - 2017.

Научная и учебная литература

7. Бриллиантов А.В. Комментарий к Уголовному кодексу Российской Федерации в 2 т. Т. 2 / Под ред. А.В. Бриллиантова. - М: Проспект, 2015. - 704 с.
8. Ветров Н.И., Дайшутов М.М., Дашков Г.В. Комментарий к

Уголовному кодексу Российской Федерации: Научно-практический / Под. ред. С.В. Дьякова, Н.Г. Кадникова. – М.: Юриспруденция, 2013. - 912 с.

9. Галахова А.В. Оценочные признаки в уголовном кодексе Российской Федерации: научное и судебное толкование: Научно-практическое пособие / Под ред. А.В.Галаховой. – М.: Норма, 2014. - 736 с.

10. Грачев Ю.В. Уголовное право России / Под ред. Ю.В. Грачева. - М: Инфра-М, 2013. - 368 с.

11. Дашян М.С. Право информационных магистралей. Law of Information Highways. Вопросы правового регулирования в сфере Интернет. – М.: Волтерс Клувер, 2007. – 288 с.

12. Иногамова-Хегай Л.В. Уголовное право Российской Федерации / Под ред. Л.В.Иногамовой-Хегай. - М.: Инфра-М, 2013. - 742 с.

13. Козаченко И.Я, Новоселов Г.П. Уголовное право. Особенная часть: учебник. - М.: Норма, 2008. – 1008 с.

14. Подройкина Е.В., Серегина Е.В., Улезько С.И. Уголовное право в 2 т. Т. 2. Особенная часть / Под ред. И.А. Подройкиной, Е.В. Серегиной, С.И. Улезько. – М.: Юрайт, 2014. - 993 с.

15. Рассолов, И. М. Право и Интернет: Теоретические проблемы. – М.: Норма, 2009. – 383 с.

16. Сверчков В.В. Уголовное право. Общая и Особенная часть / Под ред. В.В.Сверчкова. - М.: Юрайт, 2013. - 589 с.

17. Чучаев А.И. Комментарий к Уголовному Кодексу Российской Федерации / Под ред. А.И.Чучаева. - М: Контракт, 2013. - 672 с.

Публикации в научных журналах, сборниках и СМИ

18. Алавердов, О.С. Международное сотрудничество в области борьбы с Интернет-преступностью // Общество и право. – 2010. – № 3. – С. 165 – 167.

19. Андреев, В.В., Кежов, А.А. Проблемы выявления, предупреждения и уголовно-правовая квалификация незаконного

распространения порнографических материалов с участием несовершеннолетних в сети // Вестник Санкт-Петербургского университета МВД России. – 2010. – № 4. – С. 67 – 71.

20. Атаманов Р. Правонарушения, совершаемые в сети Интернет, связанные с обманом и злоупотреблением доверием с целью получения конфиденциальной информации: некоторые проблемы и способы их решения // Правовые вопросы связи. – 2010. – №2. – С. 10 – 12.

21. Боровик П.Л. Анализ положений Конвенции Совета Европы по борьбе с киберпреступностью в целях противодействия детской порнографии в сети Интернет // Проблемы укрепления законности и правопорядка: наука, практика, тенденции. -2011. - №4. - С. 276 - 283.

22. Буданова Е.А., Богомолов А.Н. К вопросу об ответственности за неправомерное завладение данными кредитных либо расчетных карт и их оборот в теневом секторе экономики // Вестник Тамбовского университета. – 2011. - №7. - С. 234 - 239.

23. Вилинов, А. Практика регулирования отношений, связанных с незаконным использованием объектов авторского и смежных прав в сети Интернет, в США, России и ряде стран // Интеллектуальная собственность : Авторское право и смежные права. - 2010. - № 12. - С. 54 - 65.

24. Гузеева, О. Квалификация мошенничества в российском сегменте сети интернет // Законность. - 2013. - № 3. - С. 21 – 24.

25. Дворецкий М.Ю., Карамнов А.Ю. Преступления в сфере компьютерной информации в России и зарубежных государствах: проблемы квалификации, уголовной ответственности и наказания // Вестник Тамбовского университета. - 2011. - №11. - С. 395 - 399.

26. Жиделев В.Г. Новые аспекты квалификации преступлений в сфере компьютерной информации в российском и зарубежном законодательстве // Человек: преступление и наказание. - 2012. - №2. - С. 23 - 25.

27. Зульфугарзаде, Т. Э., Танимов, О. В. Направления развития зарубежного законодательства об информационной безопасности // Информационное право. - 2011. - № 4. - С. 26 - 28.
28. Кананович, А. И. Духовно-нравственные факторы совершения преступлений, посягающих на авторские права в глобальной сети Интернет // Российский следователь. - 2012. - № 21. - С. 21 - 23.
29. Карамнов, А. Ю. Проблемы квалификации в отношении преступлений, совершенных в глобальной сети Интернет. // Российская академия юридических наук. Научные труды. - Выпуск 11. Том 2. – М., 2011. – С. 667 – 669.
30. Касьяненко М.А. К проблеме оборота информации этнодискриминационного и этнокриминального характера в сети Интернет // Правовые вопросы связи. – 2011. – №1. – С. 28 – 32.
31. Кобзева С. Законодательные меры по борьбе с детской порнографией в Интернет: мировой опыт и российские реалии // Информационное право. – 2009. – №2. – С. 22 – 25.
32. Коликов Н.Л. Причины и условия профессиональной компьютерной преступности // Вестник Южно-уральского государственного университета. – 2011. – №19. – С. 30 – 33.
33. Коликов, Н. Л. Профессиональная компьютерная преступность и мошенничество // Вестник Южно-Уральского государственного университета. – 2011. – Выпуск 28. – № 40. – С. 61 – 64.
34. Корнева, Л. А. Уголовная ответственность за нарушение имущественных авторских и смежных прав в Интернете // Российский следователь. – 2008. – № 6. – С. 7 – 10.
35. Королева, М. Клевета и оскорбление в сети Интернет // Законность. 2010. – № 7. – С. 50 – 53.
36. Максуров А.А. Возможности правового регулирования сети Интернет // Правовые вопросы связи. – 2011. – №1. – С. 16 – 22.

37. Максуров, А. А. Интернет как новое правовое пространство // Право и экономика. – 2010. – № 3. – С. 38 – 44.
38. Максуров А.А. О методологических основах правового регулирования интернет-отношений // Законодательство и экономика. – 2012. – № 2. – С. 59 – 61
39. Медведев, С. С. Общественная опасность мошенничества в сфере высоких технологий как основание его криминализации // Общество и право. – 2008. – № 3. – С. 164 – 166.
40. Морар, И. О. Как выглядит социально-правовой портрет участника преступного формирования, совершающего компьютерные преступления? // Российский следователь. – 2012. – № 13. – С. 34 – 38.
41. Никитина, И. А. Финансовое мошенничество в сети Интернет // Вестник Томского государственного университета. – 2010. – № 337. – С. 122 – 124.
42. Осипенко, А. Л., Кушниренко, С. Правовые и организационные основы международного сотрудничества в противодействии трансграничным преступлениям, совершаемым с использованием Интернета // Современное право. – 2008. – № 8. – С. 38 – 42.
43. Осипенко, А. Л. Организованная преступность в сети Интернет // Вестник Воронежского института МВД России. – 2012. – № 3. – С. 10 – 16.
44. Паненков А.А. Предложения по оптимизации борьбы с использованием сети Интернет в террористических целях // Правовые вопросы связи. – 2011. – №2. – С. 15 – 21.
45. Петрова Е. Под прицелом хакеров // Московский бухгалтер. – 2012. - № 3. – С. 45.
46. Пирожок, Е. Д. Способ преступления как наиболее важный элемент криминалистической характеристики угрозы убийством или причинением тяжкого вреда здоровью // Российский следователь. – 2013. – № 2. – С. 11 – 14.

47. Попов А.Б. Международное сотрудничество государств в борьбе с компьютерной преступностью // Вестник Тамбовского университета. – 2010. – №4. – С. 310 – 313.
48. Смирнов А.А. Приоритеты обеспечения безопасности информационного общества: сравнительно-правовой анализ программ России и Европейского союза // Административное право и процесс. - 2012. – №7. – С. 48 – 55.
49. Степанов-Егиянц, В. Г. Современная уголовная политика в сфере борьбы с компьютерными преступлениями // Российский следователь. – 2012. – № 24. – С. 43 – 46.
50. Сукманов А.О. Использование открытых источников информации в деятельности по раскрытию и расследованию преступлений // Вестник Калининградского юридического института МВД России. – 2010. – № 2. – С. 11 – 14.
51. Тропинина Т.Л. Борьба с киберпреступностью: возможна ли разработка универсального механизма? // Международное правосудие. – 2012. – №3. - С. 86 – 95.
52. Турканова В.И. Приватность в Интернете и распространение личных данных подростками // Научные ведомости Белгородского государственного университета. – 2010. – №14. – С. 292 – 295.
53. Чекунов, И.Г. Квалификация преступлений против собственности, совершаемых с использованием электронных платежных систем. // Российский следователь. – 2011. – № 24. – С. 26 – 28.
54. Чекунов, И.Г. К вопросу о понятии и системе преступлений, совершаемых с использованием компьютерных сетей. // Правовые вопросы связи. – 2012. – № 1. – С. 16 – 21.
55. Чекунов, И.Г. Киберпреступность: понятие и классификация. // Российский следователь. - 2012. - № 2. - С. 37 - 44.
56. Чекунов И.Г. Современные киберугрозы. Уголовно-правовая и

криминологическая классификация и квалификация киберпреступлений. // Право и кибербезопасность. – 2012. – №1. – С. 14.

57. Чирков Д.К., Саркисян А.Ж. Преступность в сфере высоких технологий: тенденции и перспективы // NB: Национальная безопасность. - 2013. - № 2. - С. 160 - 181.

58. Щуклин И.А. Криминальная глобализация в сфере высоких технологий и международный терроризм. // Известия Юго-западного государственного Университета. – 2012. – № 1 –5. С. 130 – 134.

Источники на электронных носителях

59. Официальный сайт Российской газеты. Режим доступа: <http://www.rg.ru/2011/12/22/reg-ufo/prigovor-anons.html>

60. Официальный сайт 1 канала. Режим доступа: <http://www.1tv.ru/news/social/202707>

61. Официальный сайт Федеральной службы государственной статистики [Электронный ресурс]. Режим доступа: <http://www.gks.ru>