ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«БЕЛГОРОДСКИЙ ГОСУДАРСТВЕННЫЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ»
(Н И У « Б е л Г У »)

ЮРИДИЧЕСКИЙ ИНСТИТУТ

КАФЕДРА УГОЛОВНОГО ПРАВА И ПРОЦЕССА

МОШЕННИЧЕСТВО В КИБЕРПРОСТРАНСТВЕ: УГОЛОВНО-ПРАВОВАЯ ХАРАКТЕРИСТИКА

Выпускная квалификационная работа
обучающегося по магистерской программе «уголовное право, уголовно-исполнительное право, криминология», направление подготовки 40.04.01 Юриспруденция,
очной формы обучения, группы 01001712
Морозовой Екатерины Александровны

Научный руководитель:
доцент кафедры уголовного права и процесса, к.ю.н.
Ляхова А.И.

Рецензент:
Заведующий Адвокатским кабинетом
Бариновой Татьяны Николаевны
Адвокатской палаты
Белгородской области
Баринова Т.Н.

БЕЛГОРОД 2019

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Актуальность исследования. Научно-технический прогресс, свидетелями которого мы являемся, стал причиной фундаментальных социальных преобразований, наиболее важным из которых стало возникновение нового вида общественных отношений – информационных.

На сегодняшний день, информация стала основой жизни общества, а равно одним из ведущих предметов и продуктов его деятельности. Более того, процесс ее создания, накопления, хранения, передачи и обработки в свою очередь стимулировал прогресс в области орудий ее производства: электронно-вычислительной техники, средств телекоммуникаций и систем связи. Следствием протекающих в обществе информационных процессов является возникновение и развитие новых отношений и преобразование уже существующих.

В современном мире в условиях повсеместной глобализации и информатизации всех сфер жизнедеятельности общества все большую популярность приобретают информационные технологии, которые интегрируют во все области деятельности. На сегодняшний день, практически все социальные отношения реализуются с помощью Интернет-коммуникаций, например, тех же социальных сетей. Например, только в России на начало 2017 года пользователями Интернета являются 84 млн. человек, а по данным последнего пресс-релиза Международного союза электросвязи количество интернет-пользователей в мире достигло 3,5 млрд. При этом, интернет и информационные ресурсы стали неотъемлемой частью жизни каждого человека. Люди общаются в социальных сетях, пользуются электронными досками объявлений, ведут личные сайты и блоги и т.д.

Таким образом, киберпространство стало неотъемлемой частью человеческой жизни. Оно представляет собой и средство связи, и площадку для общения, и неиссякаемый источник информации. Однако наряду с явными преимуществами, виртуальное пространство стало носителем

огромной угрозы не только для каждой личности, но и для отдельного государства и международного сообщества в целом. Дело в том, что киберпространство – это уникальная сфера человеческой жизнедеятельности, в пределах которой пользователь наделен практически неограниченными возможностями по сокрытию своей личности. Глобальная сеть позволяет миллиардам пользователей оставаться анонимными, чем не преминули воспользоваться преступники.

В современном мире, остро стоит проблема повсеместного распространения киберпреступности, которая может варьироваться от относительно безобидного мелкого мошенничества до преступлений международного масштаба, как например кибертерроризм или кибершпионаж. Помимо сложностей расследования таких преступлений, что также обусловлено и спецификой киберпространства, очень сильно «хромает» правовое регламентирование уголовной ответственности за их совершение. Лишь в немногих государствах современного мира существуют отдельные нормы или правовые акты, закрепляющие порядок наступления уголовной ответственности за совершений киберпреступлений, что в одинаковой степени относится и к России. Перед законодателем уже давно стоит задача качественного совершенствования уголовного законодательства, его модернизации и приведения в соответствие с реалиями объективного мира, однако, этого не происходит.

Одним из основных «бедствий» последних лет, связанных с повсеместным распространением кибертехнологий стало кибермошенничество. Обусловлено это высоким уровнем латентности данного вида преступлений, а также существенных трудностей, возникающих в процессе его раскрытия и расследования.

Рост числа интернет-магазинов, создание систем предоставления банковских услуг посредством глобальной сети, развитие платежных систем способствует тому, что все большее количество людей доверяют

безналичным расчетам, забывая о том, что даже в виртуальной экономической системе действуют криминальные элементы.

Степень разработанности проблемы. Современной состояние разработанности рассматриваемой нами проблемы является двояким. С одной стороны, ее разработка обладает большой практической и теоретической значимостью для современного общества, так как проблема интернет-мошенничества с каждым годом становится все актуальней, с другой – низкий уровень интереса ученых к этому конкретному виду преступных деяний. Несмотря на это, некоторые ученые достаточно полно постарались отобразить суть проблемы в своих исследованиях, например В.В. Бондарь, И.А. Никитина, Н.С. Юрочкин и др.

Объектом исследования являются общественные отношения, складывающиеся по поводу обеспечения защиты и безопасности общества и государства в сфере компьютерной информации.

Предмет исследования составляют положения современного уголовного законодательства, а также ранее действовавшего законодательства, регулирующего вопросы уголовной ответственности за совершение мошенничества в сети «Интернет», а также положения правоприменительной практики.

Цель исследования заключается в проведении всестороннего исследования феномена кибермошенничества и разработки рекомендаций по совершенствованию законодательства, предусматривающего уголовную ответственность за совершение рассматриваемого преступления.

Поставленная цель обусловила необходимость решения следующих **задач:**

1. Исследование истории развития уголовно-правового понятия мошенничества;

2. Определение понятия и признаков киберпреступности;

3. Изучение понятия и признаков киберпространства как места совершения преступления;

4. Анализ объективных признаков мошенничества в киберпространстве;

5. Анализ субъективных признаков мошенничества в киберпространстве, отграничение от смежных составов.

6. Исследование способов мошенничества в киберпространстве и проблем их квалификации;

7. Формулирование предложений по предупреждению мошеннических действий в киберпространстве и решение вопросов совершенствования уголовного законодательства.

Положения, выносимые на защиту:

1. В текст диспозиции ст. 159.6 УК РФ включить основной признак мошенничества способ обмана или злоупотребления доверием, что позволит исключить возможные правоприменительные ошибки. Таким образом, текст статьи будет выглядеть следующим образом: «мошенничество в сфере компьютерной информации, то есть хищение чужого имущества или приобретение права на чужое имущество путем обмана или злоупотребления доверием посредством ввода…».

2. Необходимо включить место совершения преступления – киберпространство – в диспозицию статьи наряду с вводом, удалением, блокированием, модификацией компьютерной информации, вследствие чего формулировка будет следующей: «…либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей, а равно совершенное в сети Интернет…». Данное включение, на наш взгляд, позволит расширить толкование данной статьи и упростить квалификацию кибермошенничества по соответствующей статье УК РФ.

3. Кроме того, мы считаем, что должна быть ужесточена санкция за совершение данного преступления. На сегодняшний день ч. 1 ст. 159.6 УК РФ не предусматривает такого наказания как лишение свободы, однако мы считаем, что в силу специфики данного вида преступления и необходимости

его тщательной подготовки и приобретения специальных знаний, оно должно быть включено. Так как последующие части статьи предусматривают максимальный срок лишения свободы до 10 лет, то считаем целесообразным включить срок до трех лет лишения свободы. Следовательно, санкция ч. 1 ст. 159.6 УК РФ должна выглядеть следующим образом: «…наказывается штрафом в размере до ста двадцати тысяч рублей или в размере заработной платы или иного дохода осужденного за период до одного года, либо обязательными работами на срок до трехсот шестидесяти часов, либо исправительными работами на срок до одного года, либо ограничением свободы на срок до двух лет, либо принудительными работами на срок до двух лет, либо арестом на срок до четырех месяцев, или лишением свободы на срок до трех лет».

Методологическая основа исследования представлена общими методами научного познания: индуктивным, дедуктивным, анализа, синтеза, а также частными: социологическим, структурно-функциональным, статистическим, сравнительным и другими.

Теоретическую основу исследования составили такие нормативные правовые акты отечественного и зарубежного законодательства как Уголовный кодекс РФ, Федеральный закон от 28 декабря 2010 № 390-ФЗ «О безопасности», Конвенция Лиги арабских государств (Арабская конвенция) о борьбе с преступлениями в сфере информационной техники, Уголовный кодекс Австрии, Уголовный кодекс Испании и др. Кроме того, были изучены и применены работы таких ведущих ученых-правоведов как В.А. Беспалов, В.А. Власихин, А.А. Галушкин, К.Н. Евдокимов, Н.И. Костенко, В.А. Номоконов, В.М. Сычев, И.Г. Чекунов и др.

Эмпирическая основа исследования представлена судебной практикой судов общей юрисдикции, а также официальными статистическими данными органов различного уровня подведомственности.

Апробация результатов **исследования**. Некоторая часть положений и выводы диссертационного исследования были изложены автором в опубликованных научных статьях:

Морозова Е.А. Киберпреступность как угроза международной безопасности в современности мире // Сборник статей Международной научно-практической конференции, Издательство МЦИИ ОМЕГА САЙНС. – 2018;

Морозова Е.А. Инсайдерство как преступление в сфере компьютерной информации // Аллея науки, Издательство ИП Шелистов Д.А. (Издательский центр «Quantum»). – 2019;

Структура представленного исследования состоит из введения, двух глав, включающих в себя шесть параграфов, заключения и списка использованной литературы.

ГЛАВА 1. ТЕОРЕТИЧЕСКИЕ АСПЕКТЫ СОВЕРШЕНИЯ МОШЕННИЧЕСКИХ ДЕЙСТВИЙ В СЕТИ ИНТЕРНЕТ

1.1. История развития уголовно-правового понятия мошенничества

Мошенничество – одно из уголовно-наказуемых деяний, закрепленное в ст. 159 Уголовного кодекса Российской Федерации (далее – УК РФ), согласно которой это «хищение чужого имущества или приобретение права на чужое имущество путем обмана или злоупотребления доверием»[1]. Обратим внимание, что помимо основного состава мошенничества, законодатель обособил в уголовном законе следующие его разновидности:

1. Мошенничество в сфере кредитования (ст. 159.1 УК РФ);
2. Мошенничество при получении выплат (ст. 159.2 УК РФ);
3. Мошенничество с использованием электронных средств платежа (ст. 159.3 УК РФ);
4. Мошенничество в сфере страхования (ст. 159.5 УК РФ);
5. Мошенничество в сфере компьютерной информации (ст. 159.6 УК РФ).

На наш взгляд, прежде чем предметно рассматривать основной состав преступления, необходимо проанализировать его историко-практическое определение. Как справедливо замечает А.П. Брагин, термин «мошенничество» демонстрирует тесную связь языка и социальных реалий государства уже на протяжении нескольких веков[2]. Первые упоминания о мошенничестве относятся к древнеримскому периоду, откуда в результате рецепции перекочевали в российское право. Впрочем, немаловажен тот факт, что древнеримские юристы не давали четкого определения

---

[1] Уголовный кодекс Российской Федерации от 13 июня 1996 № 63-ФЗ (ред. от 27.12.2018) (с изм. и доп., вступ. в силу с 08.01.2019) // Российская газета. 18.06.1996. № 113; СПС «Консультант плюс». 2019.

[2] Брагин А.П. Российское уголовное право. М.: ЕАОИ, 2008. С. 357.

мошенничества, но относили его к категории тяжких деяний, вследствие чего начиная с начала периода правления императора Адриана в 76 г. лиц, которые использовали обман в целях завладения имуществом и иных корыстных целях, ссылали на дальние острова, где люди фактически были обречены на голодную смерть[1].

В ранних памятниках российского права рассматриваемый состав преступления отсутствовал. Например, одним из первых документов, который регламентировал имущественные отношения, являлась Русская Правда, однако в ней упоминались такие составы преступления как разбой, кража, самовольное пользование чужим имуществом и др.[2] В Псковской Судной грамоте рассматриваемый состав преступления также отсутствует[3].

В Судебнике 1497 года, созданном в период правления Ивана III, несмотря на развитие законодательства об ответственности за имущественные преступления, о хищениях, совершенных путем обмана, речи не было.

Впервые мошенничество как полноценное преступление получило свое отражение в Судебнике Ивана Грозного 1550 года, ст. 58 которого гласила: «Мошеннику та ж казнь, что и татю. А хто на оманщике взыщет и доведут на него, ино у иш,еи иск пропал. А оманщика, как его мы приведут, ино его бити кнутьем». Опираясь на анализ приведенной нормы, мы можем утверждать, что в данном источнике российского права, впервые официально употреблен термин «мошенник», однако его смысл не был идентичен современному[4]. И.В. Фефлов справедливо утверждает, что рассматриваемое определение произошло от слова «мошна», что означает «карман»[5]. Соответственно, и «мошенник» интерпретировался как «карманник,

---

[1] См.: Покровский И.А. История Римского права. М.: Юстицинформ, 2002. С. 394.
[2] Русская Правда в краткой редакции (с переводом). URL: www.hrono.ru (дата обращения: 07.01.2019).
[3] См. там же.
[4] Судебник 1550 года. URL: yakov.works/acts/16/2/pravo_02.htm (дата обращения: 09.01.2019).
[5] Февлов И.В. Происхождение и развитие российского и зарубежного законодательства о мошенничестве // Территория науки. 2014. № 2. С. 14.

карманный вор, воришка, обманщик». И.Я. Фойницкий придерживался сходного мнения, указывая, что мошенничество в период XVI – XVII вв. – это одна из разновидностей татьбы, которая выражалась в совершении мелкой кражи, а сам термин произошел от слова «мошна»[1]. Таким образом, ученый предлагал рассматривать мошенничество как карманную кражу. В своей работе «Мошенничество по русскому праву» он говорил, что «мошенничество – это быстрый способ совершения кражи (например, срывание шапки прохожего)». М.И. Сизиков указывал, что мошенничество есть ни что иное как карманная кража[2]. Приведенные позиции нередко оспаривались иными учеными. Так, М.Ф. Владимирский-Буданов указывал, что тексте Судебника 1550 г. слово «мошенник» стоит рядом со словом «обманщик», следовательно и состав преступления следует рассматривать как похищение чужих вещей посредством обмана[3].

Мы считаем, что, опираясь на лингвистический анализ термина «мошенничество» в проекции на период его возникновения, рассматриваемое преступление скорее следует приравнивать к карманной краже. В пользу приведенного тезиса свидетельствует и то, что в ст. 58 Судебника 1550 года указывается три вида преступников – мошенник, тать и обманщик, однако для первых двух наказание одинаковое («мошеннику та ж казнь, что и татю…»), а для обманщика – битье кнутом. Таким образом, мошенничество так или иначе было связано с татьбой и приравнивалось к нему.

Впервые мошенничество как способ хищения было закреплено в Судебнике Федора Иоанновича 1589 года. Ст. 112 данного документа гласила, что «а хто на мошеннике или на оманщике взыщет того, что его оманул, и хоти его трою днем изымаешь и доведешь на него, ино его бити кнутом, а исцева иску не правити, потому что один оманывает, а другой

---

[1] Фойницкий И.Я. Мошенничество по русскому уголовному праву. С.-Пб.: Общественная польза, 1871. С. 243.

[2] Сизиков М.И. История государства и права России с XVII до начала XIX века. М.: ЮрЛит, 1998. С. 103.

[3] Владимирский-Буданов М.Ф. Обзор истории русского права. М.: Астрель, 2005. С. 157.

догадывайсе, а не мечися на дешевое»[1]. Суть данного тезиса, по справедливому замечанию М.Ф. Владимирского-Буданова, заключается в следующем: тот, кто выдвигает иск против мошенника или обманщика в течении трех дней с момента совершения преступления и свой иск докажет, то преступник будет подвергнут наказанию в виде битья кнутом. Частный же иск не будет удовлетворен ни при каких обстоятельствах, так как в то время как один человек обманывает, второй – должен догадаться об этом, а не льститься на дешевизну предлагаемого товара. Таким образом, вина за совершение преступления возлагается на обе стороны, что было обусловлено прежде всего менталитетом и укладом жизни того времени[2].

Мы также полагаем, что в данной статье Судебника 1589 года мошенничество обособляется от карманной кражи и постепенно начинает трансформироваться в самостоятельный состав преступления.

Следующим источником права, заслуживающим внимания, является Соборное Уложение 1649 года, принятое Земским собором. Его особенностью является то, что несмотря на существование более совершенной нормы о мошенничестве в вышеупомянутом судебнике, в гл. XXI ст. 11 Уложения она полностью продублировала ст. 58 Судебника 1550 года: «Да и мошенником чинить тот же указ, что указано чинить татем за первую татьбу»[3]. Иначе говоря, мошенничество вновь было приравнено к карманной краже. Одновременно с этим, в Уложении 1649 года закреплен ряд норм, предусматривающих наказание за присвоение чужой земли посредством обмана. Так, ст. 211 гласит, что «а будет кто похочет чюжею землею завладети насильством, и для того ту чюжую землю хлебом посеет, и учнет ту землю называти своею землею и в том на него будут челобитчики, и с суда про то сыщется допряма, что он ту чюжую землю хлебом посеял насильством для того, чтобы ему тою землею завладети, и тот весь хлеб,

---

[1] Судебник Федора Иоанновича. URL: https://www.prlib.ru (дата обращения: 12.01.2019).
[2] Владимирский-Буданов М.Ф. Обзор истории русского права. М.: Астрель, 2005. С. 158 – 159.
[3] Соборное Уложение 1649 года. URL: www.hist.msu.ru (дата обращения: 12.01.2019)

сколько на той земле будет посеяно, отдати тому, чья земля»[1]. Иначе говоря, лицо, которое в попытке присвоить чужой участок земли, посеет на нем хлеб, при наличии свидетельских показаний, лишается урожая, который отходит настоящему владельцу земли. С точки зрения современного законодательства, данные деяния можно было бы назвать мошенническими, однако в данном случае оно было выделено в отдельную категорию.

А.Н. Игнатов полагает, что мошенничество на Руси в современном понимании возникло в конце XVI – начале XVII века, что связано с активным развитием торговой деятельности[2]. В частности, формировались такие виды преступлений обман в количестве или качестве товара.

Впервые понятие мошенничества было раскрыто в Указе от 3 апреля 1781 г. «О суде и наказаниях за воровство разных родов и о заведении рабочих домов во всех губерниях», статья 5 которого выглядела следующим образом: «воровство мошенничество есть, буде кто на торгу или в ином многолюдстве у кого из кармана что вынет или обманом, или вымыслом, или внезапно у кого что отъимет, или унесет… или, купя, не платя денег, скроется, или обманом, ли вымыслом продаст, или отдаст поддельное за настоящее, или весом обвесит, или мерою обмерит, или что подобное обманом или вымыслом себе присвоит ему не принадлежащее, без воли, без согласия того, чье оно»[3]. Впрочем, говорить о том, что данная норма содержит в себе характеристику состава мошенничества в современном понимании нельзя, так как в указанной диспозиции отражены признаки иных способов хищение, например, кражи, грабежа и разбоя. Одновременно с этим впервые содержалось указание на главный признак мошенничества как уголовно-наказуемого деяния, отделяющего его от иных имущественных

[1] См. там же.
[2] Игнатов А.И. Уголовное право России. М: Статут, 2013. С. 133.
[3] Именной указ от 3 апреля 1781 г., данный Сенату «О суде и наказаниях за воровство разных родов и о заведении рабочих домов во всех Губерниях». URL: https://base.garant.ru/58105240/ (дата обращения: 12.01.2019)

преступлений – обман или злоупотребление доверием[1]. С момента принятия данного указа, начинается активное развитие законодательства, затрагивающего вопрос наступления ответственности за преступление совершенное путем обмана. Так, Устав Благочиния 1782 года предусматривал несколько видов имущественного обмана: обман в торговле, контрабанда и банкротство[2]. При этом необходимо обратить внимание на то, что смысл слова «обман» в тексте рассматриваемого документа был неоднозначен. С одной стороны, под обманом подразумевалось действие, которое ввело в заблуждение потерпевшего, а с другой – действие, рассчитанное на внезапность, лишающее потерпевшего возможности оказать противодействие преступнику. Важно, в обоих случаях, преступление должно иметь корыстную направленность и совершаться без применения какого-либо насилия к потерпевшему.

Свод законов уголовных, изданный в 1832 году выделял две разновидности преступлений, совершенных обманным путем: имущественные обманы и лживые поступки (или подлоги)[3]. Таким образом, по сравнению с предыдущим правовым актов сильных преобразований не произошло.

Например, в Уложении «О наказаниях уголовных и исправительных» 1845 года в разделе 12 «О преступлениях и проступках против собственности частных лиц» в главе 3 «О похищении чужаго имущества» содержалась ст. 1665, согласно которой «мошенничеством признается всякое, посредством какого-либо обмана учиненное похищение чужих вещей, денег или инаго движимаго имущества»[4]. Таким образом, именно в данном нормативном

---

[1] Иванов Н.Г. Уголовное право: учебник для бакалавров // Biblioclub.ru: университетская бибилиотека online. М., 2018. URL:http://biblioclub.ru/ (дата обращения: 13.01.2019)

[2] Устав Благочинияили Полицейский 1782 г. URL: музейреформ.рф/ (дата обращения: 13.01.2019).

[3] См.: Хапов К.Г. Мошенничество как форма хищения чужого имущества в истории российского законодательства (основные тенденции развития уголовного регулирования) // Общество и право. 2017. № 9. С. 10.

[4] Уложение «О наказаниях уголовных и исправительных» 1845 года. URL: музейреформ.рф/ (дата обращения: 13.01.2019).

правовом акте впервые мошенничество содержит в себе все основные признаки – хищение, совершенное путем обмана или злоупотребления доверием.

В 1922 году принимается Уголовный Кодекс РСФСР, где законодатель значительно упростил конструкцию рассматриваемого преступления. В частности, ст. 187 определяла мошенничество как «получение с корыстной целью имущества или права на имущество посредством злоупотребления доверием или обмана»[1]. В уголовном кодексе РСФСР 1926 года мошенничество получает более развернутую формулировку с указанием способа совершения преступления (злоупотребление доверием или обман) и цели (получение «чужого имущества или права на имущество или иных личных выгод»[2]). Данные признаки сохранились и при принятии Уголовного кодекса РСФСР 1960 года, и Уголовного кодекса Российской Федерации 1996 года, действующему до сих пор.

На основании вышеизложенного мы можем сделать вывод, что уголовно-правовая норма о мошенничестве в российском законодательстве появилась достаточно поздно, лишь во второй половине XVI века. Лингвистический анализ термина «мошенничество» дает право предположить, что первоначально мошенничество подразумевало под собой карманную кражу. Основополагающий же признак рассматриваемого состава преступлений – обман или злоупотребление доверием – укрепился в уголовном законе лишь в XVIII веке. Таким образом, «мошенничество» с течением времени утратило свое лексическое значение употребляемого в качестве соответствующего термина существительного.

---

[1] Постановление ВЦИК от 01.06.1922 (ред. от 25.08.1924) «О введении в действие Уголовного Кодекса Р.С.Ф.С.Р.» (вместе с «Уголовным Кодексом Р.С.Ф.С.Р.») // СУ РСФСР. 1922. № 15; СПС «Консультант Плюс».

[2] Постановление ВЦИК от 22.11.1926 (ред. от 27.04.1959) «О введении в действие Уголовного Кодекса Р.С.Ф.С.Р. редакции 1926 года» (вместе с «Уголовным Кодексом Р.С.Ф.С.Р.») // СУ РСФСР. 1926. № 80; СПС «Консультант Плюс».

Помимо прочего, хотим отметить, что специфика современного законодательного описания мошенничества заключается в том, что в нем содержится указание два способа совершения преступления (обман и злоупотребление доверием) и два предмета посягательства (чужое имущество или право на чужое имущество).

1.2. Понятие и признаки киберпреступности

Проблема борьбы с киберпреступностью – это одна из наиболее приоритетных задач, стоящих на сегодняшний день перед государством.

Впервые термин «киберпреступность» начал применяться в зарубежной печати в начале 60-х гг. XX века, когда были впервые зафиксированы случаи правонарушений, совершенных посредством ЭВМ. В 90-е гг. XX века ознаменовалось повсеместным распространением глобальной сети «Интернет», чьи технологические и коммуникационные возможности привели к резкому и динамическому росту количества пользователей Сети во всем мире[1]. На сегодняшний день национальная инфраструктура любого государства тесно связана с использованием современных компьютерных технологий, а ежедневная деятельность энергетических, транспортных и иных систем находятся в прямой зависимости от правильной и надежной работы автоматизированных электронно-вычислительных систем.

В современной юридической литературе киберпреступность определяется как 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, и против компьютерных систем,

[1] См.: Згадзай О.Э. Предупреждение кибепреступности. Проблемы и решения // Вестник Казанского юридического института МВД России. 2011. № 9. С. 16.

компьютерных сетей или компьютерных данных[1]. Таким образом, в рамках настоящего исследования мы будем отождествлять термины «преступления в сфере компьютерной информации» и «киберпреступления», выходя в своих научных изысканиях за рамки составов, предусмотренных Главой 28 УК РФ «Преступления в сфере компьютерной информации».

Необходимо акцентировать внимание, что ущерб, причиняемый киберперступлениями ежегодно исчисляется в миллиардах. Согласно данным статистики, по итогам 2016 года потери России от преступлений в сфере компьютерной информации составили 2,87 млрд. рублей[2].

Помимо прочего, по данным ЗАО «Лаборатория Касперского», ежедневно возникает до 70 тыс. новых вредоносных программ. Более того, злоумышленники все чаще применяют новые способы заражения, стремятся действовать в обход киберзащиты. За последние пять лет, около 90% российских компаний фиксировали инциденты в сфере IT-безопасности разной степени опасности. По результатам социологического опроса, проведенного А.А. Галушкиным, более половины опрошенных специалистов по информационной безопасности признало факт потери важных данных ввиду заражения вредоносным программным обеспечением[3]. При этом, в подавляющем большинстве случаев инциденты в сфере IT-безопасности приводят к утрате данных, касающихся финансовых вопросов (13%), интеллектуальной собственности (13%), клиентских баз (12%), информации о сотрудниках (12%) и пр. При этом, анализ атак, зафиксированных «Лабораторией Касперского» по состоянию на начало 2017 года свидетельствует о том, что на первый план выходят все более серьезно и разностороннее подготовленные организаторы и исполнители кибератак.

---

[1] См.: Номоконов В.А. Киберпреступность как новая криминальная угроза // Криминология: вчера, сегодня, завтра. 2012. № 24.

[2] Ущерб от хакерских атак на банки в 2016 году. URL: http://www.tadviser.ru/ (дата обращения: 01.03.2018).

[3] См.: Евдокимов К.Н. Актуальные вопросы совершенствования уголовно-правовых средств борьбы с компьютерными преступлениями // Вестник Казанского юридического института МВД России. 2016. № 2. С. 4 – 8.

Согласно отчету NCR (Norton Cybercrime Report)[1], потерпевшими от киберпреступлений по итогам 2016 года стали 689 млн. человек, что на 10% больше, чем в предыдущем 2015 году. При этом общий ущерб, причиненный мировому сообществу, составил 388 млрд. долларов, а стоимость работ, необходимых для восстановления инфраструктуры безопасности после осуществленных кибератак, составляет примерно 248 млрд. долларов[2].

Другим аспектом опасности киберпреступлений является их транснациональность, то есть данный вид преступности не знает государственных границ. Справедливо будет утверждать, что ни одно государство современного мира, даже самое высокоразвитое, не способно противостоять ей самостоятельно, что обуславливает необходимость налаживания международного сотрудничества, в частности активизации международно-правового механизма регуляции. Однако мы также должны отметить, что существенная часть средств борьбы с киберпреступностью принадлежит к национальной компетенции каждого государства, поэтому необходимо параллельно налаживать не только международный аспект сотрудничества, но и развивать внутреннее законодательство страны, опираясь на зарубежный опыт и международные правовые нормы.

Однако для того, чтобы охарактеризовать преступление как «киберпреступление», необходимо дать определение самому термину «киберпространство». Впервые оно было введено американским писателем-фантастом У. Гибсоном в его романе «Нейромант», где киберпространством он именовал «консенсуальную галлюцинацию», которую «трудно отключить реальности и в которой компьютерные системы являются своего рода заменой реального мира, существующего только в памяти компьютеров и

---

[1] Отчет Norton Cybercime Report - это одно из крупнейших в мире исследований киберпреступности в потребительском сегменте. В исследовании ежегодно принимает участие более 13 тыс. человек из 24 стран, и его цель – понять, какое влияние киберпреступность, а также развитие и внедрение новых технологий оказывают на пользователя и его безопасность.

[2] Group-IB представила отчет о киберпреступности и призвала рынок к хантингу. URL: https://www.group-ib.ru/ (дата обращения: 09.02.2019).

умах его пользователей»[1]. Таким образом, киберпространство первоначально имело скорее литературно-художественное значение, нежели доктринально-правовое.

Весьма интересной представляется схема киберпространства, предложенная М. Бэтти, который в его «географии» четыре основных уровня:

1. место, которое соответствует географическому положению, или научному определению пространства;

2. виртуальное пространство, которое создано в компьютерах на основе реального места в мире;

3. киберпространство, которое постепенно развивается благодаря компьютерным сетям;

4. мир киберместа, который выступает в качестве посредника киберпространства и относится к месту в географическом смысле.[2]

Циркуляционная модель М. Бэтти проиллюстрирована на рис. 1.1.

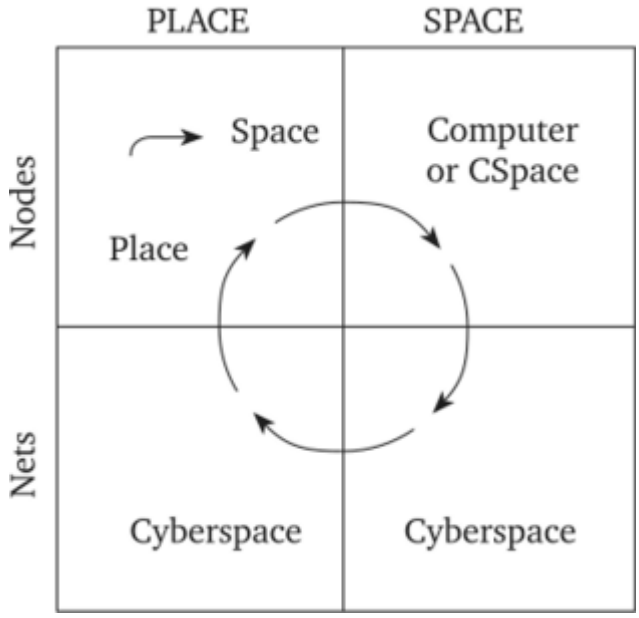


Рис. 1.1.

[1] Гибсон У. Нейромант. М.: АСТ, 1997. С. 118.
[2] Бетти Э. Герменевтика как общая методология наук о духе. М.: Перо, 2011. С. 11.

На основании вышеизложенного можно сделать вывод, что киберпространство – это пространство, которое схоже с географическим пространством, соединяющее все пространства в единое целое, хотя границы между ними размыты. Это достаточно широкое по своему смыслу понятие, одним из элементов которого является Интернет.

В киберпространстве ежедневно совершается огромное количество самых разнообразных преступлений, которые с каждым разом становятся все более изощренными. Наиболее широко в сети распространены экономические преступления, в частности мошенничество. Не менее «популярным», особенно с учетом существующей политической обстановки, стал так называемый «информационный терроризм». Кроме того, с помощью коммуникационных сетей совершаются такие преступления как незаконный оборот оружия, наркотических и психотропных веществ, торговля людьми, органами, незаконное распространение порнографии и пр. Сложность расследования указанных преступлений состоит в том, что их отличает высокая степень латентности, а также невозможность отслеживания всех интернет-ресурсов, содержащих запрещенные законом данные[1].

Помимо прочего, мы не можем не принимать во внимание тот факт, что расширяющаяся глобализация современного мира и информационного пространства, в частности, способствует созданию новых способов, средств и объектов преступных киберпосягательств[2]. Более того, киберпространство все чаще используется в целях пропаганды политической идеаологии, обмена опытом в достижении международных преступных экономических и политических целей. Для этого, спецслужбы различных государств на системной основе задействуют ресурс сети Интернет для реализации

---

[1] Тулегенов В.В. Киберпреступность как форма выражения криминального профессионализма // Вестник Южно-Уральского государственного университета. Серия Право. 2018. № 1. С. 74.

[2] Сверчков В.В.Уголовное право. Особенная часть // Biblio-online.ru: электронно-библиотечная система «Юрайт». М., 2019. URL: https://www.biblio-online.ru/ (дата обращения: 13.01.2019).

взаимодействия и координации подрывных действий, а также ведения кибервойн.

По утверждению Д.Н. Карповой, что, впрочем, является общеизвестным фактом, возможности телекоммуникационных сетей повсеместно были задействованы для формирования «цветных» революций на территории Ирака, Ливии и Сирии[1]. Более того. сложно не согласиться с В.В. Бондарь, который утверждает, что обнаруженный в 2010 году вирус типа «червь» Worm.Win32.Stuxnet был специально разработан по совместной инициативе спецслужб США и Израиля в целях осуществления кибератак, направленных на разрушение центрифуг, обогащающих уран в Иранском ядерном центре в Бушере[2]. При этом, в ходе проведения данной кибератака, была повреждена большая часть оборудования. В этой связи, технический директор компании Bit9 Гарри Свердлав совершенно справедливо говорит, что подобные атаки являются причиной формирования гонки кибервооружения стран, и те государства, которые ранее не планировали участие в ней, будут активно вовлекаться в данную сферу[3]. Обратим внимание, что создание данной программы вызвало широчайший международный резонанс, а американская газета New York Times даже опубликовала сенсационную статью, в которой «приписывала» распоряжение о создании вируса-червя Stuxnet президенту США Бараку Обаме. Белый Дом оставил данное заявление без каких-либо комментариев, однако факт существования данного средства осуществления кибератак – налицо.

Продолжая рассмотрение вопроса о создании новых способов компьютерных атак, обратим внимание на международный резонанс, который вызвало создание в 2011 году троянской программы Duqu, которая предоставила преступникам возможность получения несанкционированного

---

[1] Карпова Д.Н. Киберпреступность: глобальная проблема и ее решение // Власть. 2014. № 1. С. 89.

[2] Бондарь В.В. Киберпреступность – современное состояние и пути борьбы // Юридические записки. 2013. № 7. С. 1 – 6.

[3] Червь Stuxnet. URL: http://www.tadviser.ru/ (дата обращения: 20.02.2019).

доступа к информационной инфраструктуре безопасности, а затем и «выкачке» размещенной на взломанных серверах информации[1]. Позднее иранские информационные системы были атакованы вирусом-червем под названием «Flame», который по утверждению Гарри Свердлава «по своим размерам превосходит оригинальный Stuxnet»[2]. Таким образом, год от года планка совершенствования средств кибератак становится все выше, а методы – более изощренными. Мы не будет голословными, если констатируем, что «апофеоз» количества кибератак пришелся на 2015 – 2016 год. Так, в 2015 году в результате кибератаки Carbanak пострадало боле сотни банков и иных кредитных организаций США, каждому из которых был нанесен ущерб в пределах от 1,5 до 10 млн. долларов. Летом того же года, кибератаке подверглось американское управление кадров, в результате которой произошла утечка личных биографических данных более 20 млн. человек, включая американских военнослужащих и лиц, находящихся на государственной службе[3].

Осенью 2016 была совершена кибератака против DNS-провайдера США «Dyn», в результате которой был отключен от сети Интернет ряд крупнейших международных веб-сайтов, например Twitter, Amazon, а также веб-сайт газеты The New York Times[4]. Работа всего сервиса была нарушена на 11 часов, в результате чего потерпевшими оказались более 1 млрд. пользователей по всему земному шару.

Обратим внимание, что на сегодняшний день кибератаки производятся не только на правительственные информационные системы – киберпреступники «двигаются навстречу прогрессу семимильными шагами». На сегодняшний день, не существует сферы, где не было бы потенциальной информационной угрозы. В частности, уже достоверно известно, что

---

[1] Что такое вирус Flame. URL: http://fb.ru/article/68993/ (дата обращения: 17.02.2019).
[2] Червь Stuxnet. URL: http://www.tadviser.ru/ (дата обращения: 17.02.2019).
[3] Самые громкие кибератаки 21 века. URL: https://geekbrains.ru/ (дата обращения: 17.03.2018).
[4] Что случилось с Twitter, PayPal, Amazon и другими американскими сервисами. URL: https://www.kaspersky.ru/ (дата обращения: 22.02.2019)

«новым» полем деятельности киберпреступников становится область автомобилестроения[1]. Обусловлено это тем, что современные автомобили представляют собой продвинутые с технологической точки зрения агрегаты, в которых встроенный бортовой компьютер способен управлять подавляющим большинством основных функций машины, в том числе торможением или расходом топлива. Киберпреступники уже научились брать под контроль бортовые персональные компьютеры таких автомобилей, например, в США преступнику с помощью несложных современных технологий удалось взять под полный контроль Jeep Cherokee на расстоянии пятнадцати километров[2]. В частности, киберпреступник получил возможность управлять работой тормозной системы.

Не менее наглядно возможности киберпреступников демонстрирует инцидент в США, произошедший также в 2016 году. Тогда в нагрудных камерах американских полицейских было обнаружено вредоносное программное обеспечение, которое запускалось при подключении камеры к персональному компьютеру. В случае слабой антивирусной защиты, под угрозой оказывалась важная информация, в том числе и биографического конфиденциального характера. Несмотря на то, что этот случай не представляет собой спланированную атаку, однако он наглядно демонстрирует возможности современных преступников[3].

В последние годы также широкое распространение по всему миру получили два основных вида киберпреступлений: инсайдерство (Insiders) и хакерство (hackers)[4].

Инсайдерство происходит от английского «inside», что означает «внутри». Инсайдерами именуют лиц, которые обладают доступом к

---

[1] См.: Листеренко Р.Р. Продвинутые атаки требуют новых видов защиты информации // Вопросы кибербезопасности. 2013. № 7. С. 52.

[2] В США хакеры отключили тормоза Jeep Cherokee через интернет. URL: http://www.kolesa.ru/ (дата обращения: 17.04.2017).

[3] Топ-5 самых опасных целей кибератак мира 2016 года. URL: http://vsekommentarii.com/news/ (дата обращения: 18.04.2017).

[4] См.: Чекунов И.Г. Киберпреступность: понятие и классификация // Российский следователь. 2012. № 2.

внутренней информации. Как правило, это действующие или бывшие сотрудники крупных компаний, которые хорошо знакомы с особенностями компьютерной системы фирмы и обладают возможностью несанкционированного доступа к внутренней системе с целью вмешательства в работу автоматизированных систем[1].

На сегодняшний день выделяют три основных вида инмсайдерских атак: мошенничество, саботаж и кража интеллектуальной собственности. При этом, выявление инсайдерской атаки представляет существенные сложности для системы внутренней информационной системы безопасности, так как из общего потока информации и событий необходимо выявить именно те, которые являются вредоносными. Например, не так давно нападению инсайдера по имени Монтгомери Джона Грея подверглась Национальная библиотека медицинской литературы, к которой обращаются сотни и тысячи врачей ежедневно по всему миру. Злоумышленник совершил незаконный доступ к главной системе защиты имеющейся в системе информации и загрузил сотни файлов, в том числе наиболее важные и файлы программного обеспечения, от которых зависела бесперебойная работа всей системы. Действия преступника причинили ущерб в размере 25 тыс. долларов[2].

В контексте рассматриваемого вопроса обратим внимание, что российская компания InfoWatch выделяет шесть основных видов инсайдеров:

«Халатный» («неосторожный») – это сотрудник, соответствующий образу служащего рядового состава. необременноного интеллектом, однако отличающиеся крайней невнимательностью. Как правило, совершаемые ими нарушения носят немотивированный характер и не преследуют корыстных

---

[1] См.: Веденеев В.С. Система выявления инсайдеров // Математические структуры и моделирование. 2014. № 7. С. 33.

[2] См.: Карпова Д.Н. Киберпреступность: глобальная проблема и ее решение // Власть. 2014. № 1. С. 90.

или умышленных целей[1]. Типичный пример подобного инсайдерства – вынос информации из офиса с целью работы с ней дома или в командировке с последующей утратой носителя информации или случайным доступом к ней третьих лиц. Несмотря на то, что данный вид инсайдерства не носит злонамеренный умышленный преступный характер, урон от нее может быть не меньше, чем от промышленного шпионажа.

«Манипулируемый» инсайдер – это лицо, которое «выводит» стратегически важные сведения из информационной системы компании или предприятия «под воздействием» других лиц, действующих с преступным умыслом[2]. Для более прозрачного понимания, проиллюстрируем данный вид инсайдерства примером. На рабочий телефон одного из сотрудников офиса раздается телефонный звонок. Звонящее лицо, представившись директором одного из филиалов компании, весьма убедительно и правдоподобно сообщает о проблеме, которая связана с невозможностью доставки почты из головного офиса в филиал и просит переслать ему определенную информацию на его личный почтовый ящик. Если сотрудник обладает определенной неосмотрительностью и ничего не заподозрит, то, несомненно, он отправит на почтовый адрес злоумышленника сведения, которые в подавляющем большинстве случаев представляют собой конфиденциальную информацию, и в руках преступника окажутся сведения, использование которых в преступных целях может принести компании невосполнимый ущерб.

Данные виды инсайдеров относятся к категории незлонамеренных, так как их действия хоть и связаны с «обеспечением» утечки внутренней информации, однако совершаются не из преступного и (или) корыстного или

---

[1] Астахов К.В. Информационная безопасность как аспект стабильности экономических отношений на различных уровнях хозяйствования // Социально-экономические явления и процессы. 2018. № 3. С. 27.

[2] Бородакий Ю.В. Инсайдерология: наука о нелигитимности в компьютерной инфосере // Технические науки. 2017. № 10. С. 55.

иного умысла[1]. Однако, есть и такие инсайдеры, которые преследуют совершенно другие цели и именуются «злонамеренными».

«Обиженные» (или саботажники) – это лица, которые имеют своей целью нанесение вреда компании по личным мотивам, в качестве которых выступают месть за незаконное, на их взгляд, увольнение, низкую заработную плату, отказ в предоставлении отпуска или каких-либо льгот и т.д. При этом характерными чертами такого инсайдерства является, во-первых, отсутствие у сотрудника намерения покинуть компанию, а во-вторых – цель инсайдера – нанести вред компании, а не похитить информацию. Таким образом, его деятельность носит деструктивный характер по отношению к самой компании в целом.

«Нелояльные» инсайдеры – это сотрудники, которые приняли решение изменить место работы или открыть собственный бизнес. Сущность такого инсайдерства заключается в том, что увольняющийся работник стремится унести с собой как можно больше информации, которая пригодится им в будущем, например, копии клиентской базы, финансовые документы и пр. Наиболее часто, нелояльных инсайдеров «ловят» на имитации производственной необходимости, когда они требуют информацию, ознакомление с которой явно выходит за рамки их служебной компетенции[2].

«Подрабатывающие» инсайдеры – это сотрудники, главной целью которых является та, которую, определяет заказчик похищения информации. Данный тип инсайдерства охватывает весьма широкий спектр сотрудников компании, которым не хватает материальных средств для каких-либо нужд, нехватку которых они пытаются покрыть осуществлением деятельности по инсайдерству за определенную плату[3]. Таким образом, их преступная

---

[1] См. об этом подробнее: Маркова Т.И. Классификация инсайдеров // Вестник Волжского университета им. В.Н. Татищева. 2016. № 25.

[2] См.: Мамочка Е.А. Доказывание вины лица в инсайдерских преступлениях // Бизнес в законе. Экономико-юридический журнал. 2015. № 16. С. 31.

[3] См.: Лопатин Д.В. Безопасность пользователей инфокоммуникационных технологий // Естественные и технические науки. 2018. № 8. С. 46.

деятельность не является систематической, а носит разовый нерегулярный характер.

«Внедренные» инсайдеры – это сотрудники, основной целью которых является государственный и промышленный шпионаж с помощью инсайдерских способов доступа к информации[1]. При этом злоумышленники придумывают весьма изощренные, но одновременно с этим и простые способы внедрения «своего» человека в эшелоны сотрудников крупных компаний. Например, системному администратору приходит весьма привлекательное предложение о переходе на другую работу, которое включает в себя полный соцпакет, гибкий график и высокую заработную плату. одновременно с этим, работодателю приходит резюме на должность уволившегося системного администратора, от которого директор не может отказаться. В то время, пока увольняющийся сотрудник сдает свои дела, второй приобретает доступ к конфиденциальной информации и передает ее заказчику. После этого, его следы «исчезают», и компания остается без информации, а бывший сотрудник – без работы вовсе.[2]

Таким образом, инсайдеры могут совершать следующие виды правонарушений, которые нередко приносят ущерб не только финансовому благосостоянию компаний, но и ее деловой репутации и положению на рынке оказываемых услуг:

1. Разглашение конфиденциальной информации;

2. Кража конфиденциальной информации (например, с помощью взлома корпоративных сетей);

3. Нарушение авторских прав на информацию;

4. Нецелевое использование ресурсов компании.[3]

---

[1] См.: Маркова Т.И. Классификация инсайдеров // Вестник Волжского университета им. В.Н. Татищева. 2016. № 25. С. 29.

[2] См.: Сычев В.М. Формализация модели внутреннего нарушителя информационной безопасности // Приборостроение. 2015. № 8. С. 14.

[3] См.: Овчинников С.А. Организационно-кадровый аспект безопасности: проблема инсайдерской угрозы электронному правительству // Вестник саратовского государственного социально-экономического университета. 2012. № 7. С. 16.

Что касается хакерства, то они представляют еще большую опасность, чем инсайдеры, потому что они взламывают компьютерные сети ради получения острых ощущение или завоевания авторитета в хакерских кругах, а иногда – и с целью извлечения личной финансовой выгоды. Трудность поимки хакеров заключается в том, что они в своем большинстве являются прекрасными знатоками информационных технологий, обладают высокой интеллектуальной развитостью и неординарными способностями[1]. Кроме того, профессиональные хакеры умело «подчищают» следы своего пребывания в сети, что делает их поимку практически невозможной. Как показывает практика, от хакерских атак не застрахованы ни посредственные пользователи компьютерных сетей, ни государственные и международные органы и организации. Так, например, 28 июля 2013 года хакеры из группировки Anonymous взломали несколько правительственных сайтов в Перу, в том числе сайт президента Ольянты Умалы. В марте 2014 года китайские хакеры атаковали компьютерные системы правительства США и получили доступ к некоторым базам данных федеральных госслужащих, а 4 апреля 2016 года неизвестные хакеры опубликовали на румынском сайте архив с данными, содержащими персональную информацию о почти 50-ти млн. турецких граждан, в том числе и президента Турции Реджела Тайипа Эрдогана и премьер-министра Ахмета Давутоглу[2].

На основании вышеизложенного следует сделать вывод, что на сегодняшний день от киберпрестулений в полной мере не защищена ни одна база данных, что обуславливает необходимость осуществления исследований в сфере компьютерных технологий и защиты информации в целях создания универсального средства защиты государственных и частных данных от несанкционированного к ним доступа.

---

[1] См.: Афанасьева Д.В. Проблема DDOS-атак // Наука, образование, культура. 2019. № 1. С. 50.

[2] Крупные атаки хакеров в 2001-2016 годах: хронология. URL: http://tass.ru/ (дата обращения: 19.04.2017).

Все вышеперечисленное в совокупности одной из основных задач государства ставит проведение активной политики, направленной на совершенствование механизма расследования и раскрытия киберпреступлений.

ГЛАВА 2. ХАРАКТЕРИСТИКА СОСТАВА МОШЕННИЧЕСТВА В КИБЕРПРОСТРАНСТВЕ

2.1. Объективные признаки мошенничества в киберпространстве

Еще совсем недавно любое хищение путем обмана или злоупотребления доверием охватывалось исключительно статьей 159 УК РФ, однако возникновение новых способов совершения рассматриваемого преступного посягательства обусловило необходимость модернизации законодательства, вследствие чего возникли не только ст.ст. 159.1 – 159.6 УК РФ, но также и расширена диспозиция основной статьи, предусматривающей уголовную ответственность за мошенничество[1].

Мошенничество в сети Интернет обладает определенной спецификой своего состава, что, прежде всего обусловлено особенностями киберпространства как места совершения преступления. В данном параграфе мы более подробно рассмотрим специфику состава мошенничества в киберпространстве. Как известно, состав преступления включает в себя четыре основных компонента: объект, объективную сторону, субъект и субъективную сторону.

Объект. Объектом в целом являются охраняемые уголовным законом общественные отношения, на которое посягает преступление. Родовым объектом мошенничества как преступления, включенного в гл. 21 УК РФ, выступают отношения собственности между людьми относительно материальных благ[2]. Здесь отметим, что отношения собственности представляют собой отношения между людьми, которые складываются в процессе общественного производства, обмена и потребления произведенного продукта. Что касается самого понимания собственности, то

---

[1] См.: Юрочкин Н.С. Кибермошенничество: характеристика, приемы и методы его совершения // Таврический научный обозреватель. 2016. № 17. С. 44.

[2] См.: Сазонов М.М. Из истории понятия собственности // Проблемы современной науки и образования. 2018. № 4. С. 19 – 20.

мы солидарны с мнением В.В. Яновой, что с экономической точки зрения она представляет собой «установлением над материальные благами такого хозяйствующего господства, которое позволяет собственнику по своей воле устранять или допускать всех прочих лиц к использованию своего имущества, при этом самостоятельно определяя характер такого использования»[1]. Рассмотрение состава мошенничества в сфере компьютерной информации невозможно без анализа ее юридической природы. Спектр проблем, возникающих в процессе рассмотрения собственности в качестве правовой категории, включает в себя вопросы, которые связаны с понятием, содержанием права собственности, его субъектами и объектами, а также его пределами, ограничениями и защитой.

Ст. 8 Конституции РФ гласит, что «В Российской Федерации признаются и защищаются равным образом частная, государственная, муниципальная и иные формы собственности»[2]. В свою очередь гражданское законодательство выделяет триаду полномочий собственника, которая отражает сущность рассматриваемого понятия.

1. Правомочие пользования. Это возможность субъекта права эксплуатации, хозяйственного или иного использования имущества посредством извлечения из него каких-либо полезных свойств, а равно его потребления.

2. Правомочие владения. Это обеспеченная с точки зрения юриспруденции возможность хозяйствования лицом вещью.

3. Правомочие распоряжения. Это возможность определения субъектом права юридической судьбы принадлежащей ему на праве собственности вещи путем изменения ее принадлежности, состояния или назначения.

---

[1] Янова В.В. К вопросу ретроспективного анализа понятия собственности // Terra Economicus. 2010. № 13.С. 64.

[2] Конституция Российской Федерации (принята всенародным голосованием 12.12.1993) (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.2014. № 31; СПС «Консультант Плюс».

На основании вышеизложенного представляется возможным сделать вывод, что право собственности включает в себя такие элементы как правомочие владения, как самой вещью, так и правом на нее, а также распоряжением и пользованием имуществом и имущественными правами. При этом согласимся с В.М. Захаровым, что в отечественном законодательстве отсутствует прямое указание на материальность объекта права собственности в силу того, что им может выступать как материальные вещи, так и какие-либо имущественные права (например, авторские)[1].

Раскрывая объект мошенничества сфере компьютерной информации, отметим, что родовым объектом рассматриваемого вида преступного деяния выступают общественные отношения в экономической сфере. Например, одной из современных разновидностей интернет-мошенничества выступает банкинг, с которым связаны практически все убытки от несанкционированного снятия денежных средств.

Непосредственным видом мошенничества в сети Интернет выступают отношения собственности. Здесь согласимся с О.Л. Серегиной, что в уголовно-правовой науке собственности присуще комплексное понимание и куда более широкая трактовка сравнительно с положениями гражданского законодательства[2]. В уголовно-правовом смысле указанной категорией охватываются вещные и обязательственные отношения, а также иные имущественные отношения. Также обратим внимание, что для мошенничества характерен объект в виде совершенных форм собственности – корпоративной, банковской, акционерной и пр. Таким образом, в качестве основного непосредственного объекта интернет-мошенничества выступают имущественные отношения конкретного вида.

Ю.П. Фадина справедливо замечает, что рассматриваемый состав преступления относится к категории многообъектных деликтов, где в

---

[1] Захаров В.М. Социально-философское определение собственности // Вестник Челябинского государственного университета. 2011. № 12. С. 38.

[2] Серегина О.Л. Понятие защиты права собственности в общей системе способов защиты прав // Legal Concept. 2016. № 8. С. 23.

качестве дополнительного объекта может (и чаще всего выступает) общественная безопасность, легальное определение которой на сегодняшний день в отечественном законодательстве отсутствует, однако мы можем дать доктринальное толкование, основываясь на существующих определениях иных видов безопасности[1].

П. 6 Указа Президента РФ от 31 декабря 2015 № 683 «О Стратегии национальной безопасности Российской Федерации» гласит, что «национальная безопасность Российской Федерации - состояние защищенности личности, общества и государства от внутренних и внешних угроз, при котором обеспечиваются реализация конституционных прав и свобод граждан Российской Федерации, достойные качество и уровень их жизни, суверенитет, независимость, государственная и территориальная целостность, устойчивое социально-экономическое развитие Российской Федерации»[2]. Национальная безопасность включает в себя оборону страны и все виды безопасности, предусмотренные Конституцией Российской Федерации и законодательством Российской Федерации, прежде всего государственную, общественную, информационную, экологическую, экономическую, транспортную, энергетическую безопасность, безопасность личности». Таким образом, общественная безопасность – это составная часть национальной безопасности как более общего явления[3]. Следовательно, общественную безопасность мы можем характеризовать как состояние защищенности личности, общества и государства преимущественно от внутренних угроз общеопасного характера.

В рамках рассматриваемого вопроса, мы можем «сузить» дополнительный объект мошенничества в сети Интернет, так как одной из

---

[1] Фадина Ю.П. Уголовно-правовая характеристика мошенничества в сети Интернет // Вестник Югорского государственного университета. 2017. № 11. С. 103.

[2] Указ Президента РФ от 31.12.2015 № 683 «О Стратегии национальной безопасности Российской Федерации» // Собрание законодательства РФ. 2016. № 1; СПС «Консультант Плюс».

[3] См.: Жиделев В.Г. Эволюция законодательства об уголовной ответственности за совершение преступлений в сфере высоких технологий // Экономика и право. 2011 № 10. С. 14.

разновидностей общественной безопасности, является безопасность в сфере компьютерной информации. Согласно ст. 2 Федерального закона от 27 июля 2006 г. № 149 ФЗ «Об информации, информационных технологиях и защите информации», информация – это «сведения (сообщения, данные) независимо от формы их представления»[1]. В соответствии же с примечанием к ст. 272 УК РФ, компьютерная информация – это «сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи»[2]. Здесь необходимо обратить внимание на тот факт, что информационный характер носят не только личные данные пользователей, но также программное обеспечение, переписки и пр.

Потерпевшими от мошенничества сфере компьютерной информации – это физическое или юридическое лицо, которое использует ЭВМ, систему ЭВМ или их сеть, и которому преступлением причинен какой-либо вред. Таким образом, мы можем утверждать, что в случае рассматриваемого вида мошенничества будет специальный потерпевший – это лицо, которое является пользователем компьютерных сетей или устройств.

Объективная сторона. Объективная сторона мошенничества сфере компьютерной информации включает в себя три основных компонента: само общественно-опасное деяние, общественно-опасное последствие и причинно-следственную связь между ними.

Мошенничество в сфере компьютерной информации может быть выражено только действием. Согласно ст. 159 УК РФ, мошенничество – это хищение чужого имущество путем обмана или злоупотребления доверием[3], причем последние представляют собой способ совершения преступления.

---

[1] Федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 18.03.2019) «Об информации, информационных технологиях и о защите информации» //Российская газета. 2006. № 165; СПС «Консультант Плюс».

[2] Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 27.12.2018) (с изм. и доп., вступ. в силу с 08.01.2019) // Российская газета. 1996. № 113; СПС «Консультант Плюс».

[3] Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 27.12.2018) (с изм. и доп., вступ. в силу с 08.01.2019) // Российская газета. 1996. № 113; СПС «Консультант Плюс».

Начнем с того, что доверие представляет собой состояние внутреннего мира человека, которое обусловлено желанием взаимоотношений и характеризуется готовностью передачи конкретных прав и объектов соответствующих субъектов. Согласимся с А.И. Розенцвайг, что доверие – это отражение веры и уверенности одного человека в надежности и добросовестности другого или целой системы[1]. Согласно п. 2 Постановления Пленума Верховного суда РФ № 48 от 30 ноября 2017 года (далее – ПП ВС ПФ № 48 от 30 ноября 2017 г.), обман «может состоять в сознательном сообщении (представлении) заведомо ложных, не соответствующих действительности сведений, либо в умолчании об истинных фактах, либо в умышленных действиях (например, в предоставлении фальсифицированного товара или иного предмета сделки, использовании различных обманных приемов при расчетах за товары или услуги или при игре в азартные игры, в имитации кассовых расчетов и т.д.), направленных на введение владельца имущества или иного лица в заблуждение»[2]. Таким образом, различают два вида обмана – активный и пассивный. В качестве примера активного обмана, приведем следующий пример: Ч., представившись директором несуществующего санатория «Сказка», убедил пенсионера К. купить туда путевку, после чего скрылся вместе с деньгами.

Пример пассивного обмана: К. получала пособие на своего ребенка, после смерти которого не стала сообщать об этом с органы социального обеспечения, продолжая получать денежные средства.

На данных примерах легко проследить разницу между активным и пассивным обманом: в первом случае лицо умышленно сообщает лицу заведомо ложную информацию в целях получения от него денежных средств, во втором – лицо, опять же умышленно, действуя из корыстной заинтересованности, не сообщает в уполномоченные органы необходимой

---

[1] Розенцвайг А.И. К вопросу о конструкции состава «Злоупотребление доверием» // Вестник Волжского университета им. В.Н. Татищева. 2012. № 2. С. 196.

[2] Постановление Пленума Верховного Суда РФ от 30.11.2017 № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате» // Бюллетень Верховного Суда РФ. 2018. № 2; СПС «Консультант Плюс».

информации, продолжая незаконно обогащаться за счет социального пособия.

Что касается злоупотребления доверием, то в ПП ВС ПФ № 48 от 30 ноября 2017 г. оно «заключается в использовании с корыстной целью доверительных отношений с владельцем имущества или иным лицом, уполномоченным принимать решения о передаче этого имущества третьим лицам. Доверие может быть обусловлено различными обстоятельствами, например служебным положением лица либо его личными отношениями с потерпевшим»[1]. Например, К. будучи лучшим другом Н. попросил у него взаймы 50 тыс. рублей, которые обещал вложить в открытие общего бизнеса, после чего перестал отвечать на звонки и исчез.

Что касается интернет-мошенничества, на наш взгляд оно возможно путем активного обмана или злоупотребления доверием. Достаточно проблематично осуществить данное преступное деяние с помощью пассивного обмана, что объясняется, прежде всего, тем, что умысел виновного лица направлен на хищение денежных средств любыми способами, в качестве которых выступает активный обман. В качестве примера можно привести интернет-магазины, которые берут оплату за конкретный товар, однако покупатель его так и не получает. Или же обман на сайте знакомств, когда мошенник входит в доверие к потенциальной жертве, после чего начинает «выуживать» из нее деньги. Практическим примером такого мошенничества является дело, рассмотренное промышленным районным судом г. Самары, согласно материалам которого М. совершил мошенничество в сфере компьютерной информации, то есть хищение чужого имущества путем ввода компьютерной информации в функционирование

[1] Постановление Пленума Верховного Суда РФ от 30.11.2017 № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате» // Бюллетень Верховного Суда РФ. 2018. № 2; СПС «Консультант Плюс».

информационно- телекоммуникационных сетей, с причинением значительного ущерба гражданину.[1]

Место совершения интернет-мошенничества обладает своей спецификой, что обусловлено отсутствием у Интернета границ как таковых и его транснациональным характером. Ю.В. Гольчесвский указывает, что «установлению конкретного места совершения преступления в киберпространстве препятствует существующая коллизия между основополагающими принципами физики и международного права, которую можно выразить следующим тезисом: электроны могут перемещаться по сетям, свободно пересекая государственные границы, а национальная юрисдикция – нет»[2].

Д. Менте предлагал рассматривать правовой режим Интернета в контексте теории интернациональных пространств, на которые не распространяется национальный суверенитет[3]. Иначе говоря, ученый предлагает приравнять киберпространство к космосу, открытому морю и Антарктике. Данная точка зрения представляется не совсем корректной, так как киберпространство – это более сложная система, так как еще не существует какого-либо материального знака, на котором можно было бы отметить принадлежность какого-либо сегмента интернета конкретному государству.

М.М. Безкоровайный приравнивает киберпространство к территориям смешанного правового режима, как например исключительные экономические зоны, континентальный шельф и пр., однако на наш взгляд это также невозможно в силу транснациональности Интернета и отсутствия возможности каким-либо образом очертить его границы[4]. В.Ю. Батурин

---

[1] Приговор Промышленного районного суда г. Самары от 20.01.2017. URL: https://sud-praktika.ru // (дата обращения: 02.02.2019);

[2] Гольчевский Ю.В. К вопросу о кибербезопасности Интернет пользователей // Технические науки. 2018. № 6. С. 122.

[3] Менте Д. Юрисдикция киберпространства. теория интернациональных пространств. М.: Статут, 2012. С. 109.

[4] Безкоровайный М.М. Кибербезопасность: подходы к определению понятия // Вопросы кибербезопасности. 2014. № 11. С. 51.

предлагал сегментировать Интернет-пространство по доменам различных стран, приводя в качестве примера российский сегмент интернета (так называемый «рунет»), в рамках которого сайты имеют домены «.ru», «.рф» и «.su».[1] Однако тут же возникает противоречие: такие межнациональные домены «.edu», «.com» и пр., не принадлежат какому-либо конкретному государству, вследствие чего определение сегментирования Интернета по доменам представляется невозможным.

Наиболее рациональное решение проблемы предложил К. Корнилс, который предлагает определять место совершения инетрнет-мошенничества по месту нахождения виновного лица, конкретизирую следующие ситуации:[2]

1. Если виновное лицо совершает преступления, находясь на территории своей страны, то его действия подпадают под юрисдикцию этой страны с учетом местонахождения преступника. Например, если территориально виновное лицо находится в РФ, и преступное деяние совершается в отношении лица, находящегося на территории РФ, то на него будет распространятся юрисдикция российского государства.

2. Если преступник находится на территории одного государства, но для совершения преступления использует сервер другого государства и потерпевшим оказывается его гражданин, то преступление подпадает под юрисдикцию второго государства. Например, виновное лицо, находясь на территории Франции, совершил мошеннические действия в отношении гражданина РФ, используя для передачи данных, расположенный на территории РФ. Данный факт интернет-мошенничества будет подпадать под юрисдикцию российского уголовного права.

3. Если лицо является гражданином одной страны, находится на территории другой, но совершает акт мошенничества в отношении гражданина третей страны и с помощью сервера, находящегося на

---

[1] Батурин Ю.М. Проблемы компьютерного права. М.: Юридическая литература, 2013. С. 153.

[2] Корнилс К. Локализация места ответственности за преступления, связанные с интернетом. М.: Юрайт, 2013. С. 147.

территории этой третьей страны, то уголовная ответственность может наступать по законодательству любой из трех стран при наличии соответствующих международных соглашений. Например, преступник является гражданином РФ, находится на территории Франции, а преступление совершается путем передачи данных через сервер ФРГ и в отношении немецкого гражданина, то преступление фактически подпадает под юрисдикцию всех трех стран.

Сложности при определении места совершения интернет-мошенничества обусловлены и активным использованием VPN-сервисов не только преступниками, но и рядовыми пользователями. По своей сути, VPN - это технология, обеспечивающая зашифрованное интернет-соединение, а также позволяющая подменять реальный IP-адрес, что обеспечивает полную анонимность в сети[1]. Зачастую, отследить преступника, использующего подобного рода технологии практически невозможно.

Время совершения преступления может быть различным.

Что касается средств совершения преступлений, то в общей науке уголовного права под ними понимают предметы, устройства или механизмы, которые используют в процессе совершения преступления. В контексте исследования интернет-мошенничества они так же обладают определенной спецификой. Прежде всего, средства совершения преступления можно разделить на две категории: компьютерное оборудование и программное обеспечение.

К числу первых относятся различные технические системы и оборудование, которое является частью материального мира и используется для доступа к сети интернет. Это, например, различные виды компьютеров, телефонов с функцией выхода в интернет, сервера, WiFi-роутеры и пр. Ко второй категории относятся разнообразные программы, представляющие собой комбинации компьютерных инструкций и данных, позволяющие

[1] См.: Рябко Е.И. Калейдоскоп VPN-технологий // Телекоммуникации и транспорт. 2019. № 2. С. 3.

аппаратному обеспечению вычислительной системы выполнять вычисления или функции управления. Они не являются частью материального мира и не могут функционировать обособленно от технического устройства[1]. В качестве таковых следует признавать интернет-браузеры (Chrome, Internet Exployer, FireFox), программы управления электронными кошельками (WebMoney, Kiwi), программы, обеспечивающие анонимность в сети интернет (Hotspot Shield, Tor Browser, X-Proxy) и пр.

Зачастую сами программы и оборудование могут не представлять угрозы для пользователей, однако в умелых руках мошенника могут стать эффективным средством совершения преступления.

На основании вышеизложенного мы можем сделать вывод, что интернет-мошенничество – это специфическое преступление, которое одновременно и обладает признаками преступлений, предусмотренных ст. 159 и 159.6 УК РФ, и отличается от них, что дает основание ставить вопрос о его выделении в отдельный состав.

Объектом интернет-мошенничества является чужое имущество или право на него. Таким образом, данное преступление – это классическое преступление против собственности. Объективная сторона выражена действием в форме активного обмана или злоупотребления доверием. Спецификой обладает место совершения преступления, так как Интернет – это пространство, лишенное границ и не подпадающее под какую-либо конкретную юрисдикцию, в связи с чем возникают проблемы при определении законодательства, по которому лицо будет подлежать уголовной ответственности. Также особенными являются и средства совершения преступления, в качестве которых выступают техническое оборудование и программное обеспечение.

---

[1] См.: Михайленко И.А. К вопросу о способах мошенничества в сети интернет // Сибирские уголовно-процессуальные и криминалистические чтения. 2016. № 8. С. 20.

2.2. Субъективные признаки мошенничества в киберпространстве, отграничение от смежных составов

Субъективная сторона интернет-мошенничества представлена прямым умыслом. Иначе говоря, лицо осознает общественно-опасный характер совершаемых действий, предвидит наступление общественно-опасных последствий и желает их наступления. Цель совершения интернет-мошенничества – это незаконное получение чужого имущества (как правило, денежных средств) или же приобретения права на это имущество. Таким образом, сопутствующим признаком субъективной стороны является корыстная цель[1].

Принимая во внимание, что при совершении мошенничества преступник, действуя умышленно, преследует в качестве основной корыстную цель, стоит остановиться на том, что же побудило его совершить преступление, то есть на мотиве. В данном случае уместно привести мнение Ю.М. Антоняна: «...Мотив наиболее ярко характеризует человека, и личность такова, каковы ее мотивы»[2].

Выделяют следующие типы корыстных преступников по ведущим мотивам:

- корыстолюбивый;
- утверждающийся;
- дезадаптированный;
- семейный;
- игровой;
- алкогольно-наркотизированный

[1] См.: Балаев Р.С. Ценностный конфликт как фактор рисков и угроз экзистенциальной безопасности личности в информационном обществе // Юриспруденция и политология. 2019. № 1. С. 26.
[2] Антонян Ю.М. Криминология. М.: Юрайт, 2017. С. 213.

Исследование, проведенное О.Н. Головиновым позволяет выделить следующие типы кибермошенников:[1]

1. Корыстолюбивые — лица, которые совершают преступления для достижения своих личных алчных целей, похищенное они накапливают, имеют постоянное место работы, профессиональные знания, навыки и умения, опыт работы.

2. Утверждающиеся — лица, которые совершают преступления для самоутверждения. Следует обратить внимание, что самоутверждение их происходит не только в глазах других лиц, то есть соучастников преступления, но и в собственных, в силу того что для некоторых мошенничеств необходимо наличие не только особых знаний, умений, навыков, но и храбрости. Как показывает практика, именно данный тип киберпреступников является наиболее распространенным.

3. Семейные — лица, которые совершили преступление для обеспечения нужд своего окружения. Окружением в данном случае следует признавать не только близких родственников, но и иных лиц, состоящих с ними в родстве, свойстве (родственники супруга), а также лиц, жизнь, здоровье и благополучие которых преступникам дороги в силу сложившихся личных отношений.

Потребности, ради которых лицо совершает преступление, могут быть весьма разнообразными, от покупки продуктов питания до приобретения элитных вещей, недвижимости. Данный тип мошенника скромен, похищенное тратит не на себя, а на нужды других.

4. Игровые — лица, которые обладают низким нравственно-культурным уровнем, обусловленным их индивидуальной психологией. Таким мошенникам присущи игнорирование неприкосновенности чужого имущества, отрицательные антиобщественные черты характера (наглость, дерзость, зависть, эгоизм), а также негативные эмоциональные и волевые

[1] См.: Головинов О.Н. Киберпреступность в современной экономике: состояние и тенденции развития // Вопросы инновационной экономики. 2016. № 5. С. 23.

качества. Желание похитить чужое имущество возникает ради развлечения, шалости или игры.

5. Дезадаптированные — лица, для которых совершение мошенничеств стало основным или единственным источником дохода. К таким, как правило, относят ранее судимых лиц либо мошенников-профессионалов.

Алкогольно-наркотизированный тип встречается крайне редко, что объясняется, прежде всего, спецификой рассматриваемого преступления: кибермошенничество требует внимательности и сосредоточенности, а лицо, находящееся в состоянии наркотического или алкогольного опьянения, просто не в состоянии реализовать преступный умысел[1].

На наш взгляд, совершение рассматриваемого преступления с косвенным умыслом невозможно, так как само по себе процесс реализации преступного умысла в рассматриваемом случае достаточно трудоемкий и требует от виновного лица не только специфических знаний, но также и определенной подготовки (например, установка необходимого программного обеспечения) в целях достижения преступного результата.

Что касается субъекта преступления – это вменяемое, физическое лицо, достигшее возраста уголовной ответственности. Здесь следует сразу оговориться, что в уголовном законодательстве субъектом по ст.ст. , 159, 159.6 УК РФ является лицо, достигшее 16-летнего возраста, однако, реальность такова, что уже в 14-летнем возрасте лицо может обладать необходимым знаниями для совершения преступления[2]. Объясняется это тем, что Интернет – это среда, в которой поступающая информация не поддается контролю, и пользователь при наличии желания, может найти все, что угодно, в том числе и подробную инструкцию о том, как именно совершить

---

[1] Головинов О.Н. Киберпреступность в современной экономике: состояние и тенденции развития // Вопросы инновационной экономики. 2016. № 5. С. 22.

[2] См.: Кондратенко Е.Л. Обеспечение информационной безопасности как проблема отечественного школьного воспитания в условиях информационного общества // Проблемы современного образования. 2013. № 17. С. 46.

то или иное преступление[1]. Более того, поголовно наблюдается такое явление как акселератизм молодежи, что нельзя не принимать во внимание[2]. Таким образом, мы считаем целесообразным, что ответственность за интернет-мошенничество должна наступать с 14 лет. Например, последнее время наиболее часто мошенники совершают рассматриваемое преступление с помощью программы «Сбербанк Онлайн», в порядке пользования которым без особого труда могут разобраться и подростки до 14 лет. Показательным является приговор Ленинского районного суда г. Екатеринбурга, согласно которому Д. был осужден по ч. 3 ст. 159 УК РФ за совершение мошеннических действий в отношении Ш.[3]

Исследование, проведенное Д.И. Макушевым показало, что кибермошенничество чаще совершают мужчины[4]. Но при этом особое внимание стоит обратить на то, что женщины совершают мошенничества в два раза чаще, чем все остальные преступления в целом. Это связано со спецификой совершения противоправного деяния, сферой, в которой оно совершается, а также механизмом индивидуального преступного поведения. Не стоит забывать и о различных социальных ролях женщин и мужчин, отличительных чертах, связанных с их биологическими особенностями.

Исследование гендерной принадлежности личности мошенника показало, что она не является детерминантом данного явления, хотя в некоторых случаях и может сыграть значимую роль.

Возраст лиц, совершивших мошенничества, совпадает со среднестатистическими показателями по всем преступлениям в целом и относится к возрастной группе от 25 до 49 лет.

---

[1] См.: Заплатина Е.А. Интернет-мошенничество. Старые и новые угрозы // Гаудеамус. 2012. № 7. С. 34.

[2] См.: Никитина И.А. Финансовое мошенничество в сети Интернет // Вестник томского государственного университета. 2013. № 6. С. 38.

[3] Приговор Ленинского районного суда г. Екатеринбурга от 20.03.2017. URL: https://sud-praktika.ru// (дата обращения: 23.01.2019);

[4] См.: Макушев Д.И. Криминологическая характеристика личности киберпреступника // Актуальные проблемы гуманитарных и естественных наук. 2017. № 2. С. 18.

Из общей массы преступников мошенника всегда выделял уровень образования. Это также обусловлено спецификой совершаемого преступления, которое требует от субъекта преступления специализированных знаний в сфере компьютерных технологий и компьютерной информации, которая доступна для понимания далеко не каждому и требует от человека определенного уровня интеллектуального развития.

Как отмечает И.М. Рускаов, более половины лиц, совершивших мошенничества в сети Интернет, не имеют постоянного источника доходов[1]. Часть из трудоустроенных являются наемными работниками, служащими различных сфер, предпринимателями без образования юридического лица. Все эти характеристики отличают мошенника от среднестатистического преступника. Д.И. Макушев приводит следующие статистические данные: в России чаще совершают преступления лица без постоянного источника дохода, «обычные» преступники являются наемными работниками в 19% случаев, но только 3% из них относятся к категории «служащий»[2]. Получали образование разного уровня на момент совершения преступления 2% мошенников, что в два раза ниже показателя среди всех преступников.

Мошенникам свойственна тщательная подготовка своих действий, их обдуманность и всесторонняя проработанность. Мошенник при подготовке преступления думает не только о завладении, например, чужим имуществом, но и о мерах, необходимых для того, чтобы успешно реализовать свой преступный умысле и не оставить следов, по которым его можно было бы обнаружить.

На основании вышеизложенного можно сделать вывод, что субъективная сторона мошенничества в сети «Интернет» может быть выражена только прямым умыслом. В силу того, что совершение данного

---

[1] Русаков И.М. Криминалистическая характеристика личности преступника, совершившего мошенничество в сфере предоставления интернет-услуг // Государство и право. 2018. № 1. С. 93.

[2] См.: Макушев Д.И. Криминологическая характеристика личности киберпреступника // Актуальные проблемы гуманитарных и естественных наук. 2017. № 2. С. 19.

преступления требует от преступника серьезной подготовки и тщательного планирования, полагаем невозможным совершение данного преступного деяния по неосторожности. Мотив может быть как корыстный, так и нет.

Субъектом рассматриваемого преступления является вменяемое лицо, достигшее возраста 16 лет. Что касается характеристики самого преступника, то они могут делить на несколько типов: корыстолюбивый, утверждающийся, дезадаптированный, семейный, игровой, алкогольно-наркотизированный. Из всех перечисленных наиболее редко встречается алкогольно-наркотизированный тип кибермошенников, а чаще – утверждающийся или корыстолюбивый.

ГЛАВА 3. ПУТИ СОВЕРШЕНСТВОВАНИЯ УГОЛОВНОГО ЗАКОНОДАТЕЛЬСТВА ОБ ОТВЕТСТВЕННОСТИ ЗА МОШЕННИЧЕСТВО В КИБЕРПРОСТРАНСТВЕ

3.1. Способы мошенничества в киберпространстве и проблемы их квалификации

Киберпространство является средой, где активно возникают и развиваются различные способы мошенничества. Перечислим некоторые из них.

1. Интернет-магазины. Современный мир устроен так, что для того, чтобы найти необходимую вещь, человеку не обязательно отправляться в магазин, а достаточно открыть страницу в интернете. Ассортимент, который предлагают интернет-магазины весьма широк – от одежды и продуктов питания до технических устройств и их комплектующих. Мошенническая схема довольно проста – человек выбирает товар, «продавец» просит вас внести предоплату, после чего «пропадает» с полученными деньгами, таким образом, потерпевший остается и без денежных средств, и без товара. Нередко мошенники маскируют мошеннические сайты под сайты известных онлайн-магазинов. Например, ниже представлен официальный сайт онлайн-магазина одежда Lamoda:

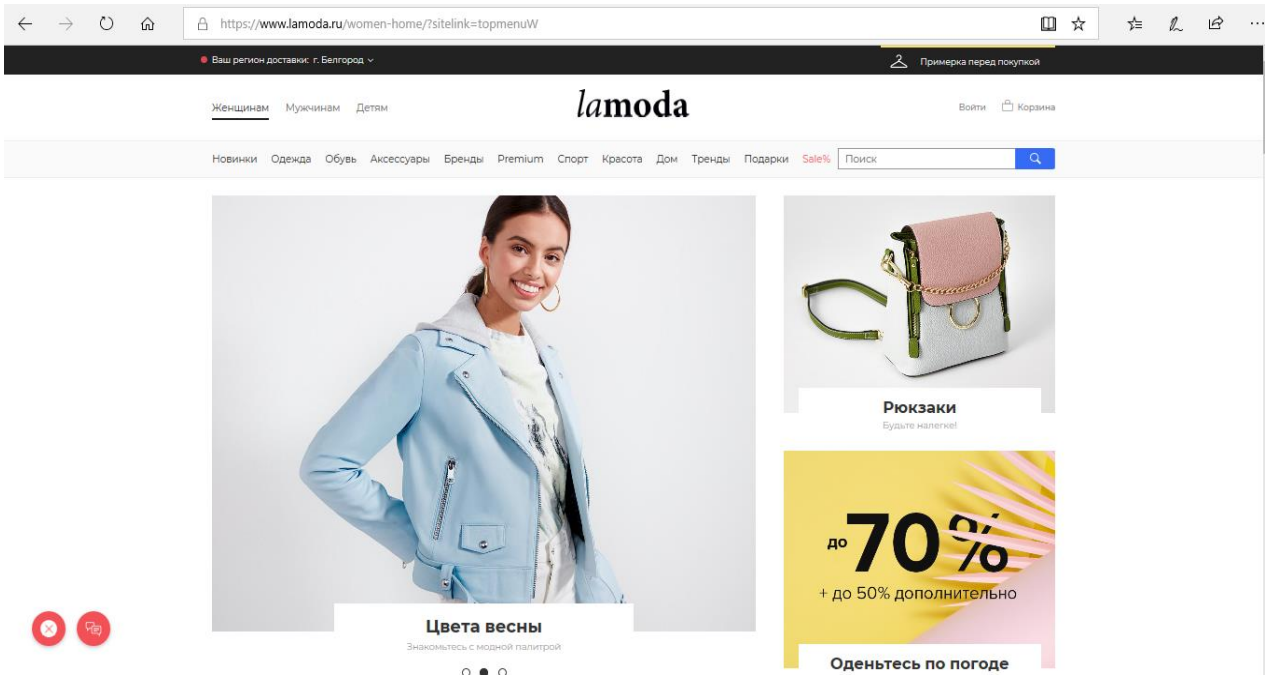


Рис. 2.1.

Мошеннический же сайт выглядит следующим образом:

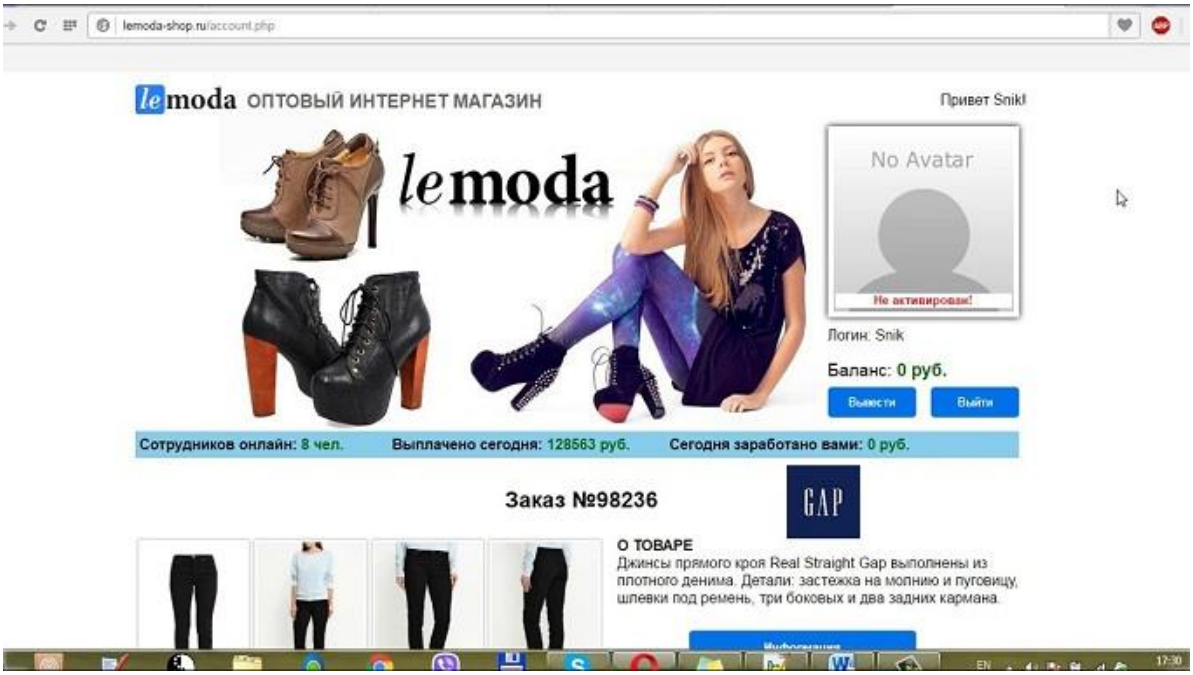


Рис. 2.2.

Обратите внимание, магазины схожи не только названиями и внешним дизайном, но и доменными именами, вследствие чего незнающему человеку достаточно легко войти в заблуждение. Нередко такие интернет-магазины называют сайтами-подделками. Очень часто в подобных магазинах цены на товары существенно ниже, чем у «настоящих» представителей, вследствие чего люди ведутся не только на внешний вид, но и на низкие цены, предполагая, что покупка будет более выгодной[1].

Отдельно в данном пункте следует отметить такой изощренный вид мошенничества как купля-продажа «аудионаркотиков», возникший в 2014 году. В целом, аудионаркотики – это общее название для звуковых файлов,

[1] См.: Алексеенко Е.А. Особенности совершения покупок и коммуникации в онлайновом пространстве // Теория и практика общественного развития. 2013. № 7. С. 16.

оказывающих действие на бинауральные ритмы человека, которые, как обещают «продавцы» помогают расслабиться и получить удовольствие[1]. Как правило, объявления об их продаже мошенники рассылают по электронной почте, однако в последнее время участились их рассылки через такие мессенджеры как Viber и WhatsApp. В данном объявлении содержится ссылка, по которой можно перейти на соответствующий «интернет-магазин», с каталогом предлагаемых товаров, однако прослушать запись возможно только после ее покупки. Как правило, вы оплачиваете покупку, деньги поступают мошеннику, но аудиозапись вам не направляют или же эффект оказывается совершенно не тем, на какой рассчитывал пользователь[2]. Что касается вопроса относительно того, является ли распространение аудионаркотиков уголовно-наказуемым деянием, то он выходит за рамки представленного исследования.

2. Попрошайничество. В данном случае речь идет о размещении преимущественно в социальных сетях просьб о помощи тяжело больным людям (особенно часто – детям), брошенным или травмированным животным, и основывается на знании мошенником человеческой психологии. Данные о таких лицах, мошенники могут брать как с официальных сайтов благотворительных фондов, так и придумывать самостоятельно. К посту прикладываются реквизиты банковского счета, на который сердобольные люди начинают переводить денежные средства, и к тому моменту, когда выясняется, что на самом деле никакого больного не существует, мошенник может получить на руки сотни тысяч рублей[3]. Очень часто для распространения информации используются рассылки писем (спам) на email-ы потенциальных жертв. Некоторые ученые, например А.К. Теохарова, склоняются к тому, что рассматриваемые действия в совокупности должны быть выделены в отдельный состав преступления – попрошайничество, а

---

[1] Что такое аудионаркотики? URL: http://megapoisk.com/ (дата обращения: 20.02.2019).

[2] См.: Осипенко А.Л. Организованная преступность в сети Интернет // Вестник Воронежского института МВД России. 2016. № 4. С. 43.

[3] Попрошайки в Интернете. URL: https://mnogomani.com/ (дата обращения: 06.03.2019)

лицо,виновное в этом подлежать ответственности не по административному, а по уголовному законодательству[1]. На наш взгляд, позиция достаточно спорная, так как мы считаем, что выделением попрошайничества в отдельный состав преступления нецелесообразно, а сами рассматриваемые действия полностью соответствуют признакам мошенничества.

3. Брачные аферы. Данный вид мошенничества в киберпространстве является одним из самых известных и распространенных, и одновременно одним из самых сложных для привлечения виновного лица к уголовной ответственности[2]. Потерпевшими, как правило, становятся молодые девушки, взрослые женщины и состоятельные мужчины. Наиболее часто брачные мошенники «работают» с иностранными гражданами или же гражданами, которые живут далеко и не имеют возможности встретиться с потенциальным женихом или невестой. Как правило, все начинается со знакомства в социальной сети или специальном сайте для знакомств, после чего мошенник начинает «обрабатывать» жертву, обещая женитьбу. состояние и пр. Когда он убеждается в том, что жертва уже готова, начинается второй этап – выманивание денег. Мошенник сообщает о резко возникших финансовых трудностях, и просит о помощи, после чего скрывается с полученными деньгами. Гораздо сложнее дело обстоит в тех ситуациях, когда жертва самостоятельно начинает дарить мошеннику дорогие подарки, делать денежные перевод и пр., так как доказать тот факт, что жертва была введена в заблуждение, практически невозможно[3].

4. Фишинг. Название данного вида мошенничества происходит от английского «Fishing», что означает «рыбалка», «выуживание». Под фишингом понимается один из видов интернет-мошенничества. заключающийся в получении доступа к конфиденциальным данным

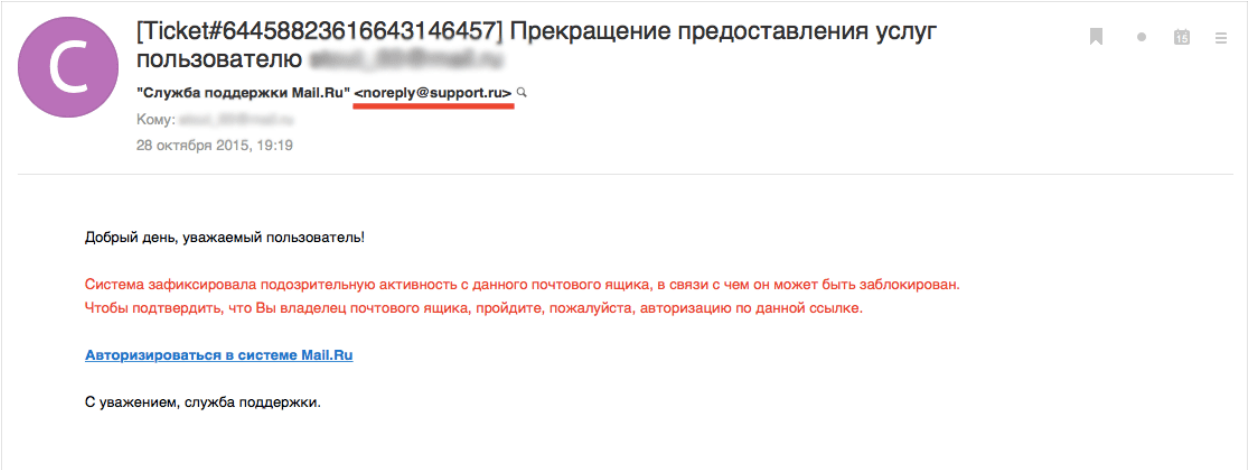
---

[1] Теохаров А.К. Понятие и признаки попрошайничества // Вестник омской юридической академии. 2017. № 14. С. 21.

[2] См.: Напханенко Е.О. Понятие и классификация угроз информационной безопасности в сети Интернет // Юристъ-Правоведъ. 2011. № 1. С. 49.

[3] См.: Сапарбаев Д.С. Совершение мошенничества с использованием средств массовой коммуникации // Вестник Московского университета МВД России. 2016. № 17. С. 94.

пользователей и содержимому их пластиковых карт[1]. Как правило, мошенники рассылают спам-письма по электронным ящикам потенциальных жертв, в которых содержатся ссылки для перехода на внешне легитимные сайты известных компаний (например, банков, интернет-провайдеров и пр.). Однако переходя по такой ссылке, пользователь по сути предоставляет



мошеннику возможность воспользоваться его личными данными и данными пластиковой карты или интернет-кошелька. Фишинговое письмо может выглядеть следующим образом:

Рис. 2.3.

Согласимся с И.С. Табаком, что фишинг представляет собой одну из разновидностей социальной инженерии, которая базируется на незнании пользователями основ сетевой безопасности[2]. В частности, сервисы не осуществляют рассылку писем с просьбами сообщить свои учетные данные, пароли и прочее. На сегодняшний день, производители основных интернет-браузеров с целью защиты пользователей, договорились об использовании одинаковых способов информирования пользователей о том, что они

[1] См.: Изотов Д.С. Виды мошенничества с банковскими картами // Вестник НГИЭИ. 2015. № 16. С. 38.
[2] Табак И.С. Мошенничество с банковскими картами // Современные инновации. 2018. № 5. С. 33.

открыли подозрительный сайт, который может оказаться мошенническим[1]. Огромный интерес для мошенников, использующих фишинг, являются социальные сети. Например, в 2006 году компьютерный червь разместил в зарубежной сети MySpace огромное количество ссылок на фишинговые сайты, которые были нацелены на кражу регистрационных данных, а в мае 2008 года подобный червь впервые появился в российской социальной сети ВКонтакте[2].

Обратим внимание, что на сегодняшний день фишинг может выходить далеко за пределы интернета, а поддельные веб-сайты становятся лишь одним из множества его направлений. Например, письма, якобы отправленные из банка, могут сообщать жертве о необходимости осуществления звонка по указанному в письме номеру для решения проблем, возникших с их банковским счетом. Данная разновидность фишинга получила название «вишинг». Когда жертва звонит по указанному номеру, то заслуживает инструкции автоответчика, указывающие на необходимость озвучивания номера своего счета, PIN-кода от пластиковой карты и иных данных, которые дают доступ преступнику к деньгам, находящимся на счете. Нередки случаи, когда вишеры сами осуществляют беседу с жертвой, представляясь представителями официальных организаций (наиболее часто – сотрудниками Сбербанка) и используя фальшивые номера[3].

В последнее время особенно популярным становится SMS-фишинг, который нередко именуется «свишингом» (от англ. SMiShing). Мошенники посредством смс-сообщений рассылают ссылки на фишинговые сайты, переходя на которые пользователь вводит свои личные данные, и преступник получает доступ к денежным средствам жертвы[4].

---

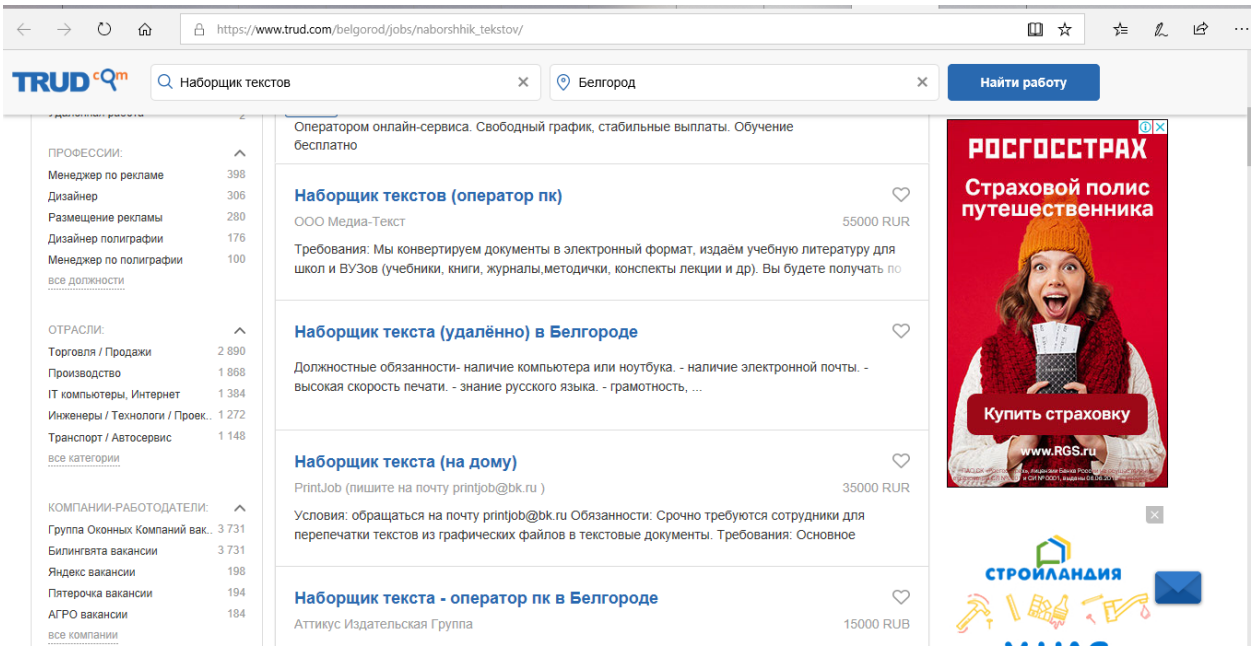
[1] См.: Хачатурова С.С. Киберпреступления в информационном обществе // Проблемы современной науки и образования. 2016. № 3. С. 67.

[2] Фишинговая атака на пользователей «ВКонтакте». URL: https://news.drweb.ru/ (дата обращения: 10.03.2019).

[3] Фишинг, вишинг, смишинг, фарминг – в чем разница? URL: https://www.protectimus.com/ (дата обращения: 10.03.2019).

[4] См. там же.

5. Удаленная работа, семинары и вебинары. Наиболее часто, люди, ищущие дополнительный заработок в интернете, встречают объявления



следующего содержания:

Рис. 2.4.

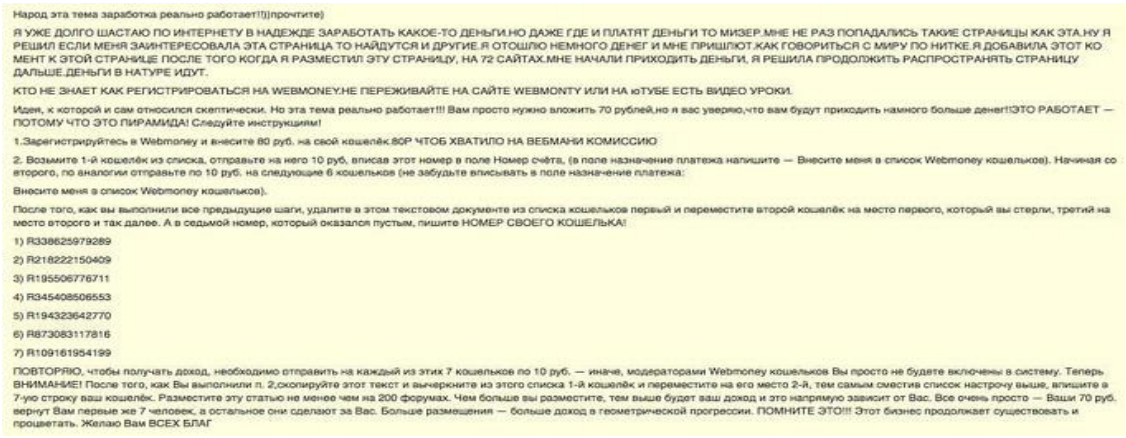
Вакансии могут быть и другого содержания: вышивание картин, администрирорвание сайтов и пр., но объединяет их одно – как только потенциальный работник откликается на вакансию, работодатель просит предоставить ему «задаток» - определенную денежную сумму, дабы он убедился, что работник настроен серьезно[1]. Естественно, после внесения предоплаты, работодатель исчезает и перестает выходить на связь.

Что касается семинаров и вебинаров, то потенциальная жертва в данном случае – люди, желающие саморазвиваться и обучиться чему-то новому. Как правило, пользователи покупают за определенные денежные суммы учебные пособия у мошенников, однако на деле оказывается. что они просто впустую потратили деньги, и доказать преступный мошеннический умысел в данном случае достаточно сложно. Как отмечает А.А. Гладкий,

[1] Работа на дому: выявляем мошенничество и обман в вакансиях. URL: https://privatline.ru/obman/ (дата обращения: 11.03.2019).

особо циничные мошенники обучают пользователей способам защиты от интренет-мошенников, а во время вебинара предлагают купить комплект учебной литературы или же заплатить за урок[1].

6. «Шесть кошельков». Данная разновидность мошенничества ориентирована на пользователей, которые хотят быстро заработать большие денежные суммы, не затрачивая для этого каких-либо усилий. Его суть заключается в следующем: человек получает электронное письмо с предложением отправить на каждый из шести кошельков по одному доллару, а затем по шаблону создать точно такое же послание и распространить его по сети, вписывая седьмым кошельком свой собственный[2]. Как правило, предыдущие шесть кошельков принадлежат одному человеку, соответственно, лица, распространяющие эти письмо «по цепочке» не столько обогащаются сами, сколько помогает обогатиться мошеннику, сами того не осознавая. Письмо может выглядеть следующим образом:



Народ эта тема заработка реально работает!!)прочтите)

Я УЖЕ ДОЛГО ШАСТАЮ ПО ИНТЕРНЕТУ В НАДЕЖДЕ ЗАРАБОТАТЬ КАКОЕ-ТО ДЕНЬГИ,НО ДАЖЕ ГДЕ И ПЛАТЯТ ДЕНЬГИ ТО МИЗЕР.МНЕ НЕ РАЗ ПОПАДАЛИСЬ ТАКИЕ СТРАНИЦЫ КАК ЭТА.НУ Я РЕШИЛ ЕСЛИ МЕНЯ ЗАИНТЕРЕСОВАЛА ЭТА СТРАНИЦА ТО НАЙДУТСЯ И ДРУГИЕ.Я ОТОШЛЮ НЕМНОГО ДЕНЕГ И МНЕ ПРИШЛЮТ.КАК ГОВОРИТЬСЯ С МИРУ ПО НИТКЕ.Я ДОБАВИЛА ЭТОТ КОМЕНТ К ЭТОЙ СТРАНИЦЕ ПОСЛЕ ТОГО КОГДА Я РАЗМЕСТИЛ ЭТУ СТРАНИЦУ, НА 72 САЙТАХ.МНЕ НАЧАЛИ ПРИХОДИТЬ ДЕНЬГИ, Я РЕШИЛА ПРОДОЛЖИТЬ РАСПРОСТРАНЯТЬ СТРАНИЦУ ДАЛЬШЕ.ДЕНЬГИ В НАТУРЕ ИДУТ.

КТО НЕ ЗНАЕТ КАК РЕГИСТРИРОВАТЬСЯ НА WEBMONEY.НЕ ПЕРЕЖИВАЙТЕ НА САЙТЕ WEBMONTY ИЛИ НА ютУБЕ ЕСТЬ ВИДЕО УРОКИ.

Идея, к которой и сам относился скептически. Но эта тема реально работает!!! Вам просто нужно вложить 70 рублей,но я вас уверяю,что вам будут приходить намного больше денег!!ЭТО РАБОТАЕТ — ПОТОМУ ЧТО ЭТО ПИРАМИДА! Следуйте инструкциям!

1.Зарегистрируйтесь в Webmoney и внесите 80 руб. на свой кошелёк.80Р ЧТОБ ХВАТИЛО НА ВЕБМАНИ КОМИССИЮ

2. Возьмите 1-й кошелёк из списка, отправьте на него 10 руб, вписав этот номер в поле Номер счёта, (в поле назначение платежа напишите — Внесите меня в список Webmoney кошельков). Начиная со второго, по аналогии отправьте по 10 руб. на следующие 6 кошельков (не забудьте вписывать в поле назначение платежа:

Внесите меня в список Webmoney кошельков).

После того, как вы выполнили все предыдущие шаги, удалите в этом текстовом документе из списка кошельков первый и переместите второй кошелёк на место первого, который вы стерли, третий на место второго и так далее. А в седьмой номер, который оказался пустым, пишите НОМЕР СВОЕГО КОШЕЛЬКА!

1) R338625979289

2) R218222150409

3) R195506776711

4) R345408506553

5) R194323642770

6) R873083117816

7) R109161954199

ПОВТОРЯЮ, чтобы получать доход, необходимо отправить на каждый из этих 7 кошельков по 10 руб, — иначе, модераторами Webmoney кошельков Вы просто не будете включены в систему. Теперь ВНИМАНИЕ! После того, как Вы выполнили п. 2,скопируйте этот текст и вычеркните из этого списка 1-й кошелёк и переместите на его место 2-й, тем самым сместив список настроч выше, впишите в 7-ую строку ваш кошелёк. Разместите эту статью не менее чем на 200 форумах. Чем больше вы разместите, тем выше будет ваш доход и это напрямую зависит от Вас. Все очень просто — Ваши 70 руб. вернут Вам первые же 7 человек, а остальное они сделают за Вас. Больше размещения — больше доход в геометрической прогрессии. ПОМНИТЕ ЭТО!!! Этот бизнес продолжает существовать и процветать. Желаю Вам ВСЕХ БЛАГ

Рис. 2.5.

Указанный перечень видов кибермошенничества далеко не исчерпывающий, и с каждым годом становится все разнообразнее. Во

[1] Гладкий А.А. Мошенничество в Интернете. Методы удаленного выманивания денег, и как не стать жертвой злоумышленников. М.: Феникс, 2012. С. 164.

[2] См.: Астишина Т.В. Проблемы расследования преступлений, связанных с мошенничеством в сети Интернет // Право и закон. 2018. № 9. С. 103.

многом это связано с активным развитием IT-сферы, а также большей интеграцией общества в виртуальное пространство. Учащаются случаи взлома аккаунтов в социальных сетях, электронных кошельков и пр., и далеко не всегда за очевидное на первый взгляд преступление виновное лицо возможно привлечь к ответственности. Кроме того, несмотря на существование ст. 159.6 УК РФ, некоторые разновидности мошенничества достаточно сложно квалифицировать. В частности это объясняется тем, что ст. 159.6 УК РФ «Мошенничество в сфере компьютерной информации» устанавливает уголовную ответственность за хищение чужого имущества или приобретение права на чужое имущество «**путем ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей»[1],** однако в случае мошенничества в киберпространстве никакого вмешательства в функционирование сети не происходит, так как и сам мошенник, и потерпевший являются равноправными пользователями компьютерной сети. Одновременно с этим, нельзя сказать, что рассматриваемые деяния должны квалифицироваться по ст. 159 УК РФ, как обыкновенное мошенничество, так как киберпространство – это специфическая сфера жизнедеятельности человека, осуществляя преступную деятельность в которой, преступник должен обладать специальными знаниями, и зачастую более тщательно готовиться к реализации преступного умысла, что, без сомнения, отягчает содеянное, и дает нам возможность обособить кибермошенничество от иных видов мошенничества[2].

На основании вышеизложенного сделаем вывод о том, что на сегодняшний день существует огромное количество самых разнообразных

---

[1] Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 27.12.2018) (с изм. и доп., вступ. в силу с 08.01.2019) // Российская газета. 1996. № 113; СПС «Консультант Плюс».

[2] См.: Абдеева З.Р. Проблемы безопасности электронной коммерции в сети Интернет // Проблемы современной экономики. 2013. № 4. С. 143.

видов мошенничества в сети Интернет. Объединяет их специфика места совершения преступления – киберпространство, что позволяет преступнику оставаться анонимным, и существенно усложняет процесс расследования и раскрытия преступлений. Кроме того, не последнюю роль в успешной реализации преступного умысла нередко играет низкий уровень компьютерной грамотности пользователей и их чрезмерная «наивность», особенно что касается способов быстрого заработка. Все это в совокупности обуславливает не только необходимость совершенствования уголовного законодательства в данной сфере, но также и повышения уровня компьютерной грамотности населения в целях профилактики и противодействия кибермошенничеству.

3.2. Предупреждение мошеннических действий в киберпространстве, вопросы совершенствования уголовного законодательства

В рамках данного вопроса необходимо говорить о двух основных аспектах проблемы: несовершенстве уголовного законодательства в сфере ответственности за кибермошенничество, а также о низком уровне компьютерной грамотности лиц, осуществляющих расследование данной категории преступных деяний[1].

Необходимость всестороннего улучшения мер, направленных на борьбу с кибермошенничеством, обусловлена рядом причин:

1. Анонимность пользователей. Именно данный фактор оказывается решающим при выборе преступником места совершения преступления, так как именно интернет гарантирует практически 100%-ую анонимность своих пользователей.

2. Низкая стоимость. Это обуславливает тот факт, что практически любое лицо может получить беспрепятственный доступ в Интернет не

[1] См.: Баландюк Р.О. Методика расследования отдельных видов преступлений, совершаемых в сфере интернет-технологий // Вестник Белгородского юридического института МВД России. 2015. № 1. С. 52.

прилагая к этому особых усилий, причем выход в него может быть осуществлен как с компьютера, так и с мобильного телефона, и не только через домашний роутер, но и общественную точку Wi-Fi, например, в торговом центре.

3. Оперативность действий. Действия, которые производятся в киберпространстве, характеризуются высокой скоростью распространения информации по всей сети, нередко являясь транснациональными.

4. Возможность охвата большой аудитории. Например, если жертвами фишинга могут стать одновременно сотни людей, а поддельных интернет-сайтов и того больше.[1]

В целях противодействия кибермошенничеству должны быть реализованы меры, как общего, так и частного характера. К числу первых, например, мы можем отнести разработку программ, программных продуктов, направленных на обеспечение безопасности использования Интернета, например, защищенных протоколов связи, криптографических методов защиты информации и пр. Особенно актуальными данные меры будут для тех, кто только начинает пользоваться благами Всемирной паутины и не знают всех тонкостей и подводных камней ее использования[2].

Что касается уголовного законодательства, то в процессе исследования мы уже не раз акцентировали внимание на том, что ни ст. 159 УК РФ, ни ст. 159.6 УК РФ, не являются в полной мере соответствующими требованиями современной правоприменительной техники. Так, ст. 159 УК РФ является чрезмерно обобщенной для квалификации по ней кибермошенничества, так как не учитывает специфику рассматриваемого вида преступления. Ст. 159.6 УК РФ – наоборот, чрезмерно узкой, так как при совершении мошенничества

[1] См.: Атаманов Р.С. Некоторые вопросы расследования мошенничества в сети Интернет // Актуальные проблемы российского права. 2018. № 2. С. 34.
[2] См. там же.

в сети Интернет не происходит вмешательства в функционирование сетей, как указывает диспозиция статьи[1].

Кроме того, в рамках данной статьи «утрачивается» такой признак мошенничества, как обман или злоупотребление доверием. Вновь обращаясь к статье, мы видим, что законодатель указывает, что мошенничество в сфере компьютерное информации – это *«это хищение чужого имущества или приобретение права на чужое имущество путем ввода, удаления…»*[2]. На наш взгляд прослеживается явное противоречие между самой сущностью мошенничества, под которым понимается хищение чужого имущества или права на него путем *обмана или злоупотребления* доверием, и диспозицией ст. 159.6 УК РФ.

Одновременно с этим, мы считаем нецелесообразным необходимость выделения кибермошенничества в отдельную статью УК РФ, как, например, предлагает Е.А. Блашникова[3]. Объясняем это тем, что законодатель опять же в ст. 159.6 УК РФ предпринял попытку охватить рассматриваемое преступление нормой уголовного кодекса, однако сделал это не достаточно эффективно. Введение еще одной схожей статьи может усложнить процесс правоприменения данных норм и привести к путанице диспозиций и санкций, что ввиду существования принципа экономии уголовного законодательства, недопустимо[4]. Таким образом, мы считаем необходимым модифицировать ст. 159.6 УК РФ и привести ее в соответствии с потребностями современной правовой науки.

Прежде всего, необходимо в текст диспозиции включить основной признак мошенничества способ обмана или злоупотребления доверием, что

---

[1] См.: Ревенков П.В. Кибербезопасность в условиях Интернета вещей и электронного банкинга // Национальные интересы: приоритеты и безопасность. 2016. № 5. С. 46.

[2] Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 27.12.2018) (с изм. и доп., вступ. в силу с 08.01.2019) // Российская газета. 1996. № 113; СПС «Консультант Плюс».

[3] См.: Блашникова Е.А. Новый этап в борьбе с мошенничеством в информационной среде // Наука, образование, культура. 2019. № 1. С. 27.

[4] См.: Бахтеев Д.В. О некоторых современных способах мошенничества в отношении имущества физических лиц // Российское право: образование, практика, наука. 2016. № 16. С. 33.

позволит исключить возможные правоприменительные ошибки. Таким образом, текст статьи будет выглядеть следующим образом: «мошенничество в сфере компьютерной информации, то есть хищение чужого имущества или приобретение права на чужое имущество *путем обмана или злоупотребления доверием посредством ввода*…».

Далее, считаем необходимым включить место совершения преступления – киберпространство – в диспозицию статьи наряду с вводом, удалением, блокированием, модификацией компьютерной информации, вследствие чего формулировка будет следующей: «…либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей, *а равно совершенное в сети Интернет*…». Данное включение, на наш взгляд, позволит расширить толкование данной статьи и упростить квалификацию кибермошенничества по соответствующей статье УК РФ.

Кроме того, мы считаем, что должна быть ужесточена санкция за совершение данного преступления. На сегодняшний день ч. 1 ст. 159.6 УК РФ не предусматривает такого наказания как лишение свободы, однако мы считаем, что в силу специфики данного вида преступления и необходимости его тщательной подготовки и приобретения специальных знаний, оно должно быть включено[1]. Так как последующие части статьи предусматривают максимальный срок лишения свободы до 10 лет, то считаем целесообразным включить срок до трех лет лишения свободы. Следовательно, санкция ч. 1 ст. 159.6 УК РФ должна выглядеть следующим образом: «…наказывается штрафом в размере до ста двадцати тысяч рублей или в размере заработной платы или иного дохода осужденного за период до одного года, либо обязательными работами на срок до трехсот шестидесяти часов, либо исправительными работами на срок до одного года, либо ограничением

[1] См.: Абышов Д.З. Некоторые особенности выявления и раскрытия бесконтактного мошенничества. 2018. № 27. С. 102.

свободы на срок до двух лет, либо принудительными работами на срок до двух лет, либо арестом на срок до четырех месяцев, *или лишением свободы на срок до трех лет*».

Отметим, что проблемой борьбы с кибермошенничством озадачены не только органы законодательной власти. Так, в октябре 2018 года Центральный банк РФ выступил с инициативой совершенствования нормативно-правового регулирования его деятельности в данной сфере. В частности, он предлагал законодательно закрепить его полномочия по блокировке сайтов в Интернете, которые распространяли информацию о деятельности организаций, осуществляющих мошенническую деятельность под видом предоставления финансовых услуг[1]. На сегодняшний день такими полномочиями обладает только Роскомнадзор.

Следующая проблема, на которую нам бы хотелось обратить внимание – это низкий уровень компьютерной грамотности лиц, осуществляющих расследование кибермошенничества. Обусловлено это тем, что для расследования данной категории преступлений необходимо обладать специальными знаниями в сфере IT-технологий, и, как правило, базовых знаний пользователя Интернета не достаточно[2]. Прежде всего, на базе высших учебных заведений необходимо вводить дополнительные обучающие курсы по вопросам информационной безопасности, квалификации и расследования преступлений в киберпространстве. Объясняем свою позицию тем, что впервые сталкиваясь с таким явлениями в практической жизни, люди зачастую не представляют даже общие принципы и способы совершения таких преступлений, а, соответственно, и расследование проходит с огромным трудом. Одним из вариантов решения проблемы мы видим организацию курсов повышения квалификации для действующих работников правоохранительных органов, процесс

---

[1] ЦБ может получить право внесудебной блокировки сайтов. URL: https://roskomsvoboda.org/ (дата обращения: 20.03.2019).

[2] См.: Теплова Д.О. Некоторые особенности мошенничества, совершаемого в сфере и с использованием высоких технологий. 2019. № 3. С. 48.

прохождения которых позволил бы им приобрести новые знания, применимые в практической деятельности.

Еще одним вариантом решения проблемы нам видится организация специальных подразделений, занимающихся расследованием киберпреступлений, в том числе – кибермошенничества. Обусловлено это тем, что иногда только поверхностных знаний бывает недостаточно, и для того, чтобы успешно раскрывать рассматриваемую нами категорию преступлений требуются не только специальные правовые знания, но и знания компьютерных технологий, сетей, компьютеров и пр. Обладать таковыми может только специалист, получивший образование по IT-направлению. В качестве примера такого подразделения можно привести Управление «К» МВД России, которое в пределах своей компетенции осуществляет выявление, предупреждение, пресечение и раскрытие преступлений в сфере компьютерной информации, преступлений, совершаемых с использованием информационно-телекоммуникационных сетей (включая сеть Интернет) и пр.[1] Таким образом, фактически назрела необходимость «объединения» двух диаметрально противоположных программ подготовки молодых специалистов: технической, связанной с компьютерными технологиями, и гуманитарной, юридической[2]. Возможно ли создание специальной программы обучения в учреждениях высшего образования? На наш взгляд да, однако, она требует тщательной разработки и подготовки, а также анализа реальной потребности рынка труда.

На основании вышеизложенного сделаем вывод, что противодействие кибермошенничеству должно осуществляться по нескольким направлениям: совершенствование уголовного законодательства и совершенствование механизма расследования данной категории преступлений.

На наш взгляд, ст. 159.6 УК РФ после внесения изменений должны выглядеть следующим образом:

---

[1] Управление «К» МВД России. URL: https://мвд.рф/ (дата обращения: 20.03.2019).

[2] См.: Соловьев В.С. Преступность в социальных сетях Интернета // Всероссийский криминологический журнал. 2018. № 9. С. 61.

УК РФ Статья 159.6. Мошенничество в сфере компьютерной информации

1. Мошенничество в сфере компьютерной информации, то есть хищение чужого имущества или приобретение права на чужое имущество путем обмана или злоупотребления доверием посредством ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей, а равно совершенное в сети Интернет -

наказывается штрафом в размере до ста двадцати тысяч рублей или в размере заработной платы или иного дохода осужденного за период до одного года, либо обязательными работами на срок до трехсот шестидесяти часов, либо исправительными работами на срок до одного года, либо ограничением свободы на срок до двух лет, либо принудительными работами на срок до двух лет, либо арестом на срок до четырех месяцев, или лишением свободы на срок до трех лет.

Помимо прочего мы считаем необходимым разработку и принятие специальной образовательной программы в высших учебных заведениях с целью подготовки специалистов одновременно в технической и правовой областях, а также повышение уровня профессиональных знаний уже действующих сотрудников путем повышения их квалификации. Кроме того, актуальным вопросом остается создание специальных подразделений в правоохранительных органах, осуществляющих расследование киберпреступлений, в том числе и кибермошенничества, что, безусловно, повысит эффективность правоохранительной деятельности в целом.

ЗАКЛЮЧЕНИЕ

На основании проведенного исследования представляется возможным сделать следующие выводы:

1. Уголовно-правовая норма о мошенничестве в российском законодательстве появилась достаточно поздно, лишь во второй половине XVI века. Лингвистический анализ термина «мошенничество» дает право предположить, что первоначально мошенничество подразумевало под собой карманную кражу. Основополагающий же признак рассматриваемого состава преступлений – обман или злоупотребление доверием – укрепился в уголовном законе лишь в XVIII веке. Таким образом, «мошенничество» с течением времени утратило свое лексическое значение употребляемого в качестве соответствующего термина существительного.

Помимо прочего, хотим отметить, что специфика современного законодательного описания мошенничества заключается в том, что в нем содержится указание два способа совершения преступления (обман и злоупотребление доверием) и два предмета посягательства (чужое имущество или право на чужое имущество).

2.На сегодняшний день от киберпреступлений в полной мере не защищена ни одна база данных, что обуславливает необходимость осуществления исследований в сфере компьютерных технологий и защиты информации в целях создания универсального средства защиты государственных и частных данных от несанкционированного к ним доступа. Все вышеперечисленное в совокупности одной из основных задач государства ставит проведение активной политики, направленной на совершенствование механизма расследования и раскрытия киберпреступлений.

Более того, киберпространство - это совершенно специфическое место совершения преступлений, которое существенно отличается от окружающей человека материальной действительности. В частности, киберпространство

не только обладаеттакой характеристикой как трансграничность, но и позволяет сохранять своим пользователям полную анонимность, что увеличивает уровень латентности кибермошенничества в разы. именно специфика киберпространства как места совершения преступлени обуславливает необходимость детального исследования рассматриваемого преступлениия.

3. Интернет-мошенничество – это специфическое преступление, которое одновременно и обладает признаками преступлений, предусмотренных ст. 159 и 159.6 УК РФ, и отличается от них, что дает основание ставить вопрос о его выделении в отдельный состав.

Объектом интернет-мошенничества является чужое имущество или право на него. Таким образом, данное преступление – это классическое преступление против собственности. Объективная сторона выражена действием в форме активного обмана или злоупотребления доверием. Спецификой обладает место совершения преступления, так как Интернет – это пространство, лишенное границ и не подпадающее под какую-либо конкретную юрисдикцию, в связи с чем возникают проблемы при определении законодательства, по которому лицо будет подлежать уголовной ответственности. Также особенными являются и средства совершения преступления, в качестве которых выступают техническое оборудование и программное обеспечение.

Субъективная стороны выражена прямым умыслом и корыстной целью, а субъектом является физическое, вменяемое лицо, достигшее 16 летнего возраста.

4. На сегодняшний день существует огромное количество самых разнообразных видов мошенничества в сети Интернет. Объединяет их специфика места совершения преступления – киберпространство, что позволяет преступнику оставаться анонимным, и существенно усложняет процесс расследования и раскрытия преступлений. Кроме того, не последнюю роль в успешной реализации преступного умысла нередко играет

низкий уровень компьютерной грамотности пользователей и их чрезмерная «наивность», особенно что касается способов быстрого заработка. Все это в совокупности обуславливает не только необходимость совершенствования уголовного законодательства в данной сфере, но также и повышения уровня компьютерной грамотности населения в целях профилактики и противодействия кибермошенничеству.

5. Противодействие кибермошенничеству должно осуществляться по нескольким направлениям: совершенствование уголовного законодательства и совершенствование механизма расследования данной категории преступлений.

На наш взгляд, ст. 159.6 УК РФ после внесения изменений должны выглядеть следующим образом:

УК РФ Статья 159.6. Мошенничество в сфере компьютерной информации

1. Мошенничество в сфере компьютерной информации, то есть хищение чужого имущества или приобретение права на чужое имущество путем обмана или злоупотребления доверием посредством ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей, а равно совершенное в сети Интернет -

наказывается штрафом в размере до ста двадцати тысяч рублей или в размере заработной платы или иного дохода осужденного за период до одного года, либо обязательными работами на срок до трехсот шестидесяти часов, либо исправительными работами на срок до одного года, либо ограничением свободы на срок до двух лет, либо принудительными работами на срок до двух лет, либо арестом на срок до четырех месяцев, или лишением свободы на срок до трех лет.

Помимо прочего мы считаем необходимым разработку и принятие специальной образовательной программы в высших учебных заведениях с

целью подготовки специалистов одновременно в технической и правовой областях, а также повышение уровня профессиональных знаний уже действующих сотрудников путем повышения их квалификации. Кроме того, актуальным вопросом остается создание специальных подразделений в правоохранительных органах, осуществляющих расследование киберпреступлений, в том числе и кибермошенничества, что, безусловно, повысит эффективность правоохранительной деятельности в целом.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

Нормативные правовые акты

1. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993) (с учетом поправок, внесенных Законами РФ о поправках к Конституции РФ от 30.12.2008 № 6-ФКЗ, от 30.12.2008 № 7-ФКЗ, от 05.02.2014 № 2-ФКЗ, от 21.07.2014 № 11-ФКЗ) // Собрание законодательства РФ. – 2014. – № 31; СПС «Консультант Плюс»;

2. Постановление ВЦИК от 01.06.1922 (ред. от 25.08.1924) «О введении в действие Уголовного Кодекса Р.С.Ф.С.Р.» (вместе с «Уголовным Кодексом Р.С.Ф.С.Р.») // СУ РСФСР. – 1922. –№ 15; СПС «Консультант Плюс»;

3. Постановление ВЦИК от 22.11.1926 (ред. от 27.04.1959) «О введении в действие Уголовного Кодекса Р.С.Ф.С.Р. редакции 1926 года» (вместе с «Уголовным Кодексом Р.С.Ф.С.Р.») // СУ РСФСР. –1926. –№ 80; СПС «Консультант Плюс»;

4. Уголовный кодекс Российской Федерации от 13 июня 1996 № 63-ФЗ (ред. от 27.12.2018) (с изм. и доп., вступ. в силу с 08.01.2019) // Российская газета. – 1996. –№ 113; СПС «Консультант плюс»;

5. Федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 18.03.2019) «Об информации, информационных технологиях и о защите информации» //Российская газета. – 2006. – № 165; СПС «Консультант Плюс»;

6. Указ Президента РФ от 31.12.2015 № 683 «О Стратегии национальной безопасности Российской Федерации» // Собрание законодательства РФ. –2016. –№ 1; СПС «Консультант Плюс»;

7. Постановление Пленума Верховного Суда РФ от 30.11.2017 № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате» // Бюллетень Верховного Суда РФ. –2018. –№ 2; СПС «Консультант Плюс»;

Судебная практика

8. Приговор Промышленного районного суда г. Самары от 20.01.2017. URL: https://sud-praktika.ru// (дата обращения: 02.02.2019);

9. Приговор Рудничного районного суда от 27.09.2017. URL: https://sud-praktika.ru// (дата обращения: 23.01.2019);

10. Приговор Ленинского районного суда г. Екатеринбурга от 20.03.2017. URL: https://sud-praktika.ru// (дата обращения: 23.01.2019);

Научная и учебная литература

11. Абдеева З.Р. Проблемы безопасности электронной коммерции в сети Интернет // Проблемы современной экономики. – 2013. – № 4. – С. 141 – 146;

12. Абышов Д.З. Некоторые особенности выявления и раскрытия бесконтактного мошенничества. – 2018. – № 27. – С. 101 – 105;

13. Алексеенко Е.А. Особенности совершения покупок и коммуникации в онлайновом пространстве // Теория и практика общественного развития. – 2013. – № 7. – С. 13 – 19;

14. Антонян Ю.М. Криминология. – М.: Юрайт, 2017. – 856 с.

15. Астахов К.В. Информационная безопасность как аспект стабильности экономических отношений на различных уровнях хозяйствования // Социально-экономические явления и процессы. – 2018. – № 3. – С. 25 – 31;

16. Астишина Т.В. Проблемы расследования преступлений, связанных с мошенничеством в сети Интернет // Право и закон. – 2018. – № 9. – С. 101 – 108;

17. Атаманов Р.С. Некоторые вопросы расследования мошенничества в сети Интернет // Актуальные проблемы российского права. – 2018. – № 2. – С. 33 – 38;

18. Афанасьева Д.В. Проблема DDOS-атак // Наука, образование, культура. – 2019. – № 1. – С. 49 – 57;

19. Балаев Р.С. Ценностный конфликт как фактор рисков и угроз экзистенциальной безопасности личности в информационном обществе // Юриспруденция и политология. – 2019. – № 1. – С. 24 – 28;

20. Баландюк Р.О. Методика расследования отдельных видов преступлений, совершаемых в сфере интернет-технологий // Вестник Белгородского юридического института МВД России. – 2015. – № 1. – С. 50 – 55;

21. Батурин Ю.М. Проблемы компьютерного права. – М.: Юридическая литература, 2013. – 425 с.;

22. Бахтеев Д.В. О некоторых современных способах мошенничества в отношении имущества физических лиц // Российское право: образование, практика, наука. – 2016. – № 16. – С. 31 – 34;

23. Безкоровайный М.М. Кибербезопасность: подходы к определению понятия // Вопросы кибербезопасности. – 2014. – № 11. – С. 48 – 53;

24. Бетти Э. Герменевтика как общая методология наук о духе. – М.: Перо, 2011. – 123 с.;

25. Блашникова Е.А. Новый этап в борьбе с мошенничеством в информационной среде // Наука, образование, культура. – 2019. – № 1. – С. 24 – 29;

26. Бондарь В.В. Киберпреступность – современное состояние и пути борьбы // Юридические записки. – 2013. – № 7. – С. 1 – 6;

27. Бородакий Ю.В. Инсайдерология: наука о нелигитимности в компьютерной инфосере // Технические науки. – 2017. – № 10. – С. 54 – 58;

28. Брагин А.П. Российское уголовное право. – М.: ЕАОИ, 2008. – 587 с.;

29. Веденеев В.С. Система выявления инсайдеров // Математические структуры и моделирование. – 2014. – № 7. – С. 31 – 39;

30. Владимирский-Буданов М.Ф. Обзор истории русского права. – М.: Астрель, 2005. – 367 с.;

31. Гибсон У. Нейромант. – М.: АСТ, 1997. – 441 с.;

32. Гладкий А.А. Мошенничество в Интернете. Методы удаленного выманивания денег, и как не стать жертвой злоумышленников. – М.: Феникс, 2012. – 846 с.;

33. Головинов О.Н. Киберпреступность в современной экономике: состояние и тенденции развития // Вопросы инновационной экономики. – 2016. – № 5. – С. 21 – 26.

34. Гольчевский Ю.В. К вопросу о кибербезопасности Интернет пользователей // Технические науки. – 2018. – № 6. – С. 120 – 126;

35. Евдокимов К.Н. Актуальные вопросы совершенствования уголовно-правовых средств борьбы с компьютерными преступлениями // Вестник Казанского юридического института МВД России. – 2016. – № 2. – С. 4 – 8;

36. Жиделев В.Г. Эволюция законодательства об уголовной ответственности за совершение преступлений в сфере высоких технологий // Экономика и право. – 2011. – № 10. – С. 10 – 16;

37. Заплатина Е.А. Интернет-мошенничество. Старые и новые угрозы // Гаудеамус. – 2012. – № 7. – С. 34 – 37;

38. Захаров В.М. Социально-философское определение собственности // Вестник Челябинского государственного университета. – 2011. – № 12. – С. 32 – 45;

39. Згадзай О.Э. Предупреждение кибепреступности. Проблемы и решения // Вестник Казанского юридического института МВД России. – 2011. – № 9. – С. 15 – 22;

40. Игнатов А.И. Уголовное право России. – М: Статут, 2013. – 406 с.;

41. Изотов Д.С. Виды мошенничества с банковскими картами // Вестник НГИЭИ. – 2015. – № 16. – С. 34 – 41;

42. Карпова Д.Н. Киберпреступность: глобальная проблема и ее решение // Власть. – 2014. – № 1. – С. 85 – 93;

43. Кондратенко Е.Л. Обеспечение информационной безопасности как проблема отечественного школьного воспитания в условиях информационного общества // Проблемы современного образования. – 2013. – № 17. – С. 45 – 51;

44. Корнилс К. Локализация места ответственности за преступления, связанные с интернетом. – М.: Юрайт, 2013. – 526 с.;

45. Листеренко Р.Р. Продвинутые атаки требуют новых видов защиты информации // Вопросы кибербезопасности. – 2013. – № 7. – С. 51 – 58;

46. Лопатин Д.В. Безопасность пользователей инфокоммуникационных технологий // Естественные и технические науки. – 2018. – № 8. – С. 41 – 53;

47. Макушев Д.И. Криминологическая характеристика личности киберпреступника // Актуальные проблемы гуманитарных и естественных наук. – 2017. – № 2. – С. 17 – 23.

48. Мамочка Е.А. Доказывание вины лица в инсайдерских преступлениях // Бизнес в законе. Экономико-юридический журнал. – 2015. – № 16. – С. 25 – 32;.

49. Маркова Т.И. Классификация инсайдеров // Компьютерные технологии. – 2010. – № 9. – С. 97 – 103;

50. Менте Д. Юрисдикция киберпространства. теория интернациональных пространств. – М.: Статут, 2012. – 288 с.;

51. Михайленко И.А. К вопросу о способах мошенничества в сети интернет // Сибирские уголовно-процессуальные и криминалистические чтения. – 2016. – № 8. – С. 19 – 25;

52. Напханенко Е.О. Понятие и классификация угроз информационной безопасности в сети Интернет // Юристъ-Правоведъ. – 2011. – № 1. – С. 47 – 54;.

53. Никитина И.А. Финансовое мошенничество в сети Интернет // Всетник томского государственного университета. – 2013. – № 6. – С. 37 – 44;

54. Номоконов В.А. Киберпреступность как новая криминальная угроза // Криминология: вчера, сегодня, завтра. – 2012. – № 24. – С. 111 – 118;

55. Овчинников С.А. Организационно-кадровый аспект безопасности: проблема инсайдерской угрозы электронному правительству // Вестник саратовского государственного социально-экономического университета. – 2012. – № 7. – С. 11 – 16;

56. Осипенко А.Л. Организованная преступность в сети Интернет // Вестник Воронежского института МВД России. – 2016. – № 4. – С. 40 – 43;

57. Покровский И.А. История Римского права. – М.: Юстицинформ, 2002. – 570 с.;

58. Ревенков П.В. Кибербезопасность в условиях Интернета вещей и электронного банкинга // Национальные интересы: приоритеты и безопасность. – 2016. – № 5. – С. 41 – 48;

59. Розенцвайг А.И. К вопросу о конструкции состава «Злоупотребление доверием» // Вестник Волжского университета им. В.Н. Татищева. – 2012. – № 2. – С. 194 – 203;

60. Русаков И.М. Криминалистическая характеристика личности преступника, совершившего мошенничество в сфере предоставления интернет-услуг // Государство и право. – 2018. – № 1. – С. 91 – 96.

61. Рябко Е.И. Калейдоскоп VPN-технологий // Телекоммуникации и транспорт. – 2019. – № 2. – С.1 – 6;

62. Сазонов М.М. Из истории понятия собственности // Проблемы современной науки и образования. – 2018. – № 4. – С. 19 – 20;

63. Сапарбаев Д.С. Совершение мошенничества с использованием средств массовой коммуникации // Вестник Московского университета МВД России. – 2016. – № 17. – С. 92 – 98;

64. Серегина О.Л. Понятие защиты права собственности в общей системе способов защиты прав // Legal Concept. – 2016. – № 8. – С. 21 – 26;

65. Сизиков М.И. История государства и права России с XVII до начала XIX века. – М.: ЮрЛит, 1998. – 291 с.;

66. Соловьев В.С. Преступность в социальных сетях Интернета // Всероссийский криминологический журнал. – 2018. – № 9. – С. 59 – 63;

67. Сычев В.М. Формализация модели внутреннего нарушителя информационной безопасности // Приборостроение. – 2015. – № 8. – С. 11 – 18;

68. Табак И.С. Мошенничество с банковскими картами // Современные инновации. – 2018. – № 5. – С. 31 – 39;

69. Теохаров А.К. Понятие и признаки попрошайничества // Вестник омской юридической академии. – 2017. – № 14. – С. 19 – 28;

70. Теплова Д.О. Некоторые особенности мошенничества, совершаемого в сфере и с использованием высоких технологий. – 2019. – № 3. – С. 47 – 54;

71. Тулегенов В.В. Киберпреступность как форма выражения криминального профессионализма // Вестник Южно-Уральского государственного университета. Серия Право. – 2018. – № 1. – С. 71 – 76;

72. Фадина Ю.П. Уголовно-правовая характеристика мошенничества в сети Интернет // Вестник Югорского государственного университета. – 2017. – № 11. – С. 101 – 111;

73. Февлов И.В. Происхождение и развитие российского и зарубежного законодательства о мошенничестве // Территория науки. – 2014. – № 2. – С. 12 – 17;

74. Фойницкий И.Я. Мошенничество по русскому уголовному праву. – С.-Пб.: Общественная польза, 1871. – 352 с.;

75. Хапов К.Г. Мошенничество как форма хищения чужого имущества в истории российского законодательства (основные тенденции развития уголовного регулирования) // Общество и право. – 2017. – № 9. – С. 1 – 16;

76. Хачатурова С.С. Киберпреступления в информационном обществе // Проблемы современной науки и образования. – 2016. – № 3. – С. 66 – 72;

77. Чекунов И.Г. Киберпреступность: понятие и классификация // Российский следователь. – 2012. – № 2. – С. 81 – 86;

78. Юрочкин Н.С. Кибермошенничество: характеристика, приемы и методы его совершения // Таврический научный обозреватель. – 2016. – № 17. – С. 43 – 49;

79. Янова В.В. К вопросу ретроспективного анализа понятия собственности // Terra Economicus. – 2010. – № 13. – С. 61 – 67;

Электронные ресурсы

80. Русская Правда в краткой редакции (с переводом). URL: www.hrono.ru (дата обращения: 07.01.2019);

81. Судебник 1550 года. URL: yakov.works/acts/16/2/pravo_02.htm (дата обращения: 09.01.2019);

82. Судебник Федора Иоанновича. URL: https://www.prlib.ru (дата обращения: 12.01.2019);

83. Соборное Уложение 1649 года. URL: www.hist.msu.ru (дата обращения: 12.01.2019);

84. Иванов Н.Г. Уголовное право: учебник для бакалавров // Biblioclub.ru: университетская бибилиотека online. М., 2018. URL:http://biblioclub.ru/ (дата обращения: 13.01.2019);

85. Именной указ от 3 апреля 1781 г., данный Сенату «О суде и наказаниях за воровство разных родов и о заведении рабочих домов во всех Губерниях». URL: https://base.garant.ru/58105240/ (дата обращения: 12.01.2019);

86. Сверчков В.В.Уголовное право. Особенная часть // Biblio-online.ru: электронно-библиотечная система «Юрайт». М., 2019. URL: https://www.biblio-online.ru/ (дата обращения: 12.01.2019);

87. Устав Благочиния или Полицейский 1782 г. URL: музейреформ.рф/ (дата обращения: 13.01.2019);

88. Уложение «О наказаниях уголовных и исправительных» 1845 года. URL: музейреформ.рф/ (дата обращения: 13.01.2019);

89. Ущерб от хакерских атак на банки в 2016 году. URL: http://www.tadviser.ru/ (дата обращения: 01.03.2018);

90. Group-IB представила отчет о киберпреступности и призвала рынок к хантингу. URL: https://www.group-ib.ru/ (дата обращения: 09.02.2019);

91. Червь Stuxnet. URL: http://www.tadviser.ru/ (дата обращения: 20.02.2019);

92. Что такое вирус Flame. URL: http://fb.ru/article/68993/ (дата обращения: 17.02.2019);

93. Самые громкие кибератаки 21 века. URL: https://geekbrains.ru/ (дата обращения: 17.03.2018);

94. Что случилось с Twitter, PayPal, Amazon и другими американскими сервисами. URL: https://www.kaspersky.ru/ (дата обращения: 22.02.2019);

95. В США хакеры отключили тормоза Jeep Cherokee через интернет. URL: http://www.kolesa.ru/ (дата обращения: 17.04.2017);

96. Топ-5 самых опасных целей кибератак мира 2016 года. URL: http://vsekommentarii.com/news/ (дата обращения: 18.04.2017);

97. Крупные атаки хакеров в 2001-2016 годах: хронология. URL: http://tass.ru/ (дата обращения: 19.04.2017);

98. Что такое аудионаркотики? URL: http://megapoisk.com/ (дата обращения: 20.02.2019);

99. Попрошайки в Интернете. URL: https://mnogomani.com/ (дата обращения: 06.03.2019);

100. Фишинговая атака на пользователей «ВКонтакте». URL: https://news.drweb.ru/ (дата обращения: 10.03.2019);

101. Фишинг, вишинг, смишинг, фарминг – в чем разница? URL: https://www.protectimus.com/ (дата обращения: 10.03.2019);

102. Работа на дому: выявляем мошенничество и обман в вакансиях. URL: https://privatline.ru/obman/ (дата обращения: 11.03.2019);

103. ЦБ может получить право внесудебной блокировки сайтов. URL: https://roskomsvoboda.org/ (дата обращения: 20.03.2019);

104. Управление «К» МВД России. URL: https://мвд.рф/ (дата обращения: 20.03.2019).