Изучение феномена Интернет-мошенничества в коммуникативном пространстве Рунета

Автор исследования:	*Научный консультант:*
Печалина Мария Константиновна	**Шилова Валентина Александровна**
	

Аннотация:

Дипломное исследование Марии Печалиной представляет собой детальный разбор типов мошенничества, совершаемого в сети Интернет, описание основных понятий и признаков нарушения законодательства в виртуальном коммуникативном пространстве, а также результаты опроса, посвященного специфике столкновения с Интернет-мошенничеством обычных пользователей, их отношение к этой проблеме.

Москва, 2011 г.

Оглавление

ВВЕДЕНИЕ

Проблема исследования

Современное общество характеризуется развитием информационных технологий и глобализацией информационных процессов. Одним из самых ярких примеров такого процесса является возникновение сети Интернет, стремительное и неуклонное расширение ее использования во всех сферах жизни общества.

Интернет предоставляет собой пространство широких коммуникативных возможностей. Например, техническими преимуществами виртуального общения являются возможность дешевой передачи больших объемов информации на любые расстояния, возможность коррекции и хранения передаваемой информации, возможность мгновенной обратной связи от другого пользователя и т.д. Благодаря своим преимуществам Интернет значительно облегчает координацию действий между людьми, поэтому часть коммуникации как делового, так и личного характера смещается из реального пространства в виртуальное. Сегодня коммуникативные возможности Интернета используются в бизнесе, политике, государственном управлении, науке. Многие аспекты реального мира становятся доступными в виртуальном. В Интернете человек может общаться, учиться, совершать покупки, работать, знакомиться и т.п.

Но также, вместе с этими возможностями из реального мира в виртуальный мир проникают и такие социальные явления, как мошенничество. Интернет-мошенничество распространяется по всем каланам общения в Сети: форумам, чатам, агентам мгновенного обмена сообщениями (ICQ, QIP, Miranda и т.д.), социальным сетям, электронной почте и т.д. Для проведения различных махинаций мошенники стремятся максимально использовать уникальные возможности Интернета, такие как мгновенная рассылка электронных сообщений большому количеству адресатов или размещение информации на веб-сайте, так, что она становится доступна всему миру [43].

Несмотря на то, что в Интернет представляет собой виртуальное пространство, в нем осуществляются реальные социальные процессы с реальными социальными последствиями. Например, Интернет-мошенничество имеет такие последствия, как финансовые потери, а также социально-психологические последствия, которые могут включать ощущение разочарования, стресс и т.д. За мошенничество в Интернете также накладывается юридическая ответственность.

Так как коммуникативные возможности Интернета постоянно расширяются, то Интернет представляет собой динамическое коммуникативное пространство, в котором интенсивно развиваются различные социальные процессы, одним из которых является мошенничество в самых разнообразных формах. Мошенничество как явление из реальной жизни обретает особые черты в виртуальном пространстве, поэтому необходим научный анализ его особенностей. В социологии Интернет-мошенничество является малоизученной областью, поэтому в нашей работе мы собираемся рассмотреть специфику мошенничества русского сегмента Интернета.

Актуальность исследования

В наше время коммуникативные технологии Интернета интенсивно развиваются. Широта покрытия зоны Интернет-доступа увеличивается, Интернет также становится доступен через мобильный телефон. В частности в пространстве Интернета идет развитие каналов коммуникации: растет их численность, доступность, простота использования. В связи с этим в Интернет перемещаются явления из реальной жизни, среди которых можно выделить мошенничество. Несмотря на виртуальность Интернет-пространства мошенничество несет за собой реальные социально-психологические последствия. Пользователи несут финансовые потери, терпят моральный ущерб. Таким образом, Интернет становится пространством для совершения уголовно-наказуемых действий, которые в силу его виртуальности сложно определить, а мошенников - привлечь к ответственности.

Из-за того, что феномен Интернет-мошенничество в наше время обретает широкое распространение, а главное сильные социальные последствия, для нас представляется актуальным изучение данного явления.

Степень разработанности проблемы

В социологии феномен Интернет-мошенничества является малоизученной областью. Как оказалось, практически не существует работ по исследованию особенностей мошенничества в Интернете и социальных последствий данного явления. Наиболее близкими к изучению Интернет-мошенничества являются *теории виртуализации* и *теории манипуляции*.

Среди авторов теорий виртуализации можно выделить *Д.В. Иванова* со своей работой «Виртуализация общества», в которой он выдвигает теорию общественных **изменений**, основанную на виртуализации общественной жизни [16]. В процессе виртуализации, по Иванову, глобальные общественные явления и процессы обретают свою форму в виртуальной реальности. Также необходимо отметить *В.И. Силаеву,* чьи научные интересы заключаются в изучении виртуальной реальности, виртуализации общества, Интернета [28;29;30]. В ее диссертации «Подмена реальности как социокультурный механизм виртуализации общества» дается а**нализ развития виртуализации общества в двух аспектах: рассмотрена электронная виртуализация (переход различных сфер деятельности на сетевой уровень) и неэлектронная виртуализация [30]. В работе выделяется типология виртуальной реальности, в которой определен основной круг социальных явлений, продуцирующих виртуальную реальность.**

Мошенничество можно рассматривать как действие, совершаемое при помощи средств манипуляций. Поэтому необходимо выделить теории манипуляций, в которых заключается психологическая составляющая мошеннического действия.

С.Г. Кара-Мурза - известный отечественный политолог и публицист. К его фундаментальным работам относится книга «Манипуляция сознанием», в которой рассказывается о формах и методах манипуляции сознанием [18].

Отечественный психолог–политолог *Е.Л. Доценко* рассматривает феномен манипуляции в психологическом ключе. Его работа «Психология манипуляции» посвящена рассмотрению особенностей манипуляции, происхождению данного феномена, механизмам и технологиям воздействия [11].

Не имея конкретных научных исследований феномена мошенничества, в Интернете, напротив, имеется большое количество ресурсов, статей и обсуждений данной проблемы. Приводятся конкретные примеры мошенничества, статьи, в которых обозреваются основные техники мошенничества, самые современные способы обмана пользователей, а также способы защиты от Интернет-мошенников.

Детальный визуальный анализ теоретической и информационной базы, касающейся феномена Интернет-мошенничества, типовых мошеннических практик в Рунете был проведен автором в курсовой работе 2010 года «Типология Интернет-мошенничества в Рунете». В той же работе была рассмотрена специфика мошенничества в Интернете, рассмотрены существующие виды и типологии Интернет-мошенничества, а также предложены собственные основания для типологии Интернет-мошенничества.

Описание единиц исследования

Объект исследования – теоретическая, правовая информация, информация в Интернете, связанная с мошенничеством и Интернет-мошенничеством, а также результаты эмпирического исследования, касающегося изучения данного феномена

Предмет исследования – уникальность и специфика мошенничества в Рунете как элемента коммуникативного пространства Рунета

Операционализация основных исследовательских категорий

Жертва Интернет-мошенничества – Интернет-пользователь, который попался на обман Интернет-мошенников [определение автора].

Интернет-мошенничество – это мошеннические махинации любого вида, совершаемых посредством виртуальных каналов коммуникации: социальных сетей, в чатах, на веб-сайтах, по электронной почте и др. с целью привлечения потенциальных жертв и проведения мошеннических актов [43].

Коммуникативное пространство Интернета – весь спектр социального взаимодействия в Интернете. В процессе изучения коммуникативного пространства Интернета анализируется: уровень коммуникативных каналов (по каким каналам осуществляется взаимодействие); качество, эффективность (успешность взаимодействия); формальные и неформальные характеристики [31].

Контентное пространство – информационное наполнение, весь спектр тем, идей, интенций, проблемных ситуаций, продуцируемых субъектами управления в коммуникативном пространстве [31].

Манипуляции — это вид психологического воздействия, искусное исполнение которого ведет к скрытому возбуждению у другого человека намерений, не совпадающих с его актуально существующими желаниями [11, с. 59].

Мошенничество – хищение чужого имущества или приобретение права на чужое

имущество путем обмана или злоупотребления доверием [25].

Рунет - русский сегмент Интернета [определение автора].

Цель и задачи

Цель: изучение Интернет-мошенничества в русском сегменте Интернета: систематизация видов, описание специфики, описание основных практик мошенничества, выяснение отношения пользователей Рунета к данному феномену.

Для достижения цели работы были поставлены следующие ***задачи исследования*:**

- анализ подходов к понятию Интернет-мошенничества;
- систематизация видов Интернет-мошенничества;
- описание особенностей Интернет мошенничества и его отличий от реального мошенничества;
- проведение анкетного Интернет-опроса пользователей Рунета.

На основании эмпирических данных, полученных в результате анкетного опроса Интернет-пользователей мы ставим задачи:

- описание типовых ситуаций мошенничества;
- выявление типологии пользователей, сталкивающихся с мошенничеством в Интернете;
- выяснение отношения Интернет-пользователей к феномену мошенничества;
- выявление социальной реакции на феномен мошенничества;
- оценка социальных последствий практики мошенничества в Интернете.

Теоретико-методологическая база

Опирается на теории виртуализации общества, а также на теории манипуляции, юридические и законодательные документы, касающиеся мошенничества и Интернет-мошенничества. Также использовался Интернет-контент, а именно ресурсы, посвященные описанию специфики и основных техник мошенничества в Интернете.

Эмпирическая база работы

- визуальный анализ сообщений мошенников в Интернете;
- визуальный анализ информационной базы, посвященной мошенничеству и Интернет-мошенничеству в Интернете;
- результаты пилотажного исследования Интернет-мошенничества;
- результаты основного исследования особенностей Интернет-мошенничества, проведенного посредством анкетного Интернет-опроса пользователей Рунета.

Ключевые понятия

Мошенничество, Интернет-мошенничество, Рунет, типология, жертва мошенничества.

Методы сбора и анализа данных:

- поиск информации в сети Интернет, теоретической и правовой литературе;
- визуальный анализ;
- анализ текстовых источников;
- анкетный Интернет-опрос через сервер «SurveyMonkey[1]»;
- анализ данных при помощи программы SPSS.

Ожидаемые результаты

В результате работы будет:

- проанализировано понятие Интернет-мошенничества;
- выделены виды и типы Интернет-мошенничества;
- выявлена специфика мошенничества в Интернете;
- выявлены категории пользователей в зависимости от различий в практиках столкновения с Интернет-мошенничеством;
- выявлены типовые ситуации мошенничества;
- выявлена типология отношения пользователей Рунета к феномену Интернет-мошенничества.

[1] «SurveyMonkey» - бесплатный сервер для организации онлайн-опросов. – Режим доступа: http://surveymonkey.com

ГЛАВА 1. ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ИЗУЧЕНИЯ ИНТЕРНЕТ-МОШЕННИЧЕСТВА

Для того чтобы изучить феномен Интернет-мошенничества, необходимо сначала определить, что он означает, а также обозначить те теоретические области, в которых данный термин задействован.

Определения мошенничества и Интернет-мошенничества в социологической литературе, к сожалению, найти не удалось. Существующее определение было создано в рамках виртуального пространства, где данное явление и появилось.

На одном из Интернет-ресурсов приводится следующее определение: «Термин «мошенничество в Интернете» применим в целом к мошенническим махинациям любого вида, где используются один или несколько элементов Интернета – такие как комнаты в чатах, электронная почта, доски объявлений или веб-сайты – для привлечения потенциальных жертв, проведения мошеннических сделок или для передачи поступлений от мошенничества в финансовые учреждения или иным лицам, участвующим в таких махинациях» [43].

В целом, определение данного термина по смыслу мало чем отличается от юридического определения мошенничества, которое подразумевает «хищение чужого имущества или приобретение права на чужое имущество путем обмана или злоупотребления доверием» [25].

Различие в определениях составляет то пространство, в котором мошенничество реализуется. И если в первом случае мы имеем дело с виртуальным пространством, в котором используются особые виртуальные коммуникативные каналы, то во втором случае мы имеем пространство реальной жизни и реальной коммуникации. В данной работе нам предстоит рассмотреть специфику виртуального мошенничества. Для лучшего понимания особенностей виртуального пространства, в котором сосредоточен изучаемый нами феномен, мы будем опираться на работы по *теории виртуализации.*

Мы выяснили, что мошенничество в реальной жизни или в Интернете предполагает завладение чужим имуществом или ресурсами при использовании определенных коммуникативных средств. В приведенных выше определениях мошенничества используются такие термины, как мошеннические махинации, обман, злоупотребление доверием. Отсюда мы можем сделать вывод, что мошенники для достижения своих целей используют определенные *средства манипуляции*.

Поэтому для изучения Интернет-мошенничества мы будем опираться: в рамках социологической теории на теории виртуализации, феномен и механизмы манипуляции, в рамках юриспруденции на статьи в *Уголовном Кодексе РФ*, касающиеся мошенничества.

§1.1 Теории виртуализации

О виртуализации общества и наступлении времени электронной цивилизации говорили многие исследователи, включая Э. Тоффлера, Д. Белла и др. [6; 35]. М. Кастельс особую роль придавал информационному ресурсу и сетевым структурам общества, распространение которых, по его взгляду, оказывает воздействие на

повседневную жизнь [19;20]. В нашей работе в рамках теории виртуализации более тщательно будут рассмотрены идеи и разработки российских авторов: Д.В. Иванова и В.И. Силаевой.

1.1.1 Теория виртуализации Д.В. Иванова

Д.В. Иванов является известным петербургским социологом, автором одной из наиболее полных исследований в отечественной литературе по виртуализации современного общества. В своей монографии «Виртуализация общества» Д.В. Иванов подчеркивает, что приоритетным в последние годы XX века стало развитие не информационных, а симуляционных технологий - технологий виртуальной реальности, поскольку достигается все большее сходство между работой на компьютере и управлением реальными объектами [22]. Автор выделяет три основных характеристики виртуальной реальности:

- нематериальность воздействия (изображаемое производит эффекты, характерные для вещественного);
- условность параметров (объекты искусственны и изменяемы);
- эфемерность (свобода входа/выхода обеспечивает возможность прерывания и возобновления существования).

Говорить о виртуальности общества можно тогда, когда оно может описываться с помощью характеристик виртуальной реальности. Автор дает определение виртуализации: «*Виртуализация - это любое замещение реальности ее симуляцией/образом - не обязательно с помощью компьютерной техники, но обязательно с применением логики виртуальной реальности»* [22, с.19].

Для разработки концепции виртуализации Д.В. Иванов предлагает постановку и решение следующих задач. Во-первых, для того чтобы иметь основание использовать дихотомию «реальное/виртуальное», необходимо проследить происхождение и развитие феномена социальной реальности. Его концепция виртуализации начинается с того, что автор анализирует возникновение социальной реальности и ее трансформацию в ходе модернизации общества. Во-вторых, чтобы построить модель общественных изменений как сдвига от «реального» к «виртуальному», автор рассматривает основные процессы, происходящие в различных институциональных сферах общества рубежа XX-XXI вв. В данных процессах виртуализация проявляется как образец общественных изменений. В-третьих, для определения теоретического статуса концепции виртуализации, Д.В. Иванов сопоставляет ее с используемыми в современном социальном знании моделями трансформации общества.

1.1.2 Исследование виртуальной реальности В.И. Силаевой

Сфера научных интересов современного отечественного социального исследователя В.И. Силаевой заключается в области изучения Интернета, виртуальной реальности, повседневного электронного дискурса и виртуализации общества. В своей работе «Об использовании понятия “виртуальный”» автор рассуждает о многообразии смыслов термина «виртуальность» [29]. В целом, сейчас в гуманитарных и социальных науках определение термина «виртуальный» связано с пониманием виртуального как

продукта компьютерных технологий. В.И. Силаева также выделяет три типа определений виртуальной реальности в гуманитарных и социальных науках:

1. определения, отождествляющие виртуальную реальность с реальностью данной;
2. определения, противопоставляющие виртуальную реальность реальности данной;
3. определения, не противопоставляющие, но и не отождествляющие виртуальную реальность с реальностью данной.

В своей диссертационной работе В.И. Силаева проводит типологизацию виртуальной реальности, а также рассматривает содержание и особенности процессов виртуализации человеческой деятельности [30]. В качестве критерия типологизации автор выбрала время появления продуцента той или иной формы виртуальной реальности. Соответственно этому критерию выделено три типа:

1) виртуальные реальности, продуценты которых возникли в древности, в доиндустриальную эпоху, к ним относятся такие продуценты как процесс творчества в искусстве, алкоголь и древние виды наркотиков, религиозный экстаз и т.д.;

2) виртуальные реальности, продуценты которых возникли в индустриальную эпоху, к ним относят такие продуценты как фотография, кинематограф и т.д.;

3) электронная виртуальная реальность (на данный момент единичный представитель единичный представитель третьего типа), продуцент которой возник в постиндустриальную эпоху.

В.И. Силаева отмечает характеристики электронной виртуальной реальности [30]:

- это реальность, онтологически обоснованная стремлением человека создавать альтернативный мир;
- она проявляется «тут, непосредственно» и преимущественно знаково, в отличие от виртуальной реальности искусства, религиозного экстаза и допинга;
- ее направленность гораздо шире по силе воздействия;
- она радикально меняет пространственно-временной континуум.

Также в работе В.И. Силаева анализирует виртуализации общества в различных общественных сферах.

Например, в экономике электронная виртуализация выражена появлением электронных денег и денежных отношений, что не изменяет сути экономических законов, но переводит экономику в электронный, более быстрый, интерактивный режим.

В сфере досуга выявлены основные виды сетевого общения, представляющие различные аспекты саморепрезентации. Среди социальных вызовов виртуализации В.И. Силаева отмечает отчуждение человека, уход в личностный виртуальный мир.

§1.2 Теоретические подходы изучения феномена манипуляции

1.2.1 Теория манипуляции Г. Шиллера

Изучением феномена манипуляции занималось много исследователей, среди которых можно назвать имена Г. Шиллера, Э. Шострома, Р. Гудина, и др.

Однако из зарубежных авторов хочется выделить Герберта Шиллера, известного американского учёного, автора работы «Манипуляторы сознанием» [39]. В своей

работе он обращается к феномену манипуляции, прежде всего, как политическому феномену. Область ее воздействия составляет не отдельная личность, а целые массы. Г. Шиллер пытается рассказать о появлении массового человека и необходимости манипуляций как метода управления им. Он определяет манипуляцию как *«скрытое принуждение, программирование мыслей, намерений, чувств, отношений, установок поведения»[39]*. К манипуляции, по мнению Г. Шиллера, относятся действия по формированию стереотипов, программирование мыслей, намерений, чувств, отношений, установок, поведения и т.п.

Объекты манипулятивной обработки, по мнению Г. Шиллера, превращаются в «марионеток», управляемых власть имущими с помощью «ниточек» — средств массовой информации.

По Г. Шиллеру, конечная «цель манипулирования массовым сознанием — пассивность масс, их инертность» [39, с. 47]. Действия манипуляторов направлены на то, чтобы снизить личностное начало масс, внушить мысль, что «за вас думают правители».

Фундамент всей иллюзорной картины мира, создаваемой манипуляторами, составляют мифы. По мнению Г. Шиллера, главными идеями, утверждающими господство правящей элиты, в США выступают пять социальных мифов:

1. Об индивидуальной свободе и личном выборе граждан. Как подчеркивает Г. Шиллер, существует достаточно оснований, чтобы утверждать, что суверенитет права личности не более чем миф, и что общество и личность неотделимы друг от друга.

2. О нейтралитете важнейших политических институтов: конгресса, суда, президентской власти, а также СМИ. Согласно этому мифу главная цель государственных институтов — служить всеобщему благу.

3. О неизменной эгоистичной природе человека, его агрессивности, склонности к накопительству и потреблению.

4. Об отсутствии в обществе социальных конфликтов, эксплуатации и угнетения.

5. О плюрализме СМИ, которые в действительности, несмотря на обилие источников, контролируются крупными рекламодателями и правительством и представляют собой единую индустрию иллюзорного сознания

Создание и поддержание этих мифов обеспечивает прочный «фундамент» для реализации манипулятивных технологий.

Среди российских исследователей феномена манипуляции нам хотелось бы выделить С. Г. Кара-Мурзу и Е.Л. Доценко.

1.2.2 Теория манипуляции С. Г. Кара-Мурзы

С.Г. Кара-Мурза является известным отечественным политологом и публицистом. К числу фундаментальных публицистических работ С.Г. Кара-Мурзы относится книга «Манипуляция сознанием» [18]. По мнению автора, человечество стоит на пороге создания такого типа общественного строя, где главным средством господства станет манипуляция сознанием. В работе рассказывается о формах и методах манипуляции сознанием. Под манипуляцией автор понимает *программирование мнений и*

устремлений отдельных лиц и масс, их настроений и даже психического состояния с целью обеспечить такое их поведение, которое нужно тем, кто владеет средствами манипуляции [18]. Манипуляция - это угнетение личности, при этом, поскольку человек желает верить в то, что хочет приобрести (знания, опыт, материальные блага), угнетение может достигаться через «ложь, в которую хотят верить» [18].

С.Г. Кара-Мурза выделяет роль особой манипулятивной семантики и риторики, которые являются одним из инструментов манипуляции сознанием. Общественные институты, массовая культура и средства массовой информации влияют на формирование этой семантики и риторики.

Признаками скрытой манипуляции, по автору, могут быть: язык, эмоции, сенсационность и срочность, повторение, дробление, изъятие из контекста, тоталитаризм источника сообщений, тоталитаризм решения, смешение информации и мнения, прикрытие авторитетом, активизация стереотипов, высказываний и т. д.

Другие примеры манипулятивных техник воздействия включают: сознание советского человека, «мягкие» чёрные мифы о советском строе, а также метафоры и стереотипы перестройки и государственного переворота августа 1991 года.

1.2.3 Социально-психологическая теория манипуляции Е.Л. Доценко

Рассмотрев феномен манипуляции как механизма политического воздействия, обратимся к ее изучению в психологическом ключе. Для этого мы проанализируем работу отечественного психолога–политолога Е.Л. Доценко «Психология манипуляции», в которой автор рассматривает особенности феномена манипуляции, его истоки происхождения, механизмы и технологии воздействия [11].

В частности автор обращается к этимологии данного слова. Слово «Manipulus» — латинский прародитель термина «манипуляция» — имеет два значения:

а) пригоршня, горсть (manus — рука + pie — наполнять), б) маленькая группа, кучка, горсточка (manus + pi — слабая форма корня) [11, с. 44].

В самом общем значении в Оксфордском словаре английского языка манипуляция (manipulation) определена как обращение с объектами со специальным намерением, особенной целью, как ручное управление, как движения, производимые руками, ручные действия.

В переносном значении Оксфордский словарь определяет манипуляцию как «акт влияния на людей или управления ими или вещами с ловкостью, особенно с пренебрежительным подтекстом, как скрытое управление или обработка» [11].

Таким образом, понятие манипуляции трансформируется в связи со сменой объектов ее применения: если раньше объектами манипуляции выступали предметы, то теперь ими являются люди. И ее ключевой особенностью является *стремление манипулятора скрыть свои намерения для достижения конкретных целей*.

Манипулятивные действия выполняются уже не руками, а с помощью иных средств.

Е.Л. Доценко находит сходство между психологическими эффектами в

межличностной манипуляции и действиями фокусника или иллюзиониста. Основные психологические эффекты создаются на основе управления вниманием (отвлечение, перемещение, сосредоточение), широкого использования механизмов психологической установки, стереотипных представлений и иллюзий восприятия.

Для выделения собственного определения манипуляции, Е.Л. Доценко опирается на представления различных авторов о понятии манипуляции (Таблица 1.2.1) [11, с. 51].

Таблица 1.2.1

Представления различных авторов о понятии манипуляции (с разбивкой определений на критерии)

№	Авторы	Определения
1.	Бессонов Б.Н.	Форма духовного воздействия, скрытого господства, осуществляемая насильственным путем
2.	Волкогонов Д.	Господство над духовным состоянием, управление изменением внутреннего мира
3.	Гудин Р.	Скрытое применение власти (силы) вразрез с предполагаемой волей другого
4.	Йокояма О.Т.	Обманное косвенное воздействие в интересах манипулятора
5.	Прото Л.	Скрытое влияние на совершение выбора
6.	Рикер У.	Такое структурирование мира, которое позволяет выигрывать
7.	Рудинов Дж.	Побуждение поведения посредством обмана или игрой на предполагаемых слабостях другого
8.	Сагатовский В.	Отношение к другому как к средству, объекту, орудию
9.	Шиллер Г.	Скрытое принуждение, программирование мыслей, намерений, чувств, отношений, установок, поведения
10.	Шостром Э.	Управление и контроль, эксплуатация другого, использование в качестве объектов, вещей
11.	Робинсон П.У.	Мастерское управление или использование

Данная систематизация определений манипуляции позволяет Е.Л. Доценко обозначить основные признаки манипуляции. В результате он выявил, что основными признаками манипуляции являются:

- родовой признак. Манипуляция - это вид духовного, психологического воздействия на человека, группу или общество;
- отношение манипулятора к другому как средству достижения собственных целей;
- стремление получить односторонний выигрыш;
- скрытый характер воздействия (как факта воздействия, так и его направленность);
- использование (психологической) силы, игра на слабостях.

А также два несколько обособленных критерия:

- побуждение, мотивационное привнесение;
- мастерство и сноровка в осуществлении манипулятивных действий.

С учетом всех признаков, Е.Л. Доценко вводит рабочее определение манипуляции:

«Манипуляция — это вид психологического воздействия, искусное исполнение которого ведет к скрытому возбуждению у другого человека намерений, не совпадающих с его актуально существующими желаниями» [11, с. 59].

В практических целях, как отмечает Е.Л. Доценко, удобнее пользоваться непосредственно метафорой: «*манипуляция — это действия, направленные на «прибирание к рукам» другого человека, помыкание им, производимые настолько искусно, что у того создается впечатление, будто он самостоятельно управляет своим поведением» [11, с.60].*

Соответственно, касательно нашей темы – мошенничество – это такой вид манипуляции, при котором целью манипулятора становится имущество или право на имущество другого человека. «Прибирание к рукам» этого имущества осуществляется путем искусного воздействия, при котором у человека возникает впечатление, что он поступает правильно, отдавая свое имущество манипулятору.

Что касается психологического воздействия, то в случае манипуляции в расчет берется одностороннее влияние манипулятора на его адресата, для достижения своих целей. «Результатом воздействия выступают некоторые изменения в психических характеристиках или состоянии адресата воздействия» [11, с. 61]

Необходимо теперь рассмотреть **технологии манипуляции**, о которых пишет Е.Л. Доценко. Он выделяет основные составляющие манипулятивного воздействия:

1) оперирование информацией, 2) сокрытие манипулятивного воздействия, 3) степень и средства принуждения, применения силы, 4) мишени воздействия и 5) тема роботообразности, машиноподобия адресата воздействия.

Кратко разберем каждую из них.

Под ***целенаправленным преобразованием информации*** Е.Л. Доценко подразумевает разнообразие производимых над информацией операций следующих видов:

- *Искажение* информации, которое варьируется от лжи до частичных деформаций;
- *Утаивание* информации;
- *Способ подачи* информации, который влияет на необходимое для отправителя восприятие адресатом содержания информации. Выделяется прием особой компоновки тем, который наводит получателя информации на вполне однозначные выводы.
- *Момент подачи* информации. Самый известный прием в телевидении— показ в наиболее (наименее) удобное для телезрителей время.

Под ***сокрытием воздействия*** имеется в виду тайный характер манипулятивного воздействия, который включает: 1) сокрытие факта манипулятивного воздействия; 2)сокрытие намерений манипулятора. Это необходимо, чтобы замаскировать цели манипуляции.

Автор также говорит о ***средствах принуждения*,** которыми на общественном уровне могут быть: сила властных политических структур или средства массовой информации.

Е.Л. Доценко вводит понятие ***мишени манипулятивного воздействия*,** под которым понимаются психические структуры, на которые оказывается влияние со стороны инициатора воздействия. Для манипуляторов, чем шире аудитория для

воздействия, тем более универсальными должны быть используемые мишени. Необходимо знание специфических качеств аудитории, чтобы манипулятор мог лучше под нее подстроиться.

Лейтмотив ***роботоподобности***, как пишет Е.Л. Доценко, опираясь на работы Г.Шиллера, состоит в идее, что «люди — объекты манипулятивной обработки превращаются в марионеток, управляемых манипуляторами с помощью средств массовой информации» [11, с.116].

Автор отмечает, что для совершения успешной манипуляции манипулятору необходимо, во-первых, подготовить ситуацию манипуляции и, во-вторых, подготовить адресата манипуляции.

Для ***подготовки ситуации манипуляции*,** необходимо проконтролировать физическое окружение, определяющие обстановку («декорации») общения и учесть социокультурные условия (язык, традиции, культурные нормы общения, социальная группа, социально-ролевые нормы).

Подготовка адресата осуществляется путем повышения вероятности возникновения у него определенных реакций, необходимых манипулятору.

Для этого необходим правильный выбор мишеней воздействия, воспользовавшись которыми манипулятор получает запланированный результат.

Е.Л. Доценко выделяет следующие виды:

1. *Изготовление побудителей активности:* потребностей, интересов, склонностей, идеалов — побудить, спровоцировать, направить.
2. *Формирование регуляторов активности:* установок, групповых норм, самооценки — убедить, настроить, внушить и т. п.
3. *Создание необходимых когнитивных структур:* мировоззрения, убеждений, верований, знаний — обучить, убедить, известить, проинформировать.
4. *Формирование требующегося операционального состава деятельности:* способа мышления, стиля поведения, привычки, умения — обучить, выдрессировать, отработать.
5. *Приведение в определенное психическое состояние:* усталость, нетерпеливость, некритичность, сосредоточенность, растерянность, нерешительность, эйфория и др.

В качестве технологии манипуляции автор также выделяет ***информационно-силовое обеспечение***, под которым он имеет в виду психологическое давление и информационное оформление.

Е.Л. Доценко в своей работе выделяет **механизмы**, **реализующие манипулятивное воздействие**. Автор считает, что в их основе лежат ***механизмы психологического воздействия***. Перечислим, на наш взгляд, самые важные из них.

Во-первых, это *удержание контакта***,** т.е. использование тех внутриличностных механизмов, которые обеспечивают надежность и стойкость «присоединения» к адресату.

Во-вторых, это те приемы воздействия в общении, которые характеризуются программирующим влиянием на поведение человека, и определяют высокую предсказуемость его поведения, т.е. *психические автоматизмы*. Психические автоматизмы выступают в роли рычагов, благодаря которым энергия желания (воздействия) манипулятора превращается в действия адресата. Возможным является

их намеренное изготовление, формирование, выработка и привитие.

В-третьих, важным механизмом воздействия также является *мотивационное обеспечение жертвы.* Любое манипулятивное воздействие в числе мишеней имеет мотивирующие элементы. Мотивационными предпочтениями человека можно управлять, если подавать соответствующие этому мотиву раздражители.

Итак, мы рассмотрели теоретические работы, посвященные изучению феномена манипуляции. Мы выяснили, как манипуляция определяется у различных авторов, какие механизмы и технологии присущи для данного явления.

Теперь нам необходимо обратиться к юридической теории, чтобы подробно изучить характеристики, присущие мошенничеству.

§1.3 Юридическое определение понятия мошенничества

Мошенничество включено в уголовный кодекс Российской федерации. Люди, совершающие мошенничество, несут уголовную ответственность. Приведем юридическое определение термина «мошенничество», обратившись к статье 159 уголовного кодекса РФ [25].

Статья 159 Уголовного кодекса РФ. Мошенничество

«Мошенничество, *то есть хищение чужого имущества или приобретение права на чужое имущество путем обмана или злоупотребления доверием*, 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 ста восьмидесяти часов, либо исправительными работами на срок от шести месяцев до одного года, либо арестом на срок от двух до четырех месяцев, либо лишением свободы на срок до двух лет» [25].

Также в статье отмечаются следующие виды мошенничества:

- Мошенничество, совершенное группой лиц по предварительному сговору, а равно с причинением значительного ущерба гражданину;
- Мошенничество, совершенное лицом с использованием своего служебного положения, а равно в крупном размере;
- Мошенничество, совершенное организованной группой либо в особо крупном размере.

Степень ответственности за совершение акта мошенничества различается и достигает (как в последнем виде) лишением свободы сроком до 10 лет и штрафом в размере до одного миллиона рублей.

Однако нам необходимо более тщательное выяснение особенностей мошенничества. Какие характеристики присущи мошенничеству? Какие действия мы назовем мошенничеством? Данные пояснения даны в комментариях к статье 159.

Комментарии к статье 159

Мы обратимся к некоторым комментариям статьи 159, выделяя наиболее важные, на наш взгляд, характеристики, присущие мошенничеству [25].

№ 1. Мошенничество является формой хищения, ему присущи все признаки этого понятия.

Поэтому еще одной статьей, которая может использоваться для определения действий Интернет-мошенников, является статья 158 УК РФ. Она устанавливает наказание за кражу, то есть за «тайное хищение чужого имущества». Ключевым здесь является слово «имущество». Если в результате действий Интернет-мошенника в его распоряжение перешло какое-то реальное имущество потерпевшего, то это уже считается кражей.

Важно выяснить специфические особенности мошеннических посягательств.

№ 2. Предметом мошенничества может быть не только имущество, но и право на него, отдельные правомочия по имуществу (например, виновный может завладеть правом пользования жильем).

№ 3. При мошенничестве способом завладения чужим имуществом является *обман* или *злоупотребление доверием*. При совершении данного преступления потерпевший *сам* передает имущество преступнику, полагая, что последний имеет право получить его.

№ 4. Обман при мошенничестве может выразиться в ложном утверждении о том, что заведомо не соответствует действительности, либо в умышленном умолчании о фактах, сообщение которых было обязательно.

№ 12. При мошенничестве средством хищения чужого имущества может быть *злоупотребление доверием*. Это возможно, когда виновный использует определенные гражданско-правовые (договорные) отношения, основанные на доверии сторон (например, договор бытового проката, торговый кредит), при получении от граждан денег под условием выполнения обязательств, впоследствии не выполненных.

Злоупотребление доверием тесно примыкает к обману. Виновный использует *особые доверительные отношения* между ним и собственником или иным законным владельцем, *чтобы обман был более убедительным*, либо прибегает к обману для того, чтобы заручиться доверием потерпевшего.

№ 13. При любой форме обмана и злоупотребления доверием сущность их заключается в том, что виновный путем уверений или умолчаний создает у потерпевшего неверное представление о каких-либо обстоятельствах и приводит его к убеждению об обязанности либо выгодности для него передачи имущества или имущественных прав. Иными словами, при мошенничестве переход имущества в пользу виновного осуществляется по волеизъявлению самого потерпевшего.

№ 15. Субъективная сторона предполагает *прямой умысел*. Виновный осознает, что вводит в заблуждение потерпевшего либо заведомо использует его доверие для получения чужого имущества и завладения им, и желает этого. Признаком субъективной стороны (как и любого хищения) является и корыстная цель.

Таким образом, мы выяснили, какое юридическое определение и характеристики присущи мошенничеству, и какая ответственность за совершение данных действий налагается. Из комментариев к статье 159 можно сделать следующий вывод: мошенничество есть завладение чужим имуществом путем обмана или установления доверительных отношений между мошенником и его жертвой, в результате чего жертва сама отдает мошеннику свое имущество. Очевидно, что мошенники используют различные средства манипуляции, чтобы данные доверительные отношения были

установлены. Жертвы верят мошенникам. Мошенничество можно назвать формой воровства, при которой жертва по собственной воле отдает свое имущество вору. Из-за того, что действия жертв совершаются добровольно, мошенничество, как уголовно наказуемый акт, довольно тяжело фиксировать и привлекать к ответственности людей, эти акты совершающие.

Однако как быть с проявлением Интернет-мошенничества в Интернет-пространстве? Самостоятельно, без помощи правоохранительных органов найти мошенника в Интернете практически невозможно. В уголовном кодексе про Интернет преступность сказано не так много, как их существует в виртуальной реальности. Помимо перечисленных нами статей, выделяются следующие статьи, относящиеся к компьютерной преступности, которыми можно воспользоваться для привлечения к ответственности Интернет-мошенников:

- *статья 272* – неправомерный доступ к компьютерной информации;
- *статья 273* – создание, использование и распространение вредоносных программ для ЭВМ;
- *статья 274* – нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети [53].

Вывод можно сделать следующий: для любого мошенничества в Интернете, в принципе, можно найти подходящую статью УК РФ. Правда, отмечаются некоторые проблемы, и управление «К» МВД РФ, которое занимается расследованием всех Интернет-преступлений, постоянно с ними сталкивается. Все инциденты, связанные с глобальной сетью, отличаются очень большой латентностью, поэтому представляется трудным их отследить. В свою очередь жертвы мошенников не обращаются в правоохранительные органы, считая это бесполезным [45; 53]. И, пока эта ситуация не изменится, исправить положение с мошенничеством в Интернете представляется затруднительным.

Итак, мы рассмотрели юридическое определение понятия мошенничества, определили его характеристики и выделили те статьи, по которым можно привлечь Интернет-мошенников к ответственности. Теперь нам необходимо рассмотреть особенности проявления данного феномена в Интернет-пространстве.

ГЛАВА 2. ИНТЕРНЕТ-МОШЕННИЧЕСТВО КАК ЭЛЕМЕНТ КОММУНИКАТИВНОГО ПРОСТРАНСТВА РУНЕТА

В данной главе нами будут рассмотрены особенности Интернет-мошенничества как элемента коммуникативного пространства Сети. На основании изученных Интернет-источников, посвященных специфике данного явления, мы рассмотрим подходы к определению Интернет-мошенничества, выделим его основные характеристики, существующие типологии, выделив собственные основания для классификации различных видов мошенничества в Сети.

§2.1 Теоретические подходы к определению Интернет-мошенничества

В результате обзора Интернет-источников, посвященных мошенничеству в Интернете, выяснилось, что данному явлению в большинстве случаев присваивается юридическое определение мошенничества [44; 46; 47]. Таким образом, мошенничество определялось как хищение чужого имущества или приобретение права на чужое имущество путем обмана или злоупотребления доверием.

Тем не менее, на одном из ресурсов, нами были найдено определение мошенничества, обусловленное проявлением в рамках Интернет-пространства

«Термин "мошенничество в Интернете" применим в целом к мошенническим махинациям любого вида, где используются один или несколько элементов Интернета – такие как комнаты в чатах, электронная почта, доски объявлений или веб-сайты – для привлечения потенциальных жертв, проведения мошеннических сделок или для передачи поступлений от мошенничества в финансовые учреждения или иным лицам, участвующим в таких махинациях» [43].

В данном определении подчеркивается, что мошенничество в Интернет-пространстве осуществляется по коммуникативным каналам Интернета, везде, где установление коммуникативной связи между пользователями является возможным.

Основной принцип мошенничества в Интернете остается тем же, что и у мошенничества в реальной жизни — ввести жертву в заблуждение, установив с ней доверительные отношения, и, воспользовавшись этим доверием, побудить её под тем или иным предлогом добровольно передать деньги, имущество, права на что-либо мошеннику. На разных ресурсах основной механизм мошенничества имеет различные формулировки, но общий для всех смысл:

«Основной целью лохотронщика является завоевать доверие своей жертвы. Если доверие завоевано, жертва будет делать то, что требуется» [49].

«Сколько бы не было типов мошенничества в Интернете, у мошенника все сводится к простой схеме:

1. Найти «лоха»;
2. Завоевать его доверие;
3. Кинуть его;
4. Исчезнуть. [42]»

§2.2 Особенности мошенничества в Рунете

Следует отметить, какие особые черты присущи мошенничеству в виртуальном пространстве. Авторами различных ресурсов, посвященных Интернет-мошенничеству, преимущественно подчеркиваются особенности Интернет-пространства. В силу этих особенностей мошенничество в Интернете приобретает особые черты, которые мы постарались обозначить.

Во-первых, события и операции в виртуальном мире обычно совершаются «в режиме Интернет-времени», что означает, что в Интернете все совершается быстрее, чем в реальной жизни – деловые решения, поиск информации, личное взаимодействие и многое другое. При этом все эти действия могут совершаться в любое время суток, параллельно совершаемым действиям в реальном мире. Мошенники в Интернете также действуют «в режиме Интернет-времени». Они стремятся использовать уникальные возможности Интернета, такие как мгновенная рассылка сообщений по всему миру, размещение информации на сайтах, которая также доступная всему миру, - для проведения различного рода махинаций [43].

Во-вторых, особенностями Интернет-пространства является физическая удаленность пользователей друг от друга, а также анонимность пользователей в Сети. Поэтому привлечь к ответственности мошенников оказывается весьма затруднительно.

В-третьих, между особенностью мошенничества в Интернете является то, что многие методы не являются нарушением закона в явном виде, и это также не позволяет преследовать мошенников по закону [45;46].

В-четвертых, по мере роста количества пользователей Интернета, а также количества ресурсов с возможностями коммуникации между пользователями возрастает число мошенников, пытающихся использовать данные коммуникативные каналы, чтобы заработать на этих пользователях. В данном случае подчеркивается массовость проявления актов мошенничества в Интернете.

В-пятых, мошенничеством в Интернете также называются акты, связанные с вымогательством. Иными словами, не всегда акты мошенничества совпадают с тем его свойством, что имущество жертвы мошенник приобретает путем установления доверительных отношений. Мошенники могут ставить жертву в условия, неудобные или вредящие ей. Чтобы избавить жертву от этих неудобств, мошенники обычно требуют взамен деньги [40;42;43].

§2.3 Типологии Интернет-мошенничества

На разных ресурсах в Рунете нами были найдены различные классификации видов мошенничества. Приведем примеры основных видов мошенничества в Интернете по методике их исполнения [40; 41; 42; 44; 47; 49].

2.3.1 Типология Интернет-мошенничества по методике исполнения

Кибersквоттинг

Кибersквоттинг (*от англ.* cybersquatting) — это «почти законный» способ заработка денег. Он основан на анализе новостей рынка с целью выявления названий компаний и брендов новых товаров, для которых еще не зарегистрированы

одноименные доменные имена. Обнаружив такой бренд, кибersквоттер регистрирует доменное имя на себя в надежде перепродать его впоследствии компании, владеющей соответствующим брендом.

В общем случае заработок кибersквоттера основан на следующих составляющих:

- продажа доменного имени владельцу бренда.
- шантаж владельца бренда, который может быть основан на угрозах создать подложный сайт компании с информацией, порочащей ее честь и достоинство, или содержащий некорректную информацию о товарах;

Согласно законодательству кибersквоттинг незаконен, так как зарегистрированный товарный знак или бренд имеет приоритет над доменным именем, и у владельца товарного знака есть законные основания для судебного иска.

Тайпсквоттинг

Тайпсквоттинг — это разновидность кибersквоттинга, основанная на регистрации доменных имен, отличающихся от имен раскрученных доменов опечатками или доменной зоной (термин образован *от англ.* type — печатать). Для достижения высокой эффективности тайпсквоттер должен проанализировать статистику типовых опечаток пользователей. Для демонстрации примеров тайпсквоттинга, обратимся к популярным доменными именами «yandex.ru» и «rambler.ru». Первые же попытки сделать опечатку в адресе позволили найти сайты тайпсквоттеров: http://www.yadex.com/**,** http://www.andex.ru/**,** www.ranbler.ru**,** www.rambdler.ru**.** Заработок тайпсквоттера составляет прибыль от размещенной на сайте рекламы, платных ссылок на некие ресурсы или от продажи доменного имени владельцу созвучного имени. В отличие от классического кибersквоттинга, преследовать тайпсквоттера по закону невозможно.

Фишинг

Фишинг является одним из самых распространенных видов мошенничества в Интернете. Термин образован от английского словосочетания «password fishing» (буквально «выуживание паролей») и означает введение пользователя в заблуждение при помощи поддельного сайта, визуально имитирующего сайт банка или иной Интернет-системы, предполагающей идентификацию пользователя. Главная задача фишера — заманить пользователя на такой сайт-ловушку и каким-либо образом убедить его сообщить идентификационные данные. Для решения такой задачи фишеры обычно применяют одну из следующих методик:

- **спам** — его типичная идея заключается в том, чтобы напугать пользователя некими проблемами, требующими от пользователя немедленной авторизации для выполнения тех или иных операций (разблокировки счета, отката ошибочных транзакций и т.п.). В подобном письме имеется ссылка на поддельный сайт, причем визуально подобная ссылка обычно неотличима от настоящей. Более простая форма фишинга состоит в рассылке поддельных писем от имени банка или некого провайдера услуг с просьбой уточнить номер счета, логин/пароль и прочие персональные данные, отправив их по указанному адресу;

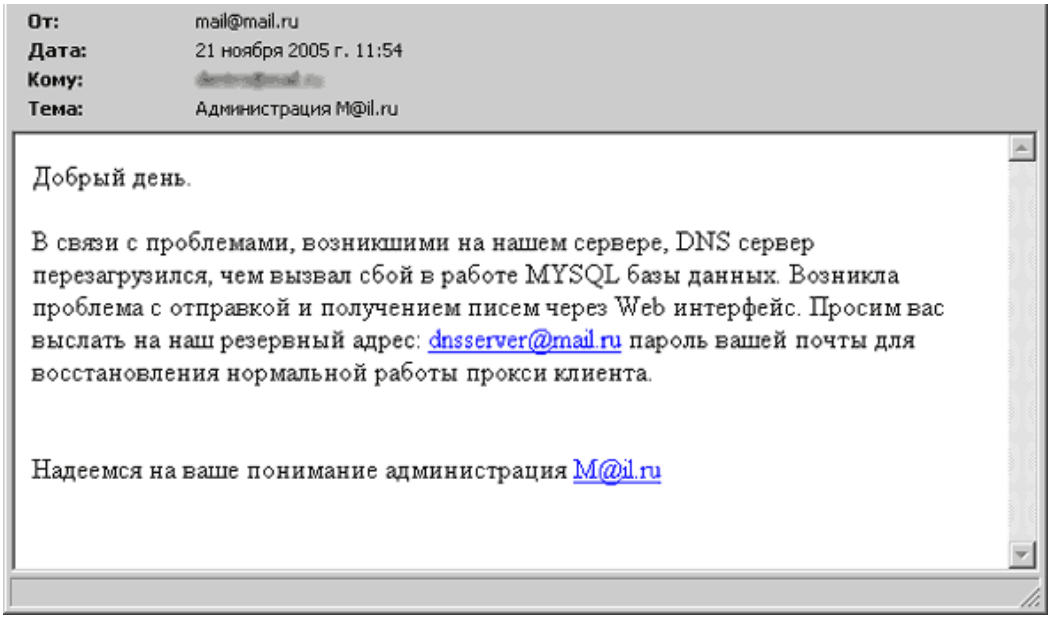


Рис. 2.3 1. Пример фишинг-письма пользователям почты Mail.ru [40]

○ **реклама неких товаров или услуг**, которые можно приобрести в Интернет-магазине или же ознакомиться об услуге на сайте, причем в рекламе обязательно приводится ссылка на данные сайты. Методика аналогична предыдущей — вместо сайта магазина пользователь может попасть на сайт фишеров или на сайт созданного мошенниками магазина-однодневки;

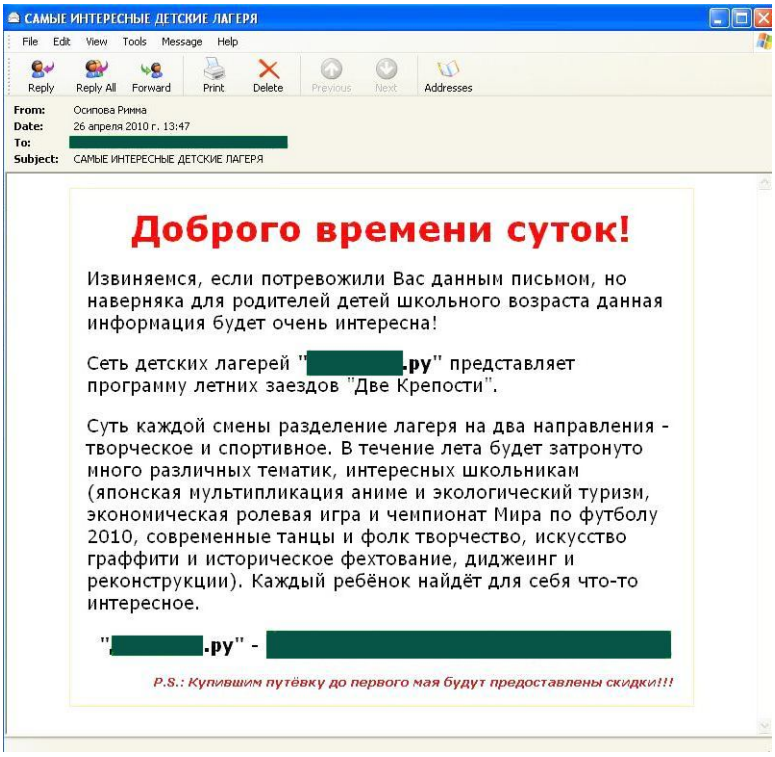


Рис. 2.3.2. Пример фишинг-письма в виде предложения услуги [50]

- **применение троянской программы** (например, класса Trojan.Win32.DNSChanger) для перенаправления пользователя на сайт фишеров при попытке доступа к обычному легитимному сайту.

В последнее время появилась новая форма фишинга — **выуживании у пользователя отсканированных копий его документов**. В частности, имея ксерокопию паспорта и образец подписи, теоретически можно оформить кредит от имени пользователя. Получить отсканированные копии документов доверчивого пользователя несложно — например, прислать ему сообщение о том, что он выиграл в лотерею, является *N*-тысячным посетителем сайта X и т.п.

Мошенничество с платежными системами

Различные методики мошенничества с платежными системами и системами экспресс-оплаты нередко могут быть классифицированы как одна из форм фишинга. Однако ввиду особой распространенности рассмотрим данную форму мошенничества более подробно. С точки зрения реализации можно назвать массу вариантов, в частности:

- **магические кошельки** — принцип обмана состоит в том, что при помощи спама или специально созданного веб-сайта злоумышленник описывает некую уязвимость или «недокументированную особенность» системы, позволяющую получить прибыль, переводя некоторую сумму на указанный кошелек. В описании метода сообщается, что через некоторое время деньги вернутся, к примеру, в удвоенном количестве. Естественно, что уязвимости никакой нет, и деньги получает злоумышленник;

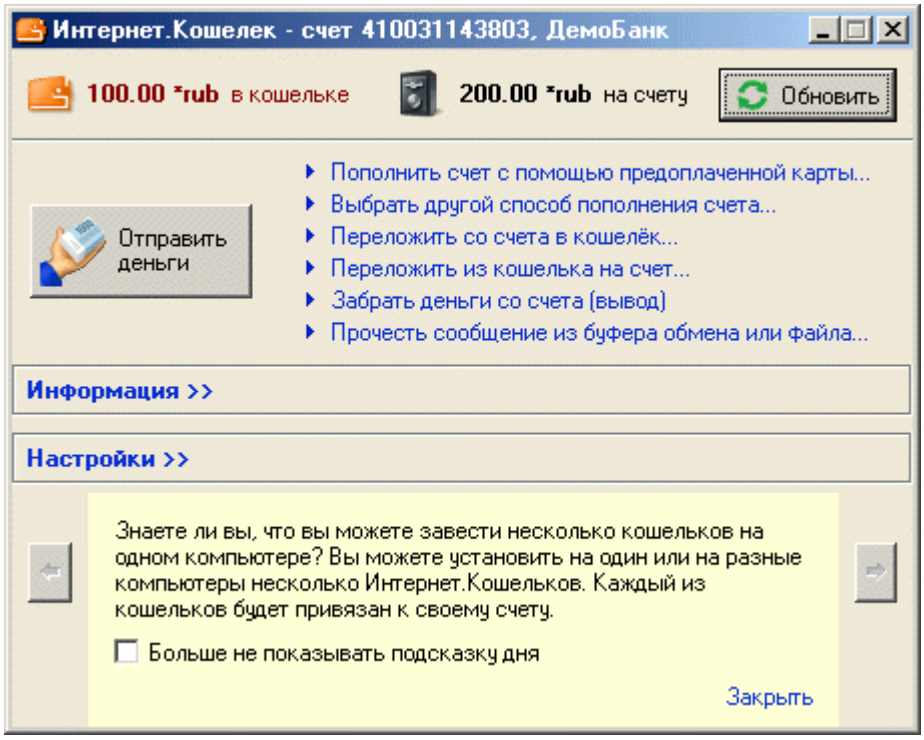


Рис. 2.3.3. Пример мошенничества по методике «Магический кошелек» [48]

- **поддельные обменники** электронных денег и сервисы оплаты различных услуг;

- **пирамиды с использованием платежных систем**;
- **мошеннические Интернет-банки**, которые предлагают вложить электронные деньги на очень выгодных условиях, после чего пользователь не получает ни денег, ни процентов;
- **мошеннические биржи труда**, предлагающие за небольшую плату подыскать престижную работу (естественно, что деньги они получают, но взамен ничего не предоставляют). Аналогичным образом устроены мошеннические системы дистанционной работы: соискателю обещают дистанционную работу, но за «оформление документов» или иную операцию предлагают заплатить 10-15 долл.;
- **Интернет-лотереи**, казино и прочие виды азартных игр; Пользователям рассылаются **фальшивые извещения о выигрыше в лотерею,** якобы проводимую среди случайных e-mail адресов/номеров телефонов, и предложения получить «бесплатные» подарки в качестве выигрыша. Для убедительности в таком письме может присутствовать фотография приза и всевозможные «атрибуты подлинности» лотереи - номер билета, свидетельство о регистрации/лицензии и прочая фальшивая информация. Для получения выигрыша пользователю под разными предлогами предлагается предварительно совершить платеж на некую сумму по указанным мошенниками счетам.

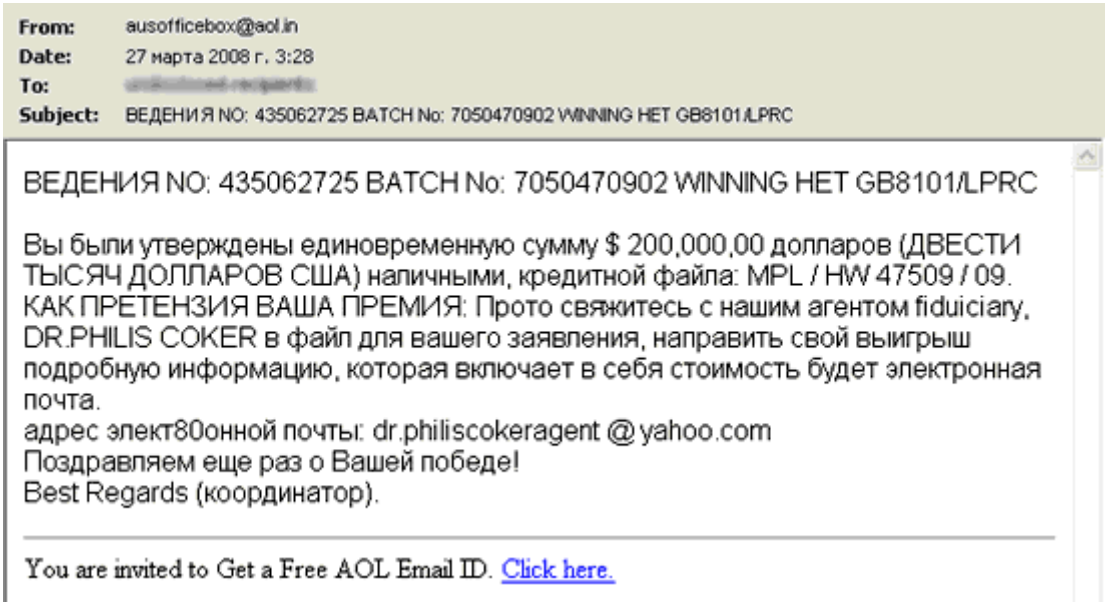


Рис. 2.3.4. Пример письма-извещения о выигрыше в лотерею [42]

- **поддельные письма или сообщения по ICQ** от имени пользователя с просьбой одолжить небольшую сумму денег. Типовая схема — похищение паролей с ПК пользователя при помощи троянской программы, захват электронной почты и ICQ и последующая отсылка просьбы одолжить деньги;
- **попрошайничество** — это обычно спам (по почте и в различных форумах) с просьбой перевести деньги на срочную операцию для спасения ребенка, ремонт или восстановление храма, помощь детскому дому и прочие подобные вещи;

- **«Нигерийские» письма** – схема мошенничества, разработанная и применяемая мошенниками из Нигерии, за что и получила свое название. Однако в настоящее время «нигерийским» мошенничеством промышляют аферисты во всем мире. При реализации классической «нигерийской» схемы спамеры рассылают письма от имени представителя знатной семьи (как правило, проживающей в каком-либо африканском государстве), которая попала в немилость на родине по причине гражданской войны /государственного переворота/экономического кризиса/политических преследований. В классических «нигерийских» письмах к адресату обращаются на ломаном английском языке с просьбой помочь «спасти» крупную сумму денег, переведя ее со счета опального семейства на другой счет. За услугу по переводу денег мошенники обещают солидное вознаграждение – как правило, проценты от переводимой суммы. В ходе «спасательной операции» выясняется, что добровольному (хотя и небескорыстному) помощнику требуется перевести небольшую по сравнению с обещанным вознаграждением сумму для оформления перевода /дачи взятки /оплаты услуг юриста и т.п. Как правило, после перечисления денег всякая возможность общения с «вдовой бывшего диктатора» или «сыном покойного опального министра» исчезает. Иногда жертву вынуждают еще несколько раз раскошелиться, под тем предлогом, что возникли очередные непредвиденные осложнения.
- **«скамерство»**. Скамерство (от английского «scam» – жульничество) в русском Интернет-пространстве означает знакомство в Интернете для выманивания денег [51]. Технологический процесс скамерства заключает в том, что мошенники регистрируются на сайтах знакомств, где находят потенциальных жертв - обычно иностранных граждан, чтобы завязать с ними виртуальные отношения. Мошенник под именем девушки заводит быстрый Интернет-роман, а потом просит перевести «ей» определенную сумму денег. Деньги «необходимы» девушке по разным причинам – на визу, билеты, на то, чтобы быть вместе. Обычно первые деньги скамер получает через два месяца, в которые нужно уложить знакомство, дружбу, любовь и желание встретится наяву, к сожалению, неосуществимое.

Итак, данный список содержит только основные формы мошенничества, однако у них есть общая черта — попытка выудить у пользователя деньги. Проблема усугубляется тем, что электронный платеж сложно проследить, а незначительность сумм зачастую не позволяет возбудить уголовное дело.

Hoax-программы

Задача программы Hoax - ввести пользователя в заблуждение с целью получения финансовой выгоды. По принципу действия можно выделить несколько разновидностей Hoax:

- платные программы для взлома чего-либо, обмана платежных систем или интернет-казино. Подобную программу обычно можно скачать и запустить в демо-режиме, у нее есть сайт и документация. В случае запуска пользователь видит интерфейс программы, а в документации указано, что якобы в демо-режиме заблокирована функциональность программы. После оплаты происходит одно из двух: либо программа исчезает, либо жертве высылается ключ активации, после ввода

которого программа или имитирует процесс взлома чего-то, или попросту выдает сообщение о том, что взламывать что-либо нехорошо, и что это был розыгрыш.

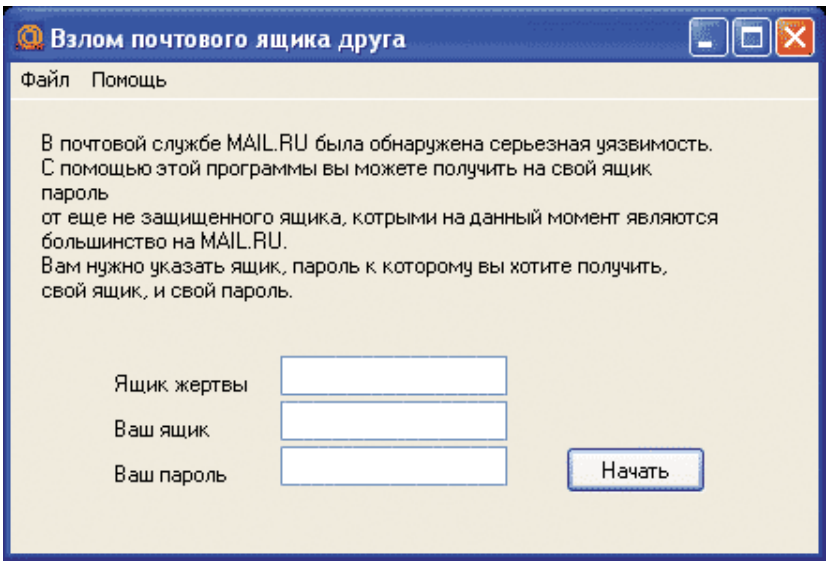


Рис. 2.3.5 . Пример программы для взлома почтовых ящиков, в реальности отправляющая введенные данные злоумышленнику [40]

- **генераторы кодов активации**. Обычно эти Hoax по сути представляют собой троянские программы, предлагающие ввести номер неактивированной карты экспресс-оплаты для ее «клонирования». Принцип работы подобной троянской программы сводится к отправке введенных данных злоумышленнику и имитации процесса «клонирования» на время, достаточное злоумышленнику для активации карты;

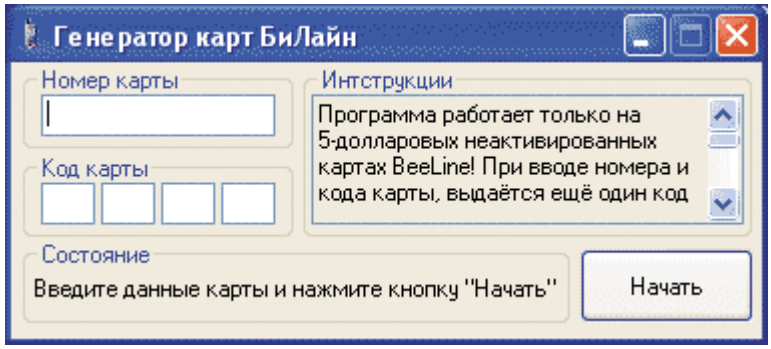


Рис. 2.3.6. Пример программы для клонирования карт оплаты телефона, которая пересылает введенный код неактивированной карты злоумышленнику [40]

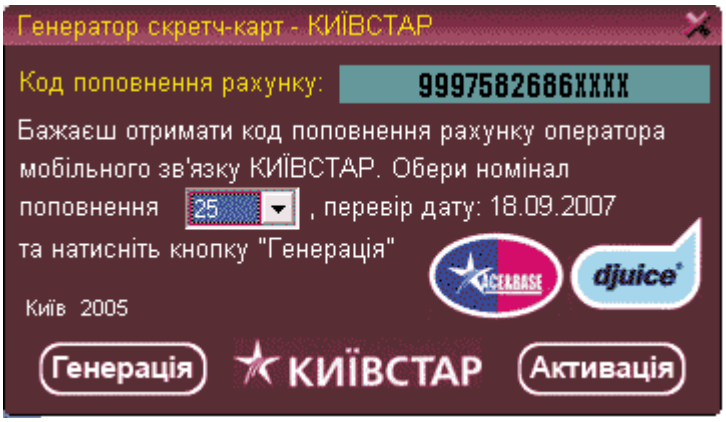


Рис. 2.3.7. Пример Hoax-программа, авторы которой обещают, что в случае покупки и активации программа будет генерировать номера карт оплаты провайдера KievStar

- **имитаторы вирусов и антивирусов**. Работают они следующим образом: имитируется заражение компьютера вредоносной программой и настоятельно рекомендуется скачать программу-антивирус. Интересно, что последние версии таких программ скрытно загружают и устанавливают рекламируемый «антишпион», что теоретически просто обязано насторожить пользователя.

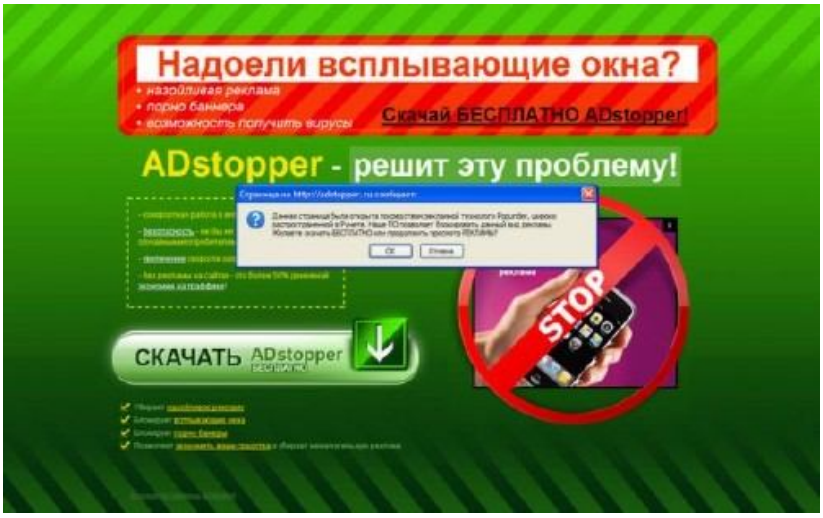


Рис.2.3.8 Пример Hoax-программы в виде программы-антивируса [49]

SMS-голосование и оплата

Принцип данного мошенничества основан на появлении в последнее время систем оплаты при помощи отправки SMS на специальный номер. Принцип обмана состоит в том, что на неком Интернет-сайте пользователю предлагается послать SMS с заданным текстом на указанный короткий номер под любым предлогом, обычно предлагается проголосовать за сайт, оплатить доступ к закрытому разделу сайта или загружаемому контенту и т.п. Обман состоит в том, что не указывается реальная стоимость, которая будет списана со счета отправившего SMS пользователя (Рисунок 2.3.9).

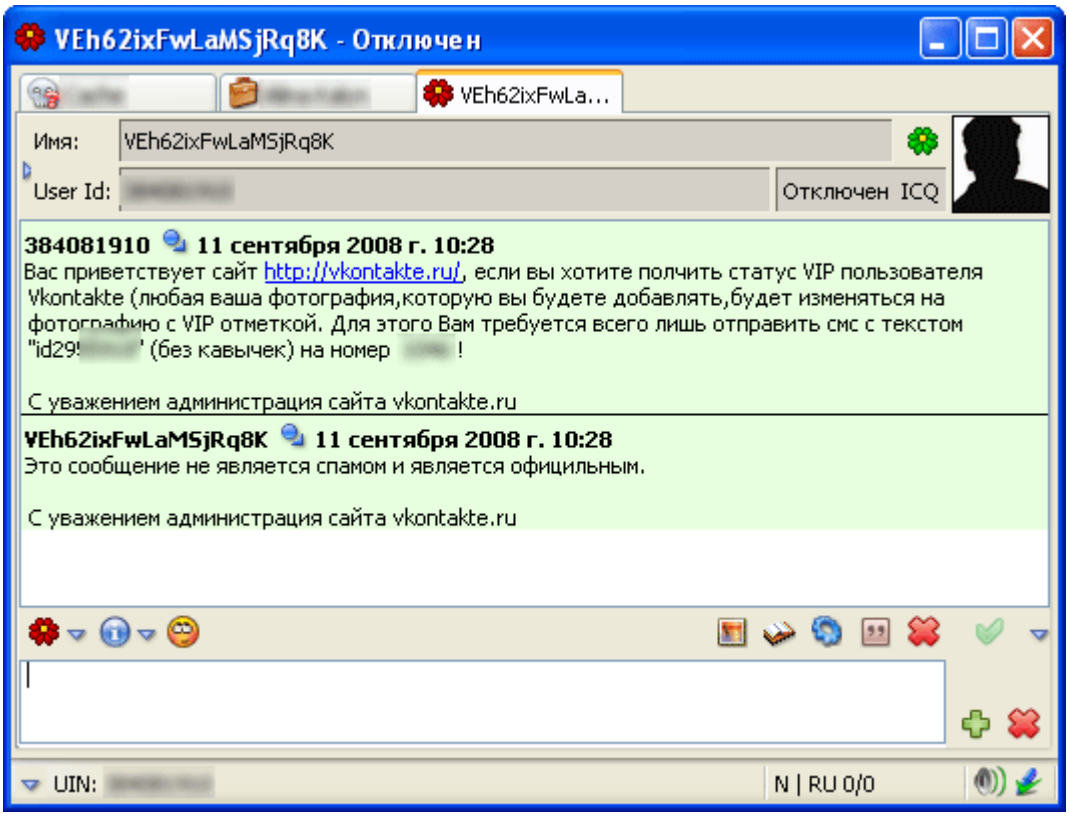


Рис. 2.3.9. Пример мошенничества посредством SMS-оплаты услуг [52]

Взлом сайтов и DDoS-атаки

Данное направление является криминальным в чистом виде и основано на том, что злоумышленники нарушают функционирование того или иного Интернет-ресурса с последующим вымоганием денег за прекращение атаки, информацию об обнаруженной уязвимости или за гарантию того, что сайт не будет взламываться в течение определенного времени.

Широко распространенным примером взлома является кража пароля от учетной записи пользователя ICQ. Впоследствии злоумышленник предлагает обладателю этой учетной записи «выкупить» ее обратно.

Блокировка компьютера и данных пользователя

Такая методика вымогательства основана на обратимой блокировке работы компьютера. Типовой пример — использование троянского вируса Trojan.Win32.Agent.il. После того, как мошенники заражают компьютер пользователя, они предлагают пользователю заплатить некоторую сумму за «противоядие».

Примером блокировки данных пользователей могут служить баннеры, которые появляются на основной центральной части экрана монитора пользователя поверх всех окон, что заметно затрудняет работу. Чтобы избавиться от баннера, обычно необходимо отправить SMS на определенный номер, чтобы получить код для его снятия.

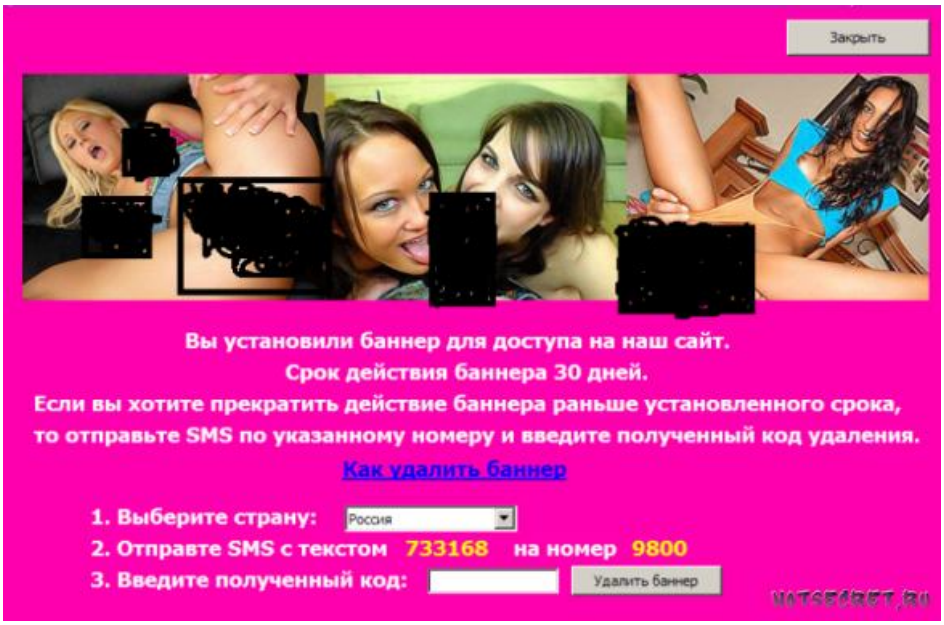


Рис. 2.3.10 . Пример взлома компьютера пользователя в виде установки баннера [41]

Мы привели пример типологии мошенничества в Сети по принципу используемой методики. В ней, на наш взгляд, описано большинство основных способов мошенничества. В результате уже изученных нами видов мошенничества, мы выделили несколько собственных оснований для типологии и классификаций видов мошенничества в виртуальном пространстве.

2.3.2 Типология Интернет-мошенничества по каналам коммуникации

Виды мошенничества могут распределяться и иметь свою специфику в зависимости от канала коммуникации:

- **Агенты мгновенного сообщения (ICQ, QIP и т.д.)**. Данные каналы используются обычно фишерами и киберсквоттерами для личного обращения к пользователям данных программ. Обращения могут быть в форме предложению товаров и услуг, в форме просьб перевести небольшое количество денег, уведомления о выигрыше в лотерее и т.д. Часто мошенники притворяются «знакомыми» адресату людьми, чтобы войти к нему в доверие.
- **Форумы/чаты.** На форумах и в чатах обращение к пользователям носит публичный характер. Используются мошенничества с платежными системами, различные формы фишинга с рекламой и предложением услуг, просьбами, попрошайничеством о переводе писем, Hoax-программы и т.д.
- **Аккаунты пользователей социальных сетей («ВКонтакте», «Одноклассники»)**. Обращение к пользователю по данному каналу несет личный характер, как и в случае с агентами мгновенных сообщений. Мошенники способны с помощью определенных программ отправлять личные сообщению с аккаунтов друзей и знакомых пользователя, обращаясь с просьбами перевести сумму денег, проголосовать за друзей, отправив SMS, и т.д.

- **Электронная почта.** По электронной почте с помощью спама осуществляется деятельность фишеров: нигерийские письма, мошенничество с платежными системами, реклама и предложение различных видов услуг, просьб, попрошайничество, вакансии на работу. Активно предлагают свои услуги распространители Hoax-программ, услуги по «SMS». Через электронную почту обычно связываются с пользователями кибберсквоттеры и тайпсквоттеры.
- **Сайты.** На сайтах возможно использование всевозможных видов мошенничества. Многое зависит от тематики сайта. Если это сайт определенного контента, то мошенники могут использовать мошенничество с платежными системами, разные виды фишинга, используя ссылки и текстовые сообщения, соответствующие контенту сайта. Стоит особенно выделить сайты знакомств. **Сайты знакомств** являются основным пространством для деятельности скамеров. Однако тут также можно встретить акты фишинга в виде рекламы, баннеров и т.д. Здесь можно попасть на вредоносные ссылки, открытие которых может повлечь за собой запуск Hoax-программ или других программ, вредящих данным компьютера пользователя.
- **Личный ПК пользователя.** В данном случае имеются в виду взломы компьютера пользователей в виде поражения компьютеров вирусами, блокировкой данных, установлением баннеров. Также используются Hoax программы – имитаторы вирусов и антивирусов.

2.3.3 Типология Интернет-мошенничества по сфере воздействия

- **Личная сфера. Сфера чувственных мотиваций**. В данную категорию мы отнесем те виды мошенничества, которые ориентированы на эмоционально-чувственный отклик у пользователя. Сюда мы включим те мошенничества, которые осуществляются в форме просьб о денежной помощи, благотворительных акций, попрошайничества, помощи в голосовании. В данном случае мошенники «давят» на чувство жалости пользователя и его великодушие. Зачастую используются приемы отправки сообщений от лица знакомых и друзей пользователей, чтобы привлечь внимание пользователя и повысить его желание помочь. Сюда также включаются оповещения о внезапном выигрыше в лотерею, разнообразие «совершенно бесплатных» услуг, которые предлагают мошенники. В данную категорию мошенничества мы отнесем и скамерство. За счет того, что жертва влюбляется в образ, созданный мошенником, она готова оказывать финансовую помощь объекту своих чувств. В данном виде мошенничества особенно сильно задействована чувственная мотивация жертвы.

«Доброго здоровья! Месяц назад к нам приблудился кот. Он был поранен злыми собаками. Кровь сочилась фонтаном из его лапок. Я выходил его и он выздоровел. Мне мама давала денег на завтрак, но я покупал еду для больного котика. За это время он стал мне единственным другом, который не предаст и не продаст. Но беда в том, что у меня брат просто живодер какой-то. Он сказал, что сдаст его на шапку. Он бил моего друга ногой, обутой в кирзовый сапог! Впрочем, он сказал, что не тронет кота, если я ему дам 100 долларов. Люди добрые, помогите! Он такой чудный и ласковый! Он пушистый, белый, с серыми подпалинами. Не будьте черствыми, я хочу верить, что справедливость на свете существует. Деньги перечислите на WMZ(R)XXXXXXX».

Рис. 2.3.11. Пример Интернет-мошенничества по сфере чувственных мотиваций [47]

- **Деловая сфера. Сфера профессиональных, деловых мотиваций.** Сюда относятся Интернет-мошенничества, связанные со сферой деловых отношений, труда и заработка. Поэтому сюда мы отнесем, в первую очередь, кибersквоттинг и тайпсквоттинг, поскольку мошенники, используя данные техники, зарабатывают именно на мотивации пользователя завладеть необходимым для него доменом, находящегося в обладании сквоттеров. Сюда также можно отнести все мошенничества, связанные с финансовым заработком: магические кошельки, пирамиды с использованием платежных систем, мошеннические биржи труда и т.д.

2.3.4 Типология Интернет-мошенничества по коммуникативным средствам

Виды мошенничества можно классифицировать по тому коммуникативному средству, которое используется в его оформлении.

- **Визуальные.** К визуальным средствам мы отнесем использование мошенниками различных образов. В основном они имеют вид картинок или баннеров. Они используются в спам-рассылках или же оформляются на сайтах в виде гиперссылок или баннеров, в качестве рекламы или предложений товаров, услуг, Интернет-магазинов и т.д. Также спамеры используют в рассылке форму визуализации текста, т.е. оформления текста в виде файла-изображения, что снижает для них риск блокировки входящих спам-писем со стороны Интернет-пользователей.

Рис. 2.3.12. Пример визуального мошенничества в виде баннера-рекламы[42]

- **Текстовые.** Текстовые средства подразумевают оформление мошенничества в виде текста. Сюда относятся ICQ-сообщения, текстовые спам-рассылки, описание предложений, объявлений, которые адресуются пользователям в текстовой форме. К текстовому способу оформления мошенничества относятся многие формы фишинга, кибersквоттинга, тайпсквоттинга, мошенничества с платежными системами, Hoax-программы и т.д.

«Здравствуйте! Я недавно завел себе WM-кипер. Как известно, WM-идентификаторы, если за полгода там остается нулевой остаток, то WM-кипер закрывается. Я работаю со спонсорами, но не набрал еще минималку. Если мне закроют кипер, то я не получу свои деньги. Пожалуйста, вышлите на WMZ(R)XXXXXXX 1 цент (копейку). Выручите меня, прошу Вас. Я новичок, мне так трудно».

Рис. 2.3.13. Пример Интернет-мошенничества в виде текста [47].

- **Смешанные.** К смешанной категории относятся большинство видов Интернет-мошенничества. При данном оформлении используются как визуальные образы, так и текстовая информация.

2.3.5 Типология Интернет-мошенничества по степени оказываемого психологического давления

- **Предложение.** В эту категорию относятся все виды мошенничеств, в основе которых лежит предложение какой-либо услуги или же товара. Предложение подразумевает добровольность действий и свободу выбора адресата мошенничества. Сюда входят некоторые из форм фишинга, основанные на рекламе товаров или услуг; волшебные кошельки; поддельные обменники; финансовые Интернет-пирамиды; Интернет-лотереи, казино; Интернет-биржи труда; программы Hoax для взлома, генераторы ключей активаций; различные SMS-предложения
- **Просьба.** Мы включаем сюда мошенничество с платежными системами, где формой обращения мошенников к пользователям является просьба. Сюда относятся нигерийские письма, поддельные письма или сообщения по ICQ с просьбой одолжить небольшую сумму денег, попрошайничество денег с целью оказания благотворительной помощи и т.д.
- **Требование.** Мошенники ставят пользователей в такие условия, когда жертва становится мотивированной перевести мошенникам определенную денежную сумму. Действия мошенников имеют форму принуждения, а просьба денежных средств в данном случае сменяется вымогательством денег у жертвы. Сюда входят такие виды мошенничества, как взлом сайтов и данных пользователя; блокировка компьютера пользователя; Hoax-программы, имитирующие вирусы и антивирусы; кража учетных записей пользователей мошенниками, впоследствии требующих выкуп за возвращение паролей; кибersквоттинг; тайпсквоттинг; формы фишинга, в которых пользователей запугивают некими проблемами, требующими от них немедленной авторизации для выполнения необходимых операций или же «выуживания» денег.

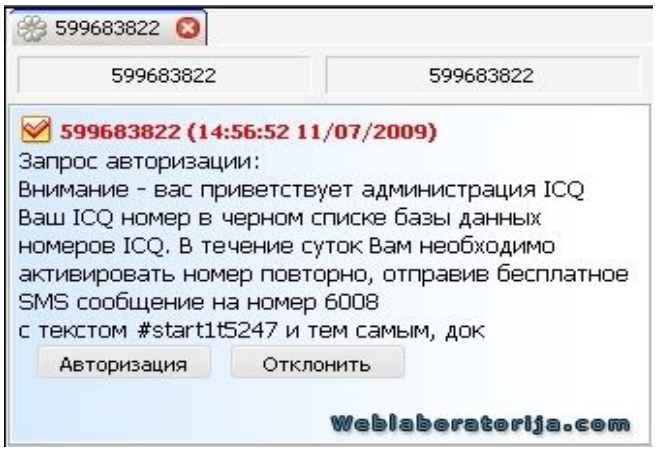


Рис. 2.3.14. Пример Интернет-мошенничества по ICQ в форме требования [49]

- **Угроза.** Мошенники оказывают на пользователя давление посредством угрозы. Примерами могут служить: взломы сайтов пользователей, в которых мошенники угрожают безвозвратно навредить или заблокировать данные пользователя; формы фишинга в виде, спам-писем, где угрожают заблокировать аккаунт ICQ или e-mail, поскольку он якобы попал в «черный список» за спам-рассылки, и.т.д. Во всех случаях мошенники обычно требуют деньги, чтобы оставить пользователя «в покое». Примером может служить «выуживание денег» через SMS. Пользователю шлется письмо с угрозой, что ему заблокируют почтовый ящик, если он не пошлет SMS.

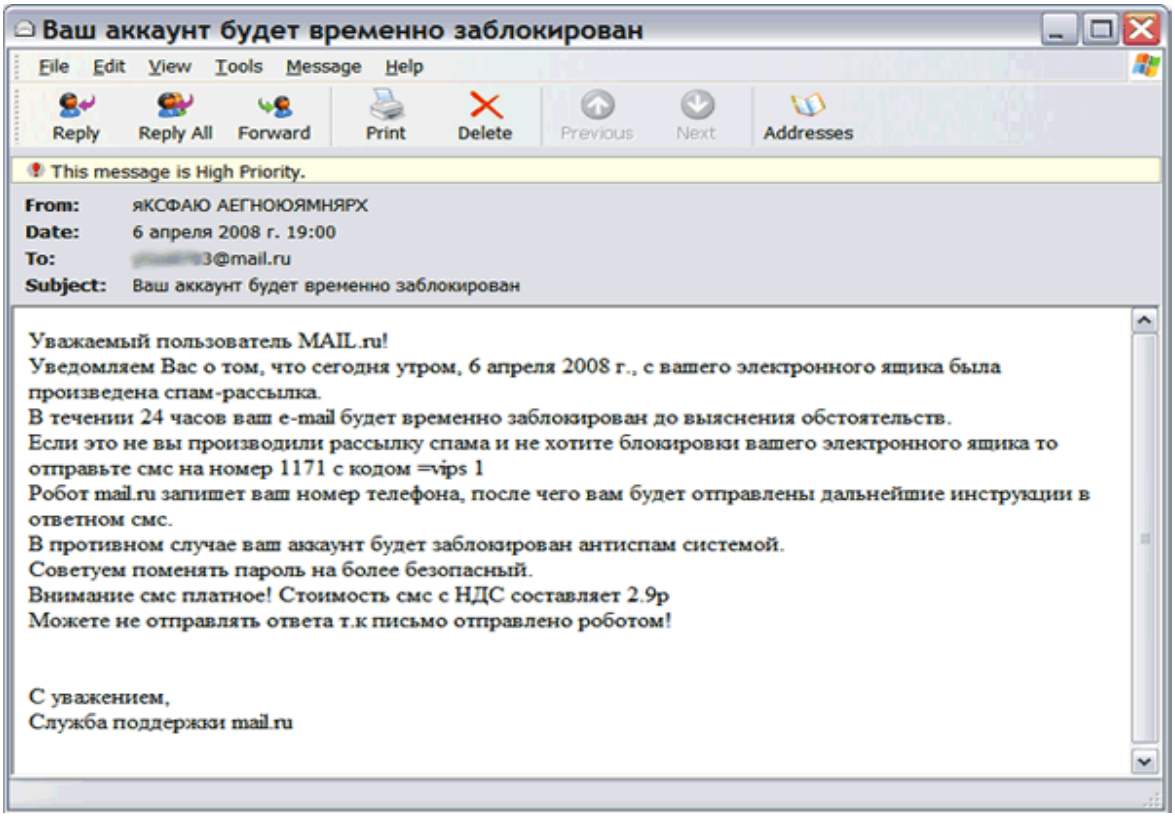


Рис. 15. Пример Интернет-мошенничества в форме угрозы [50]

ГЛАВА 3. ЭМПИРИЧЕСКОЕ ИССЛЕДОВАНИЕ ФЕНОМЕНА ИНТЕРНЕТ-МОШЕННИЧЕСТВА

В предыдущих главах были рассмотрены теоретические основания для изучения феномена Интернет-мошенничества. Мы рассмотрели феномен мошенничества, основываясь на теориях виртуализации, а также через призму понятия манипуляции. Нами также была изучена правовая база, регулирующая мошенничество в реальной и виртуальной жизни. Мы выяснили, как определяется понятие Интернет-мошенничества в Рунете, определили основные виды мошенничества. Помимо этого, были предложены собственные типологии видов данного явления по следующим основаниям: по каналам коммуникации, по сфере воздействия, по коммуникативным средствам, по степени оказываемого психологического давления.

Если подвести итог двух глав работы, то можно сказать, что был проведен анализ теоретической и информационной базы, касающейся феномена Интернет-мошенничества, а также подготовлена теоретическая основа для эмпирического исследования данного явления.

В данной главе будет изложена программа и результаты эмпирического исследования, касающегося изучения Интернет-мошенничества.

§ 3.1 Программа исследования феномена Интернет-мошенничества

Цель исследования – изучение специфики практик столкновения пользователей Рунета с Интернет-мошенничеством, а также отношения пользователей к данному феномену.

Задачи исследования:

- Выяснить типовые ситуации мошенничества, которые знакомы пользователям, и с которыми они сталкивались;
- Определить каналы коммуникаций, которые используют мошенники;
- Выяснить отношение пользователей к Интернет-мошенничеству;
- Выделить категории пользователей в зависимости от различий в практиках столкновения с Интернет-мошенничеством:
  - пользователи, которые никогда не встречались с Интернет-мошенничеством;
  - пользователи, которые встречались с Интернет-мошенничеством, но никогда не попадались на обман мошенников;
  - пользователи, которые встречались с Интернет-мошенничеством и сумели вовремя предотвратить акт мошенничества по отношению к ним;
  - пользователи, которые встречались с Интернет-мошенничеством и которые попадались на мошенничество;
- Выяснить типовые ситуации мошенничества, которые использовались по отношению к пользователям;
- Выяснить социально-психологические последствия действий мошенников: какие потери понес пользователь-жертва, и как он себя ощущает;

- Выяснить ответные действия жертвы и результаты этих действий: пытался ли человек обращаться в правоохранительные органы или другие места для того, чтобы найти мошенников, привлечь их к ответственности и вернуть потерянное имущество.
- Выделить категории пользователей в зависимости от типа ответных реакций на мошенничество:

  - пользователи, обращавшиеся в правоохранительные органы по делу мошенничества;

  - пользователи, обращавшиеся в другие места по делу мошенничества;

  - пользователи, ничего не предпринимавшие после совершенного мошенничества;

  - пользователи, ничего не предпринимавшие после совершенного мошенничества.

Объект исследования - люди, включенные в коммуникативное пространство Рунета.

Для более глубокого изучения особенностей Интернет-мошенничества нам следовало бы обратиться самим субъектам, участвующим в процессе мошенничества - мошенникам и их жертвам - с целью изучения специфики их деятельности, мотивов обеих сторон, технологий мошенничества. Однако изучение мошенников представляется затруднительным, поскольку данная социальная группа попадает в категорию правонарушителей, что, вероятно, мотивирует их скрывать свои действия и личности. Исследователь же не обладает необходимыми связями для возможного установления контакта с Интернет-мошенниками. Поэтому их деятельность мы изучаем исходя из анализа их сообщений, адресованных потенциальным жертвам, а также информационной базы, т.е. Интернет-ресурсов, где совершаются мошенничества и обсуждаются практики мошенничества.

Мы также решили не ограничиваться опросом жертв Интернет-мошенничества. Жертвы Интернет-мошенничества – это лишь узкий сегмент пользователей Рунета, которые сталкивались с мошенничеством. Поэтому в нашем исследовании мы посчитали целесообразным опросить любых пользователей Рунета, чтобы в дальнейшем выделить категории пользователей в зависимости от различий в их опыте столкновения с Интернет-мошенничеством.

Предмет исследования - уникальность и специфика Интернет-мошенничества как элемента коммуникативного пространства Рунета

Основные гипотезы исследования

Гипотеза 1: Частота попаданий в число жертв Интернет-мошенничества зависит от опыта пользования сетью Интернет.

Гипотеза 2. Частота попаданий в число жертв Интернет-мошенничества зависит от знаний основных техник мошенничества и опыта столкновения с ними.

Гипотеза 3: Частота попаданий в число жертв Интернет-мошенничества зависит от возраста Интернет-пользователя.

Гипотеза 4: Попавшись на мошенничество, Интернет-пользователи не пытаются предпринять действия, чтобы привлечь мошенников к ответственности.

Гипотеза 5: Отношение к Интернет-мошенничеству зависит от возраста Интернет-пользователя.

Гипотеза 6: Отношение к Интернет-мошенничеству зависит от того, сколько раз пользователь Интернета попадался на мошенничество.

Гипотеза 7: Большинство Интернет-пользователей в ситуации мошенничества обвиняют мошенников, которые обманули пользователя.

Метод

В качестве метода исследования был использован метод виртуального анкетного опроса, размещенного на сервере «SurveyMonkey» (образец анкеты дается в приложении 2). Веб-страница с опросом находилась в свободном доступе для всех пользователей Рунета до окончания срока проведения исследования. Метод электронной анкеты является, на наш взгляд, наиболее оптимальным для применения в нашем исследовании по трем причинам:

Во-первых, Интернет-мошенничество - это явление, рожденное в виртуальном пространстве, соответственно проводить опрос нам показалось также необходимым в рамках виртуального пространства.

Во-вторых, по целям нашего исследования нам необходим опрос Интернет-пользователей, поэтому мы посчитали целесообразным опрашивать пользователей непосредственно в Интернете.

В-третьих, электронная анкета – это наиболее удобный способ опроса большого количества людей в Интернете, поскольку она удобна в навигации и заполнении. Заполненная анкета автоматически отправляется в базу исследователя.

Все заполненные анкеты автоматически перенаправлялись в базу программы «ДА-система», откуда база могла быть экспортирована в любые программы по работе с табличными данными, включая Microsoft Excel и SPSS. В нашем случае для обработки данных мы использовали программу SPSS.

Выборка

В нашем исследовании использовалась ***стихийная выборка***, поскольку по цели исследования нас интересовали все категории пользователей Рунета. Объем выборки заранее не устанавливался. Анкета находилась в доступе в период с 13 апреля 2011 г. по 4 мая 2011 г. (3 недели). Мы придерживались принципа получения максимально большого объема выборки за этот период.

Ссылка на анкету рассылалась по различным коммуникационным каналам сети:

1. Рассылка списку лиц из контакт-листа программы QIP;
2. Рассылка через программу Mail-ru – агент;
3. Рассылка через личные сообщения в электронных социальных сетях «ВКонтакте» и «Одноклассники»;
4. Публикация ссылок в группах в социальной сети «ВКонтакте»;

5. Форумы, на которых обсуждается тема Интернет-мошенничества: «форум фан-клуба Лаборатории Касперского», форум сайта «Антимаг.ру», форум сайта «W-security» [53;54;55];
6. Также использовался «метод снежного кома»: каждому пользователю была адресована просьба переслать ссылку на анкету своим друзьям или близким.

Этапы проведения исследования

Исследование проводилось в три этапа:

- На первом этапе было проведено 10 пилотажных Интернет-опросов с пользователями Рунета, чтобы уточнить понятия, связанные с Интернет-мошенничеством. Результаты данного исследования помогли нам, во-первых, в определении значений некоторых понятий, а, во-вторых, в последующем составлении более подробной анкеты.
- На втором этапе исследования проводился электронный анкетный опрос пользователей Рунета.
- На третьем этапе производилась обработка результатов опроса при помощи программы SPSS, проверка гипотез, формулировались выводы и заключение.

§ 3.2 Основные результаты проведения эмпирического исследования Интернет-мошенничества

В данном параграфе будут изложены основные результаты эмпирического исследования. В целях экономии места и удобства чтения основные выводы будут приводиться в текстовом виде с указанием ссылок на данные таблиц сопряженности и вычислений коэффициентов, размещенных в Приложении 3.

В период с 13 апреля 2011 г. по 4 мая 2011 г. в опросе участвовали 365 пользователей Рунета. Из них 312 респондентов заполнили анкету более, чем на 50%, и дошли до конца опроса. Для дальнейшего анализа мы использовали базу из 312 ответивших респондентов.

Дадим описание выборки по основным демографическим характеристикам:

- *По возрасту.* Более половины ответивших респондентов относятся к возрасту 18-22 лет (53% респондентов). На анкету ответили 39% респондентов в возрасте 23-35 лет, 5% ответивших в возрасте 13-17 лет, 2% в возрасте 36-50 лет, а также 1% ответивших оказались старше 50 лет (Таблица 3.2.1).
- *По полу.* Среди ответивших респондентов 71% - женского пола, и 29% респондентов – мужского пола (Таблица 3.2.2).
- *По образованию.* Среди ответивших 44% респондентов с незаконченным высшим образованием, 41% ответивших с высшим образованием. Среднее образование имеют 8% ответивших, среднее специальное – 5% ответивших, и неполное среднее – 3% респондентов (Таблица 3.2.4).
- *По типу населенного пункта.* Среди респондентов большинство ответивших проживают в Москве (85%), 4% респондентов проживают в районных центрах, малых городах, 3% респондентов из Санкт-Петербурга (Таблица 3.2.5). На опрос также

ответили 3% респондентов из областных центров, и 2% респондентов, проживающих в поселке городского типа.

Далее перейдем к ответам на исследовательские вопросы и проверке гипотез.

Среди ответивших выделилась группа респондентов, которые не сталкивались с мошенничеством в Интернете (3% к числу ответивших) (Рисунок 3.2.1). Данной группе респондентов по задаче опроса полагалось пропустить основную часть анкеты и переходить к социально-демографической части опроса.

Одной из задач исследования было определение типовых ситуации мошенничества, которые знакомы пользователям, и с которыми они сталкивались.

Респонденты отмечали, с какими техниками мошенничества они знакомы и встречались, о каких знают, но не встречались. Практически все респонденты встречались в Интернете со спамом (98% респондентов) (Таблица 3.2.6). Большинство респондентов сталкивались с мошенничеством с платежными системами: SMS-оплатой и голосованиями (83%), фальшивыми извещениями о выигрыше в лотерею (72%). Также большинство респондентов знакомы и встречались в Интернете с фишинг-мошенничеством в виде рекламы товаров и услуг (71%), попрошайничеством (68%), тайпсквоттингом (56%), имитаторами вирусов и антивирусов (53%).

Среди техник, которые знакомы, но не встречались пользователям, большинство респондентов отметили взлом сайтов и DDoS-атаки: кража пароля от учетной записи пользователя (52%) (Таблица 3.2.7). В целом результаты показали, что большинство респондентов осведомлены об основных техниках мошенничества в Интернете, а со многими видами мошенничества им приходилось сталкиваться.

Чаще всего респонденты сталкивались с Интернет-мошенничеством в электронных социальных сетях (73%), в сообщениях, посылаемых на электронную почту (73%), через переписку в клиентах мгновенного обмена сообщениями (61%), на сайтах с интересующей респондента тематикой (39%) (Таблица 3.2.8).

Сообщения мошенником в большинстве случаев адресовалось пользователям лично, но без указания их фамилии (Таблица 3.2.9). К 42% респондентов мошенники обращались лично с указанием имени. В целом можно сказать, что чаще всего мошенники пытаются осуществить акт мошенничества, используя такие коммуникативные каналы, через которые они могут обратиться в личной форме к конкретному пользователю.

Среди респондентов, которые сталкивались с мошенничеством в Интернете, выделились ***группы пользователей, различающиеся по опыту столкновения с Интернет-мошенничеством*** (Таблица 3.2.10).

Первую группу составляют респонденты, которые попадались на обман мошенников (21% к числу ответивших).

Вторая группа респондентов – это те пользовали Интернета, которым было адресовано сообщение мошенников, но они вовремя поняли, что это действия мошенников, и не среагировали на сообщение (60% к числу ответивших).

Третью группу составляют респонденты, которые не попадались на обман Интернет-мошенников (19% к числу ответивших).

Мы пытались определить, почему некоторым пользователям удалось избежать обмана мошенником (Таблица 3.2.11). Большинство пользователей утверждают, что они не попадаются на обман, поскольку критически оценивают все сайты/сообщения/предложения в Интернете (70% ответивших). Большинство респондентов также отмечают, что причиной является опыт и пример других людей, которые стали жертвой мошенничества (54% ответивших). Также можно выделить такие причины, как знание основных техник и способов мошенничества (46% ответивших), количество лет работы в Интернете (35% ответивших), навыки работы с основными возможностями Интернета (28% ответивших).

Среди техник, которые использовались по отношению к респондентам, самым популярным ответом оказался спам (89% ответивших) (Таблица 3.2.12). Также к большей части респондентов мошенники использовали такие техники, как поддельные письма или сообщения по ICQ (76%), фишинг-техники в виде рекламы товаров или услуг (71%), поддельные письма или сообщения по ICQ (61%), фальшивые извещения о выигрыше в лотерею (58% ответивших). Реже всего среди ответов встречались такие техники, как мошеннические Интернет-банки (4% ответивших) и скамерство (5%).

Большинство респондентов отметили, что не знали мошенников лично (90% ответивших) и не имели с ними виртуального знакомства (88% ответивших) (Таблицы 3.2.13 и 3.2.14). Только 5% респондентов отметили, что знали мошенников лично, и 8% респондентов знали мошенников виртуально.

Нам необходимо было выяснить, какие потери понесли пользователи, столкнувшиеся с мошенничеством. По таблице 3.2.15 можно увидеть, что большинство респондентов не понесли никаких потерь (64% ответивших). Около трети респондентов понесли моральные потери (29% ответивших). В меньшей степени респонденты понесли материальные потери (13%). Также несколько респондентов написали, что единственное, что они потеряли в результате мошенничества – это время, затраченное на устранение последствий мошенничества (восстановление нормальной работы компьютера после атаки мошенников).

Мы выяснили, что некоторые пользователи попадались на обман мошенников не один раз (Таблица 3.2.16). Один раз становились жертвами мошенников около половины респондентов (48% ответивших). От 2-4-х раз на мошенничество попадались 40% респондентов, а 12% респондентов становились жертвой более 4-х раз. Таким образом, мы делаем вывод, что большинство респондентов попадались на обман мошенников по нескольку раз.

Нам необходимо было выяснить, как ощущал себя респондент, когда оказался обманутым мошенниками в первый раз. По ответам респондентов в таблице 3.2.17 мы видим, что, попавшись в первый раз на мошенничество, 38% респондентов ощущали расстройство и разочарование, 25% респондентов испытывали злость. 24% респондентов отнеслись к произошедшему спокойно, и 12% ответивших отнеслись к мошенничеству с юмором. Один респондент сообщил, что в целом для него ситуация мошенничества оказалось полезна, поскольку его компьютер оказался заблокирован, и ему пришлось вспоминать и пробовать разные способы, чтобы вернуть компьютер в рабочее состояние.

Можно сделать вывод, что попавшись в первый раз на мошенничество, не всегда пользователи испытывают негативные чувства. Некоторые пользователи относятся к этому спокойно, кто-то даже с юмором, а кто-то приобретает в данной ситуации полезный опыт.

Теперь обратимся к проверке исследовательских гипотез.

Для установления связи признаков мы использовали коэффициенты связи: критерий хи-квадрат; коэффициент лямбда Л. Гутмана; коэффициент Гудмэна-Краскэла; однофакторный дисперсионный анализ; дисперсионный анализ Краскэла-Уоллиса; факторный анализ.

Гипотеза 1: Частота попаданий в число жертв Интернет-мошенничества зависит от опыта пользования сетью Интернет

Для определения опытности респондента в пользовании Интернетом мы используем следующие переменные:

- «Сколько свободного времени в день респондент тратит на работу в Интернете»;
- «Насколько опытным пользователем Интернета считает себя респондент»;
- «Сколько лет респондент пользуется Интернетом».

Мы предполагали, что чем больше времени респондент ежедневно проводит в Интернете, тем более он осведомлен в данном пространстве, поэтому он меньше попадался на обман мошенников.

Наибольший процент ответивших респондентов (44%) проводят ежедневно в Интернете от 4-6 часов. 36% респондентов тратят на работу в Интернете 1-3 часов (Таблица 3.2.18). Среди всех групп респондентов, отметивших, что им приходилось попадаться на обман мошенников, чуть больше половины (52%) респондентов приходится на группу, проводящую в Интернете 4-6 часов. Однако в целом можно отметить, что процентное соотношение тех респондентов, кто попался на мошенничество, кто сумел его вовремя избежать, и кто никогда не попадался на него, во всех группах респондентов примерно одинаковое.

По критерию хи-квадрат, а также по коэффициентам лямбда, Гудмэна-Краскэла мы делаем вывод, что частота попаданий на обман мошенников не зависит от количества времени, которое респондент проводит в день в Интернете (Таблицы 3.2.19 и 3.2.20).

Мы предполагали, что более опытные пользователи, владеющие многими функциями Интернета, меньше попадались на мошенничества, чем менее опытные пользователи. Среди всех групп пользователей Интернета наибольший процент респондентов (94%), не попадавших на обман мошенников, принадлежит к группе, оценивших себя как экспертов в области Интернета (Таблица 3.2.21). Однако как группа экспертов, так и группа пользователей-«чайников» (те пользователи, которые могут пользоваться лишь отдельными функциями Интернета самостоятельно) оказались довольно малочисленными. Если выделить группу Интернет-пользователей, респонденты которой больше всех попадались на обман, то в данном случае такой группой являются пользователи-«чайники». Однако в результате проверки связи признаков по критериям хи-квадрат, коэффициентам лямбда, Гудмэна-Краскэла,

выяснилось, что частота попаданий в число жертв мошенников не зависит от переменной «Насколько опытным пользователем Интернета считает себя респондент» (Таблицы 3.2.22 и 3.2.23).

Мы пытались определить зависимость между тем, сколько лет респонденты пользовались Интернетом и тем, попадались ли они на мошенничества или нет. Таблица сопряженности данных признаков показала, что респонденты, которые пользуются Интернетом 1-5 лет, попадались на обман мошенников чуть больше в процентном соотношении (28%), чем более давние пользователи Интернета (20% и 21%) (Таблица 3.2.24). Однако группа респондентов - «новичков» оказалась наименее наполненной, поэтому четких выводов по данной таблице сделать нельзя. По результатам хи-квадрат, а также коэффициентов лямбда, Гудмана-Краскэла связи данных признаков практически не наблюдается (Таблицы 3.2.25 и 3.2.26).

Среди причин, по которым пользователи попадались на обман мошенников, чаще всего респонденты отмечали, что они оказывались обманутыми по невнимательности (75% ответивших), из-за излишней доверчивости (37% ответивших), из-за отсутствия опыта попадания на обман мошенников (27% ответивших), а также из-за некритической оценки Интернет-ресурсов (23%) (Таблица 3.2.27). Пользователи в меньшей степени считают, что попались на обман мошенников по причине небольшого количества лет работы в Интернете (14% ответивших), из-за недостатка навыков работы с различными возможностями Интернета (14% ответивших) и по причине незнания основных техник мошенничества (13%) .

В результате, мы отвергаем гипотезу о том, частота попаданий в число жертв Интернет-мошенничества зависит от опыта пользования сетью Интернет. Мы отметили лишь слабую зависимость: респонденты, которые пользуются Интернетом много лет, меньше попадались на обман мошенников.

Гипотеза 2. Частота попаданий в число жертв Интернет-мошенничества зависит от знаний основных техник мошенничества и опыта столкновения с ними

Мы выяснили при помощи критерия хи-квадрат, а также коэффициента Гудмэна-Краскэла, что существует зависимость между частотой попаданий в число жертв Интернет-мошенничества и количеством техник мошенничества, которые знает респондент (Таблицы 3.2.29 и 3.2.30). Всего в нашем опросе было перечислено 22 техники мошенничества. По данным таблицы сопряженности меньше всего на обман мошенников попадались респонденты, которые знают более 15 видов мошенничества (13%) (Таблица 3.2.28). Но в тоже время самый большой процент обманутых в соотношении с другими ответами приходится на тех респондентов, кто знает 11-15 видов мошенничества (29%). Однако в таком распределении ответов мы не видим ничего необычного: чем больше респондент сталкивался с мошенничествами, тем больше у него было возможностей попасться на обман. Тем более респондент мог приобрести знание о технике мошенничества уже после того, как попался на него. В целом, можно резюмировать, что существует зависимость между тем, сколько техник мошенничества знает и со сколькими сталкивался респондент, и тем, попадался он на обман мошенников или нет. Поэтому делаем вывод, что наша гипотеза подтвердилась.

Гипотеза 3: Частота попаданий в число жертв Интернет-мошенничества зависит от возраста Интернет-пользователя

Критерий хи-квадрат, коэффициенты лямбда, Гудмэна-Краскэла показали нам, что нет зависимости между тем, оказывался ли респондент обманутым мошенниками, и его возрастом (Таблицы 3.2.32 и 3.2.33). Поэтому мы делаем вывод, что частота попаданий в число жертв Интернет-мошенничества не зависит от возраста Интернет-пользователя.

Гипотеза 4: Попавшись на мошенничество, Интернет-пользователи не пытаются предпринять действия, чтобы привлечь мошенников к ответственности

Мы выделили категории пользователей в зависимости от типа ответных реакций на мошенничество:

- пользователи, обратившиеся в правоохранительные органы по поводу совершенного мошенничества;
- пользователи, обратившиеся в другие места по поводу совершенного мошенничества;
- пользователи, ничего не предпринимавшие после совершенного мошенничества.

Среди респондентов, которые попались на обман мошенничества, лишь 1% ответивших обратились в правоохранительные органы по поводу совершенного мошенничества (Таблица 3.2.34). При этом правоохранительным органам не удалось привлечь мошенников к ответственности по данному делу (Таблица 3.2.35).

Однако 7 респондентов сообщили, что они обращались в другие места, чтобы привлечь к ответственности мошенников (Таблица 3.2.36). Респонденты обращались в банк, где была скомпрометирована кредитная карта; к друзьям; к администрации игрового сервера, где произошло мошенничество; в адвокатскую фирму; к телефонному оператору, с номера которого мошенники вымогали деньги. Из 7 респондентов 5-и (71% ответивших) пользователям удалось привлечь мошенников к ответственности, а 2-м респондентам (29% ответивших) не удалось этого сделать (Таблица 3.2.37).

Мы выяснили, почему подавляющее большинство респондентов никуда не обращались по вопросу совершенного мошенничества (Таблица 3.2.39). 43% респондентов ответили, что не верили в возможности правоохранительных органов раскрыть преступление; 36% ответили, что не желали иметь дело с формальными уголовно-процессуальными отношениями, 35% ответивших не знали, куда обращаться по делу совершенного мошенничества.

Таким образом, наша гипотеза частично подтвердилась, частично нет. Большинство пользователей не пытались привлечь мошенников к ответственности. Однако есть малая доля респондентов, которые предпринимали действия, чтобы вернуть потерянное имущество или наказать мошенников. Среди данной группы пользователей практически никто из ответивших не прибегал к помощи правоохранительных органов, используя иные способы и каналы помощи: личные знакомства, локальные органы контроля в том коммуникативном пространстве, где произошло мошенничество; адвокатские конторы.

Гипотеза 5: Отношение к Интернет-мошенничеству зависит от возраста Интернет-пользователя

Чтобы выяснить типы отношений пользователей Рунета к Интернет-мошенничеству, мы провели факторный анализ, включив в факторную модель 10 переменных-суждений, выражающих различное отношение к данному феномену. Коэффициент Кайзера—Мейера—Олкина и тест сферичности Бартлетта показали адекватность применения факторного анализа в данном случае (Таблица 3.2.40). В результате мы получили 3 фактора-переменных, каждый из которых представляет собой особый тип отношения к феномену Интернет-мошенничества как явлению Рунета (Таблица 3.2.44). Мы назвали факторы следующим образом:

- Негативное отношение к Интернет-мошенничеству и мошенникам;
- Отношение к Интернет-мошенничеству как к ситуации, в которой виноват пользователь;
- Отношение к мошенничеству как нормальному явлению.

Далее мы провели дисперсионный анализ, чтобы определить, влияет ли возраст респондента на его отношение к Интернет-мошенничеству (Таблица 3.2.45). В результате мы определили, что существует связь между негативным отношением к Интернет-мошенничеству и возрастом респондента.

В целом дисперсионный анализ позволяет лишь фиксировать наличие-отсутствие связи между переменными, однако возможно проанализировать некоторое направление данной связи. Мы попробовали проанализировать направления выявленных зависимостей при помощи дисперсионного анализа Краскэла-Уоллиса.

Так как нашу факторную переменную мы ранжировали, то, соответственно, более высокий ранг соответствует более ярко выраженному негативному отношению к Интернет-мошенничеству. Мы пытались определить, у какой возрастной группы в среднем более негативное отношение к Интернет-мошенничеству. Выяснилось, что в среднем наиболее негативно к Интернет-мошенничеству относятся пользователи Рунета в возрасте 18-25 лет (Таблица 3.2.46). А наименее ярко выраженная негативная оценка Интернет-мошенничества в среднем у пользователей старше 35 лет.

Таким образом, мы можем сказать, что гипотеза подтвердилась. Мы обнаружили, что негативное отношение пользователя к Интернет-мошенничеству зависит от его возраста.

Гипотеза 6: Отношение к Интернет-мошенничеству зависит от того, сколько раз пользователь Интернета попадался на мошенничество

Мы провели дисперсионный анализ с использованием факторных переменных, отражающих 3 типа отношения респондентов к Интернет-мошенничеству, а также с использованием группирующей переменной «Сколько раз пользователь попадался на Интернет-мошенничество», представленной в интервалах. По результатам дисперсионного анализа выяснилось, что количество раз попадания на обман мошенников влияет на отношение к Интернет-мошенничеству как ситуации, в которой виноват сам пользователь (Таблица 3.2.48).

Напомним, что переменную «Сколько раз пользователь попадался на Интернет-мошенничество» мы представили в интервалах. При помощи дисперсионного анализа

Краскэла-Уоллиса мы пытались определить, в каком интервале в среднем наиболее сильно выражено отношение к мошенничеству как к ситуации, в которой виноват сам пользователь. Выяснилось, что в среднем больше всего видят вину пользователей в ситуации мошенничества респонденты, попадавшиеся на мошенничества 2-4 раза (Таблица 3.2.49).

Делаем вывод, что наша гипотеза подтвердилась. Мы выяснили, что отношение респондентов к Интернет-мошенничеству как к ситуации, в которой виноват пользователь, зависит от того, сколько раз респонденты попадались на мошенничество.

Гипотеза 7: Большинство Интернет-пользователей в ситуации мошенничества обвиняют мошенников, которые обманули пользователя

Мы выяснили у респондентов, кто, на их взгляд, виноват в ситуации мошенничества. Вопрос в анкете был задан, в первый раз, для всего массива респондентов, чтобы узнать мнение респондентом о том, кто виноват в ситуации мошенничества в целом. Во второй раз вопрос задавался только тем респондентам, которые попадались на обман мошенников.

В первом случае почти половина респондентов (47% ответивших) посчитали, что в ситуации мошенничества виноват сам пользователь (Таблица 3.2.51). 31% респондентов посчитали виновными Интернет-мошенников, и лишь 8% обвинили правоохранительные органы.

Во втором случае, когда тот же вопрос задавался пользователям, попавшимся на мошенничество, распределение ответов оказалось примерно таким же (Таблица 3.2.52). Половина «обманутых» респондентов (51%) посчитали, что они сами виноваты в ситуации мошенничества. Респондентов, обвинивших Интернет-мошенников, оказалось 40% от числа ответивших. И 9% респондента посчитали, что виноваты в ситуации оказались правоохранительные органы.

Таким образом, наша гипотеза частично подтверждается, частично отвергается. Пользователи обвиняют в ситуации мошенничества как мошенников, так и самих пользователей Сети. Причем пользователей Сети респонденты обвиняют больше, чем мошенников.

ЗАКЛЮЧЕНИЕ

Интернет-мошенничество – это явление, проникшее из реального мира в мир виртуальный. Мошенничество в Интернете по определению идентично мошенничеству из реального мира: это хищение чужого имущества или приобретение права на чужое имущество путем обмана или злоупотребления доверием. Однако Интернет-мошенничество подчиняется законам виртуального пространства: режиму «Интернет-времени», физической удаленности пользователей друг от друга, анонимности пользователей в Сети. Благодаря данным свойствам, привлечь к ответственности мошенников оказывается весьма затруднительно.

В нашей работе мы рассматривали Интернет-мошенничество как элемент коммуникативного пространства Интернета. Интернет-мошенники используют все возможные каналы коммуникации в Интернете, чтобы найти потенциальных жертв. Сами сообщения мошенников являются формами коммуникации между ними и пользователями Интернета.

Проанализировав сообщения мошенников, а также информационную базу, касающуюся мошенничества в Интернете, мы выделили типологии Интернет-мошенничества: по методике исполнения, по каналам коммуникации, по сфере воздействия, по коммуникативным средствам, по степени оказываемого психологического давления

По результатам эмпирического исследования мы выяснили, что большинство пользователей Рунета осведомлены об основных техниках мошенничества, а также встречались с ними во время работы в Интернете. Мы доказали, что частота попадания в число жертв Интернет-мошенников зависит от количества техник мошенничества, которые знает пользователь Интернета.

Типовыми мошенническими техниками, с которыми встречалось большинство пользователей, являются: спам, SMS-оплата или SMS-голосования, фальшивые извещениями о выигрыше в лотерею, фишинг-мошенничества форме рекламы товаров и услуг.

Мы выделили несколько категорий пользователей в зависимости от различий в опыте столкновения с Интернет-мошенничеством:

- пользователи, которые никогда не попадались на обман мошенников;
- пользователи, которым мошенники адресовали сообщение, но они сумели вовремя предотвратить акт мошенничества по отношению к ним;
- пользователи, которые попадались на обман мошенничество.

Большинство респондентов относятся ко второй категории пользователей.

В ситуации мошенничества пользователи обвиняют как мошенников, так и самих себя – пользователей Интернета. Оказавшись обманутыми мошенниками, большинство пользователей не пытаются предпринять действия, чтобы привлечь мошенников к ответственности. Пассивность поведения респондентов объясняется неверием в возможности правоохранительных органов раскрыть преступление, нежеланием иметь дело с формальными уголовно-процессуальными отношениями, а также незнанием, куда обращаться по делу совершенного мошенничества.

Среди малой доли респондентов, которые предпринимают действия, чтобы вернуть потерянное имущество или наказать мошенников, никто не прибегает к помощи правоохранительных органов. Пользователи используют иные способы и каналы помощи: личные знакомства, локальные органы контроля в том коммуникативном пространстве, где произошло мошенничество; адвокатские конторы.

Наблюдается 3 типа отношений к Интернет-мошенничеству в Рунете:

- негативное отношение к Интернет-мошенничеству и мошенникам;
- отношение к Интернет-мошенничеству как к ситуации, в которой виноват пользователь;
- отношение к мошенничеству как нормальному явлению.

Мы выяснили, что отношение респондентов к Интернет-мошенничеству как к ситуации, в которой виноват пользователь, зависит от того, сколько раз респонденты попадались на мошенничество. Также существует связь между негативным отношением пользователя к Интернет-мошенничеству и его возрастом.

Полученная в результате исследования информация дает комплексное представление о феномене Интернет мошенничества как элемента коммуникативного пространства Рунета. Интернет-мошенничество – это не негативный феномен, а нормальное явление, которое учит пользователя быть внимательным во время работы в Интернете.

В заключение работы дадим несколько практических рекомендаций. Мы бы посоветовали пользователям расширять знания касательно возможностей Интернета, а главное, *особенностей виртуального пространства*, в силу которых неосведомленный пользователь оказывается уязвимым перед мошенниками. Необходимо создавать веб-сайты, посвященные информированию пользователей Рунета об основных техниках мошенничества. Информация того же рода должна освещаться в СМИ.

Главная причина широкого распространения мошенничества в Интернете – это безнаказанность мошенников. Правоохранительным органам необходимо законодательно урегулировать меры ответственности за виртуальное мошенничество, вводить больше органов по контролю за безопасностью в Интернете и *практиковать наказания Интернет-мошенников.*

БИБЛИОГРАФИЯ

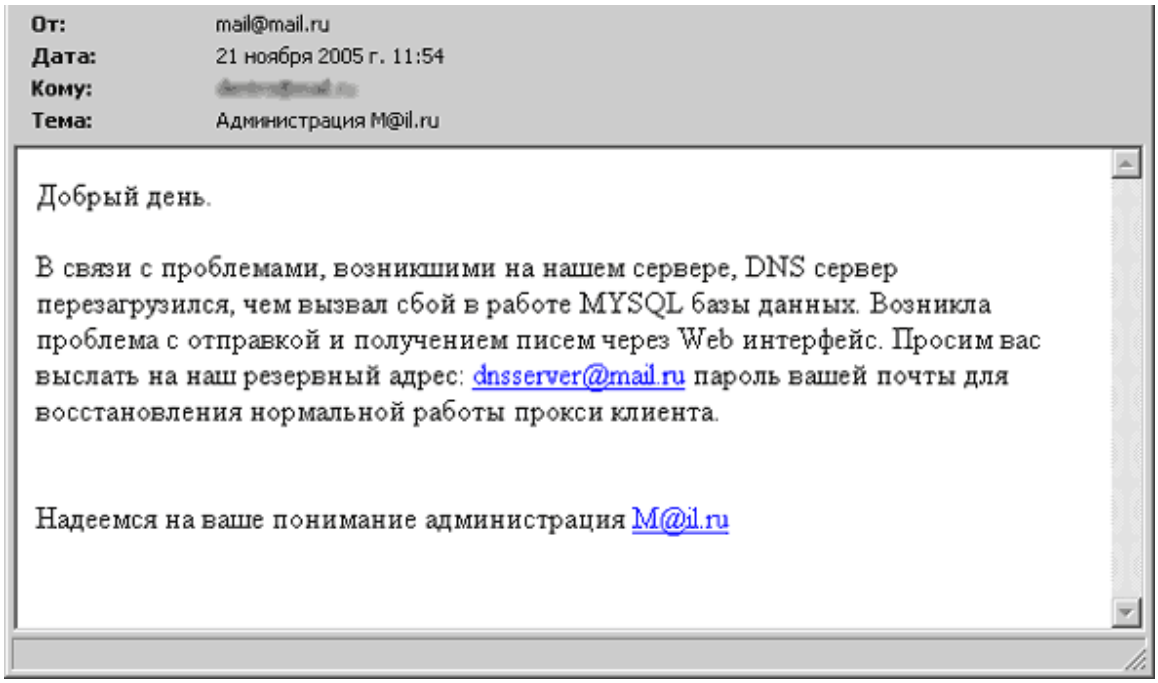
1. *Адамьянц Т.З.* Особенности и тенденции современных коммуникационных процессов [Электронный ресурс]. – Режим доступа: http://lib.socio.msu.ru/l/library?e=d-000-00---0kongress--00-0-0-0prompt-10---4------0-1l--1-ru-50---20-about---00031-001-1-0windowsZz-125100&a=d&c=kongress&cl=CL1&d=HASH0122c16e30498d4f56a24080
2. *Адамьянц Т.З.* К диалогической телекоммуникации: от воздействия к взаимодействию. М., 1999 [Электронный ресурс]. - Режим доступа: http://business.fortunecity.com/geffen/407/ogl.htmhttp://future.museum.ru/link.asp?back=part06/060403.htm&url=http://business.fortunecity.com/geffen/407/ogl.htm
3. Актуальные проблемы теории коммуникации/Санкт-Петербург: Изд-во СПбГПУ, 2004, 362 с.
4. Анатомия общения: Учебное пособие. СПб.: Изд-во Михайлова В. А., 1999.
5. *Андреева Г. М.* Социальная психология. Учебник для высших учебных заведений. М.: Аспект Пресс, 1999.
6. *Белл Д.* Социальные рамки информационного общества// Новая технократическая волна на Западе/ Под ред. П.С. Гуревича. М., 1998.
7. *Бодрияр Ж.* Символический обмен и смерть. М. 2000.
8. *Гидденс Э.* Социология / Пер. с англ.; науч. ред. В. А. Ядов; общ. ред. Л. С. Гурьевой, Л. Н. Посилевича. — М.: Эдиториал УРСС, 1999.
9. *Глазычев В. Л.* Проблема «массовой культуры» // журнал «Вопросы философии», 1970. № 12.
10. *Девятко И.Ф.* Методы социологического исследования. - Екатеринбург: Изд-во Урал.ун-та, 1998.
11. *Доценко Е. Л.* Психология манипуляции: феномены, механизмы и защита. М.: ЧеРо, Издательство МГУ, 1997.
12. *Дридзе Т.М.* Текстовая деятельность в структуре социальной коммуникации. М.,1984 [Электронный ресурс]. – Режим доступа: http://www.isras.ru/?page=activity&sub=pubs&pubid=704
13. *Ермолаев А.* Выборочный метод в социологии. Методическое пособие. Москва 2000.
14. *Журавлева Е. Ю.* Основные категории пользователей среды сети Интернет/Интернет-конференция «Социология и Интернет: перспективные направления исследования», 2004-2005.
15. *Залесский П.* Интернет: российская аудитория в анфас и в профиль // Медиа-альманах. 2000. № 7-8.
16. *Иванов Д.В.* Виртуализация общества. СПб.: "Петербургское Востоковедение", 2000. - 96 с.
17. История теоретической социологии. В 4-х т. Т. 4/ Отв. Ред. Ю.Н. Давыдов. М.:«Канон+» ИО «Реабилитация», 2002.
18. *Кара-Мурза С.* Манипуляция сознанием. М.: Эксмо «Алгоритм», 2004.
19. *Кастельс М.* Информационная эпоха: экономика, общество и культура / Пер. с англ. под науч. ред. О. И. Шкаратана. — М.: ГУ ВШЭ, 2000. — 608 с.
20. *Кастельс М.* Становление общества сетевых структур// "Новая постиндустриальная волна на Западе. Антология" (под ред. В.Л. Иноземцева). М., 1999.
21. *Конецкая В.П.* Социология коммуникации. Москва: Международный университет Бизнеса и Управления, 1997 [Электронный ресурс]. – Режим доступа: http://lib.socio.msu.ru

22. *Корытникова Н.В.* Интернет как средство производства сетевых коммуникаций в условиях виртуализации общества//Социологические исследования. 2007. № 2. С. 85-93.
23. *Корытникова Н. В.* Интернет-зависимость и депривация в результате виртуальных взаимодействий//Социологические исследования. 2010. № 6. С. 70-79.
24. *Крыштановский А.О.* «Анализ социологических данных с помощью пакета SPSS». Издательский дом: «ГУ-ВШЭ», 2003.
25. Мошенничество. Статья 159 Уголовного кодекса РФ/ Большой юридический словарь. 3-е изд., доп. и перераб. / Под ред. проф. А. Я. Сухарева. — М.: ИНФРА-М, 2007. [Электронный ресурс]: Яндекс. Словари. - Режим доступа: http://slovari.yandex.ru/dict/jurid
26. *Омельченко. Е.* Поколение Text: новые имена молодежной культуры [Электронный ресурс]. – Режим доступа: http://www.regioncentre.ru/resources/articles/article15/
27. *Семенова В.В.* «Качественные методы: введение в гуманистическую социологию». М.,Добросвет, 1998.
28. *Силаева В.Л.* Интернет как социальный феномен // Социологические исследования. 2008. № 11. С. 101-107.
29. *Силаева В.Л.* Об использовании понятия «виртуальный» // Социологические исследования. 2010. № 8. С. 19-35.
30. *Силаева В.Л.* Подмена реальности как социокультурный механизм виртуализации общества [Диссертация] М.,2004. – Режим доступа: http://ecsocman.edu.ru/data/870/521/1219/DisserSilaeva.pdf
31. Современные коммуникативные технологии и личность: столкновение массового и индивидуального / Отв. Ред. В.А. Шилова. Москва: типография «Маска», 2009.
32. *Татарова Г.Г.* Методология анализа данных в социологии.Учебное пособие для вузов. Москва: Издательский дом «Стратегия», 1998.
33. *Толстова. Ю. Н.* Анализ социологических данных (Методология, дескриптивная статистика, изучение связей между номинальными признаками). Москва: Научный мир, 2000.
34. *Толстова. Ю. Н.* Измерение в социологии. Москва: Инфра-М, 1998.
35. *Тоффлер Э.* Третья волна. - М.: ООО «Издательство АСТ», 1999. - С. 276-277.
36. *Фурс В.Н.* Философия незавершенного модерна Юргена Хабермаса. Мн.: ЗАО «Экономпресс», 2000.
37. *Хилл С., Тернер Б.С., Аберкромби Н.* Социологический словарь/ Под ред. С.А. Ерофеева. Москва: Экономика, 2004.
38. *Чуриков А.* Случайные и неслучайные выборки в социологических исследованиях//Социальная реальность.2007.№4.
39. *Шиллер Г.* Манипуляторы сознанием. М: Мысль, 1980.
40. Зайцев О. Мошенничество в Интернете и защита от него//КомпьютерПресс. 2007.№ 7. [Электронный ресурс]: Электронный журнал «КомпьютерПресс: тестирование, безопасность, программное обеспечение, обзоры, уроки, обучение. – Режим доступа: http://www.compress.ru/article.aspx?id=18184&iid=842
41. Как удалить баннер из системы?/Электронный портал «No secrets»[Электронный ресурс]. – Режим доступа: http://notsecret.ru/komp/kompsecret/page/2/
42. Лохотрон, Интернет, мошенничество, кидалово в Интернет / Интернет работа – заработок Интернете, созадние сайтов, SEO, блоггинг. [Электронный ресурс]: Блог о заработке в Интернете, создании сайтов, SEO и блоггинге. – Режим доступа: http://blogwork.ru/loxotron-internet-moshennichestvo-kidalovo-v-internet/
43. Мошенничество в Интернете/ Государственные Департамент США [Электронный ресурс]: На сайте содержится информация о текущей внешней политике и жизни в

Соединенных Штатах Америки. – Режим доступа: http://www.infousa.ru/information/internet_fraud.htm .
44. Мошенничество/ Википедия. Свободная энциклопедия [Электронный ресурс]. – Режим доступа: http://ru.wikipedia.org/wiki/Мошенничество
45. Мошенничество в Интернете/ Сайт МВД: структура Министерства. [Электронный ресурс]. – Режим доступа: http://www.mvd.ru/struct/10000220/10000287/10000321/
46. Мошенничество в Интернете: перспективы привлечения к ответственности [Электронный ресурс]: юридические консультации, услуги. Юридическая фирма Вадима Колосова. – Режим доступа: http://www.kolosov.info/kommentarii/moshennichestvo-v-internete
47. Мошенничества в Интернете/ Викиучебник [Электронный ресурс]: портал образовательная литература. - Режим доступа: http://ru.wikibooks.org/wiki/Мошенничество в Интернете (по состоянию на 24.05.2011 г.
48. Мошенничество: как заработать денег в Интернете. Волшебные кошельки (умножители денег) [Электронный ресурс]. – Режим доступа: http://zkan.com.ua/main/dtp/292-internet-moshennichestvo-volshebnye-koshelki.html
49. Письма в спаме (письма радости) [Электронный ресурс]: Портал Интернет-«хитростей». – Режим доступа: http://www.shram.kiev.ua/hacker/spam.shtml
50. Спам в апреле 2010/ securelist. Com [Электронный ресурс]: информационный портал об Интернет-безопасности. – Режим доступа: http://www.securelist.com/ru/analysis/208050634/Spam_v_aprele_2010_goda
51. Что такое скамерство? (хозяйке на заметку) [Электронный ресурс]. – Режим доступа: http://www.aliveinternet.ru/post32974761
52. Парад спама/запись с тэгом ICQ в Интернет-дневнике [Электронный ресурс]. – Режим доступа: http://www.alexrus.info/showjournal.php?journalid=887204&tagid=240
53. Уголовный кодекс РФ и Мошенничество и Интернет - Интернет и безопасность/ w-security: Интернет и безопасность. [Электронный ресурс]: Ресурс посвящен Интернет-мошенничеству и борьбе с ним. – Режим доступа: http://www.w-security.ru/publ/1-1-0-19
54. Форум фан-клуба Лаборатории Касперского [Электронный ресурс] – Режим доступа: http://forum.kasperskyclub.ru/index.php
55. Форум «Антимаг.ру» - сайт рассказывает о том, как не стать жертвой обмана [Элетронный ресурс] – Режим доступа: http://forum.antimag.ru/index.php

ПРИЛОЖЕНИЯ

Приложение 1: Примеры Интернет-мошенничества



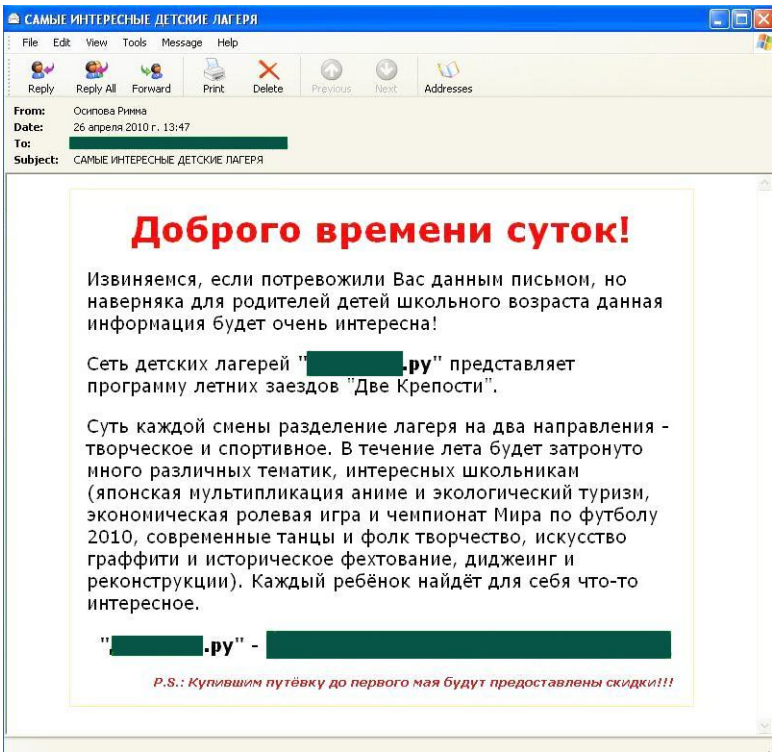
От: mail@mail.ru
Дата: 21 ноября 2005 г. 11:54
Кому: [redacted]
Тема: Администрация M@il.ru

Добрый день.

В связи с проблемами, возникшими на нашем сервере, DNS сервер перезагрузился, чем вызвал сбой в работе MYSQL базы данных. Возникла проблема с отправкой и получением писем через Web интерфейс. Просим вас выслать на наш резервный адрес: dnsserver@mail.ru пароль вашей почты для восстановления нормальной работы прокси клиента.

Надеемся на ваше понимание администрация M@il.ru

Рис. 2.3.1. Образец фишинг-письма пользователям почты Mail.ru



САМЫЕ ИНТЕРЕСНЫЕ ДЕТСКИЕ ЛАГЕРЯ

File Edit View Tools Message Help

Reply Reply All Forward Print Delete Previous Next Addresses

From: Осипова Римма
Date: 26 апреля 2010 г. 13:47
To: [redacted]
Subject: САМЫЕ ИНТЕРЕСНЫЕ ДЕТСКИЕ ЛАГЕРЯ

Доброго времени суток!

Извиняемся, если потревожили Вас данным письмом, но наверняка для родителей детей школьного возраста данная информация будет очень интересна!

Сеть детских лагерей "[redacted].ру" представляет программу летних заездов "Две Крепости".

Суть каждой смены разделение лагеря на два направления - творческое и спортивное. В течение лета будет затронуто много различных тематик, интересных школьникам (японская мультипликация аниме и экологический туризм, экономическая ролевая игра и чемпионат Мира по футболу 2010, современные танцы и фолк творчество, искусство граффити и историческое фехтование, диджеинг и реконструкции). Каждый ребёнок найдёт для себя что-то интересное.

"[redacted].ру" - [redacted]

P.S.: Купившим путёвку до первого мая будут предоставлены скидки!!!

Рис. 2.3.2. Образец фишинг-письма в виде предложения услуги

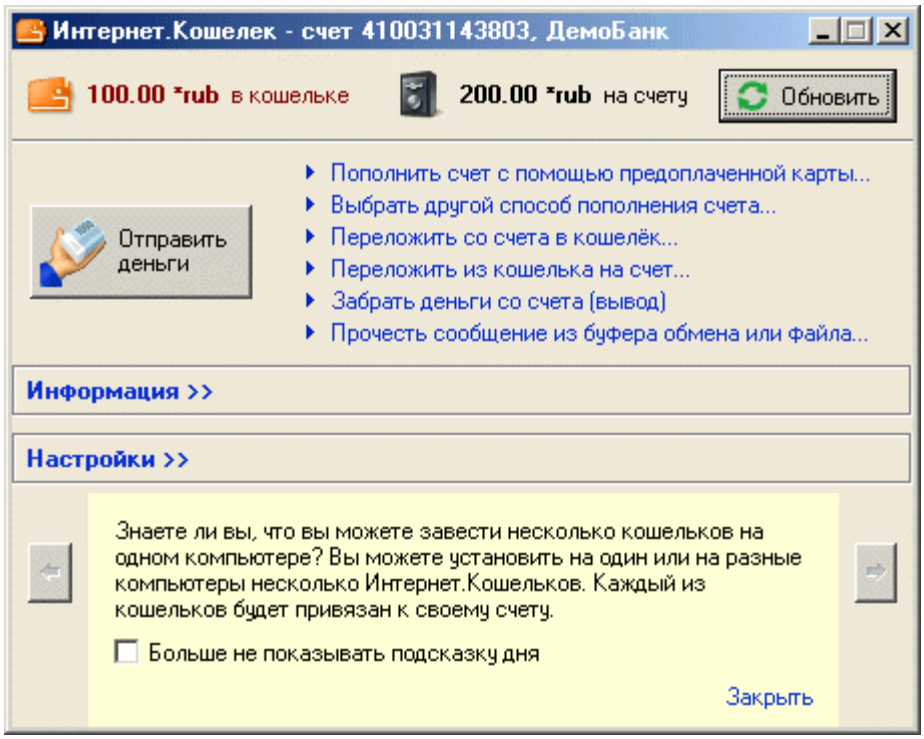


Рис. 2.3.3. Пример мошенничества по методике «Магический кошелек»

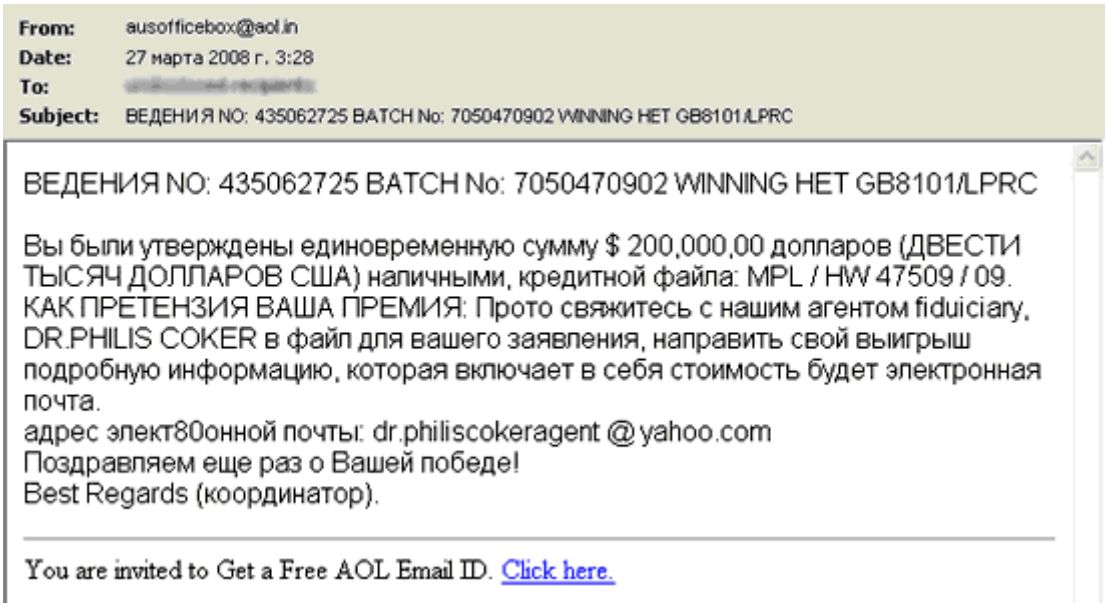


Рис. 2.3.4. Пример письма-извещения о выигрыше в лотерею

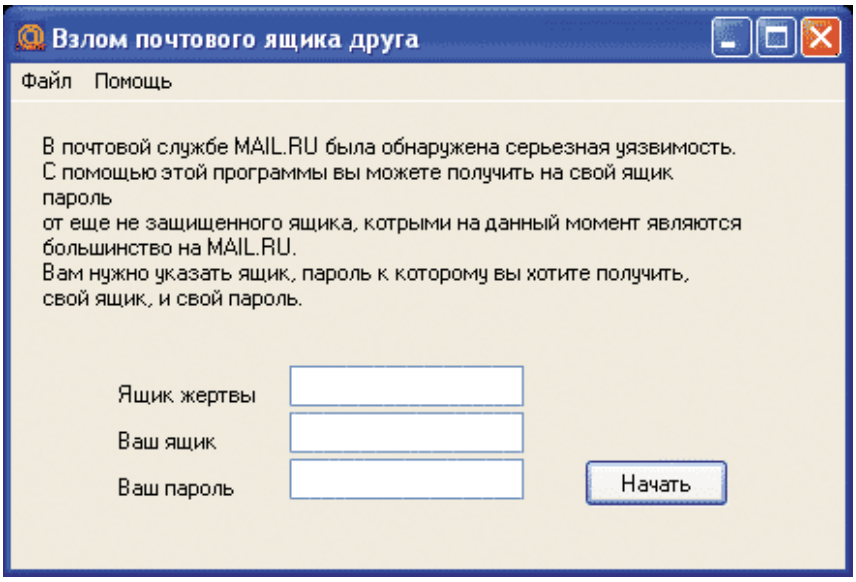


Рис. 2.3.5 . Пример программы для взлома почтовых ящиков, на самом деле отправляющая введенные данные злоумышленнику

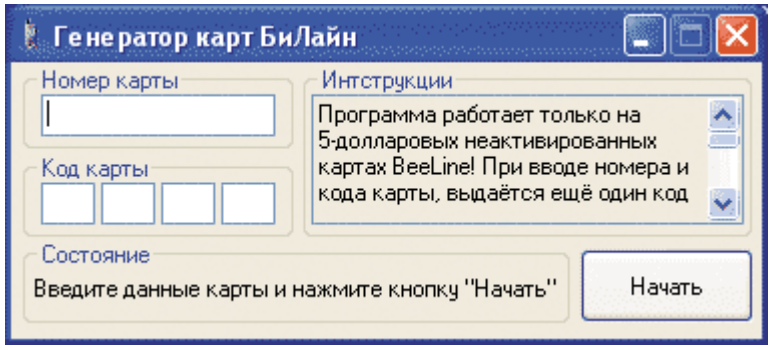


Рис 2.3.6. Пример программы для клонирования карт оплаты телефона, которая пересылает введенный код неактивированной карты злоумышленнику

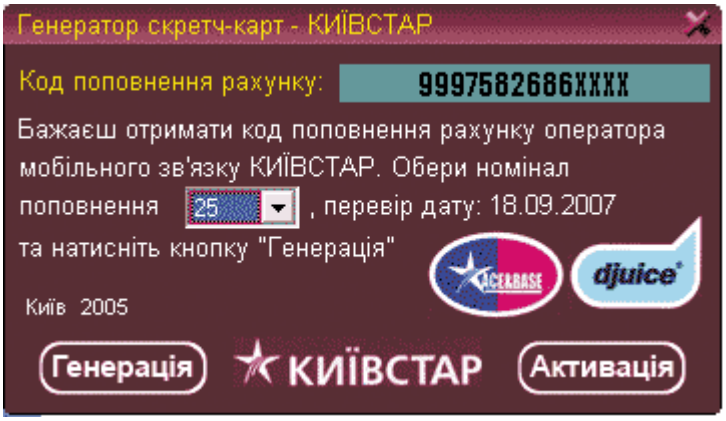


Рис. 2.3.7. Пример Hoax-программа, авторы которой обещают, что в случае покупки и активации программа будет генерировать номера карт оплаты провайдера KievStar

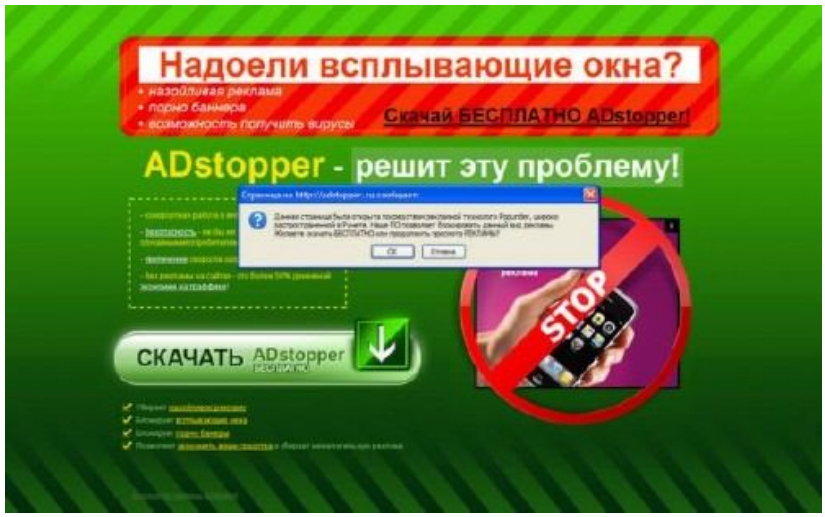


Рис. 2.3.8 Пример Hoax-программы в виде программы-антивируса

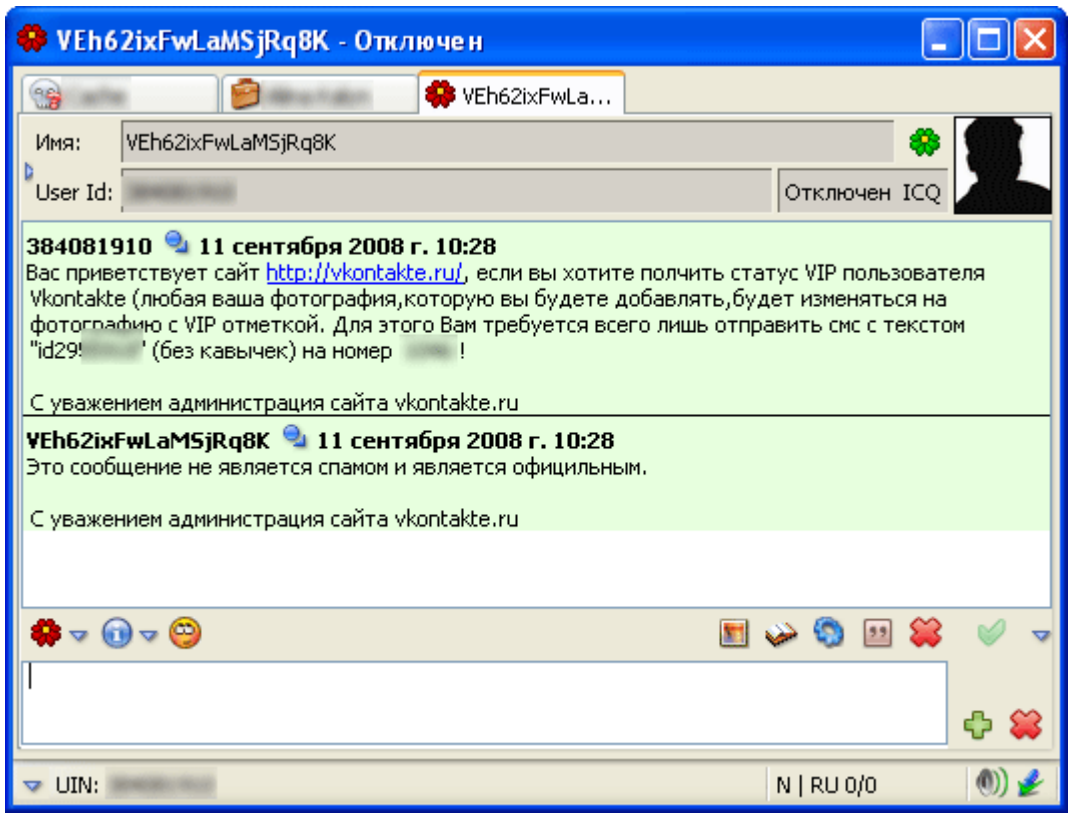


Рис. 2.3.9. Пример мошенничества посредством SMS-оплаты услуг

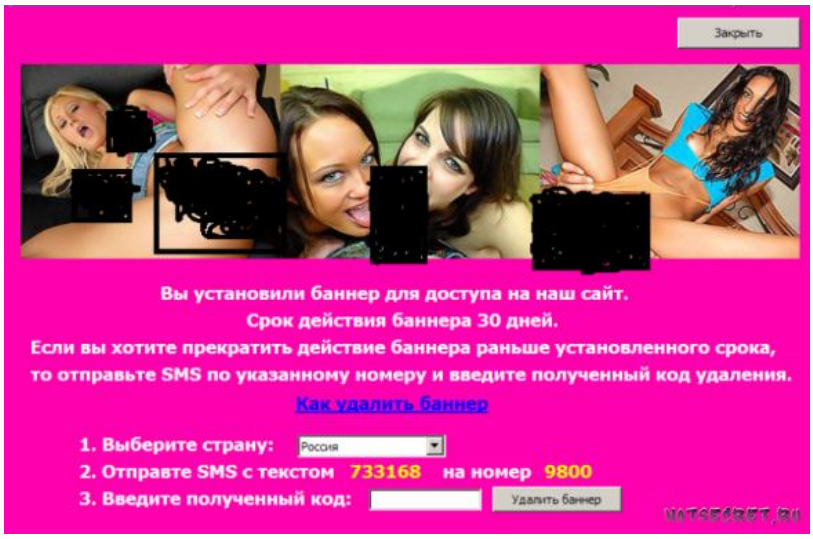


Рис. 2.3.10 . Пример взлома компьютера пользователя в виде установки баннера

«Доброго здоровья! Месяц назад к нам приблудился кот. Он был поранен злыми собаками. Кровь сочилась фонтаном из его лапок. Я выходил его и он выздоровел. Мне мама давала денег на завтрак, но я покупал еду для больного котика. За это время он стал мне единственным другом, который не предаст и не продаст. Но беда в том, что у меня брат просто живодер какой-то. Он сказал, что сдаст его на шапку. Он бил моего друга ногой, обутой в кирзовый сапог! Впрочем, он сказал, что не тронет кота, если я ему дам 100 долларов. Люди добрые, помогите! Он такой чудный и ласковый! Он пушистый, белый, с серыми подпалинами. Не будьте черствыми, я хочу верить, что справедливость на свете существует. Деньги перечислите на WMZ(R)XXXXXXX».

Рис. 2.3.11. Пример Интернет-мошенничества по сфере чувственных мотиваций

Рис. 2.3.12. Пример визуального мошенничества в виде баннера-рекламы

«Здравствуйте! Я недавно завел себе WM-кипер. Как известно, WM-идентификаторы, если за полгода там остается нулевой остаток, то WM-кипер закрывается. Я работаю со спонсорами, но не набрал еще минималку. Если мне закроют кипер, то я не получу свои деньги. Пожалуйста, вышлите на WMZ(R)XXXXXXX 1 цент (копейку). Выручите меня, прошу Вас. Я новичок, мне так трудно».

Рис. 2.3.13. Пример Интернет-мошенничества в виде текста

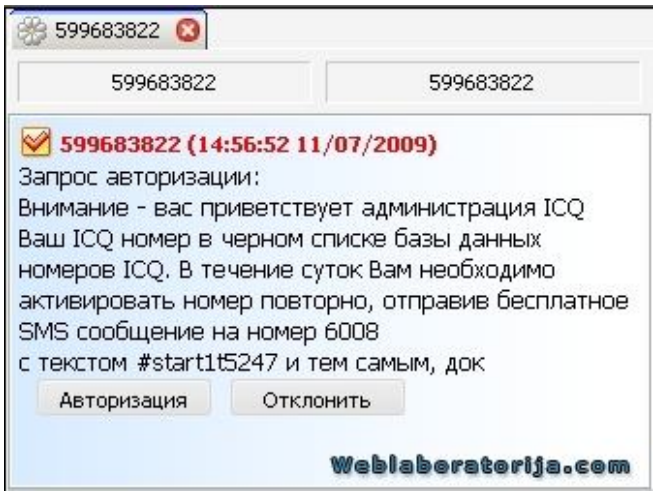


Рис. 2. 3.14. Пример Интернет-мошенничества по ICQ в форме требования

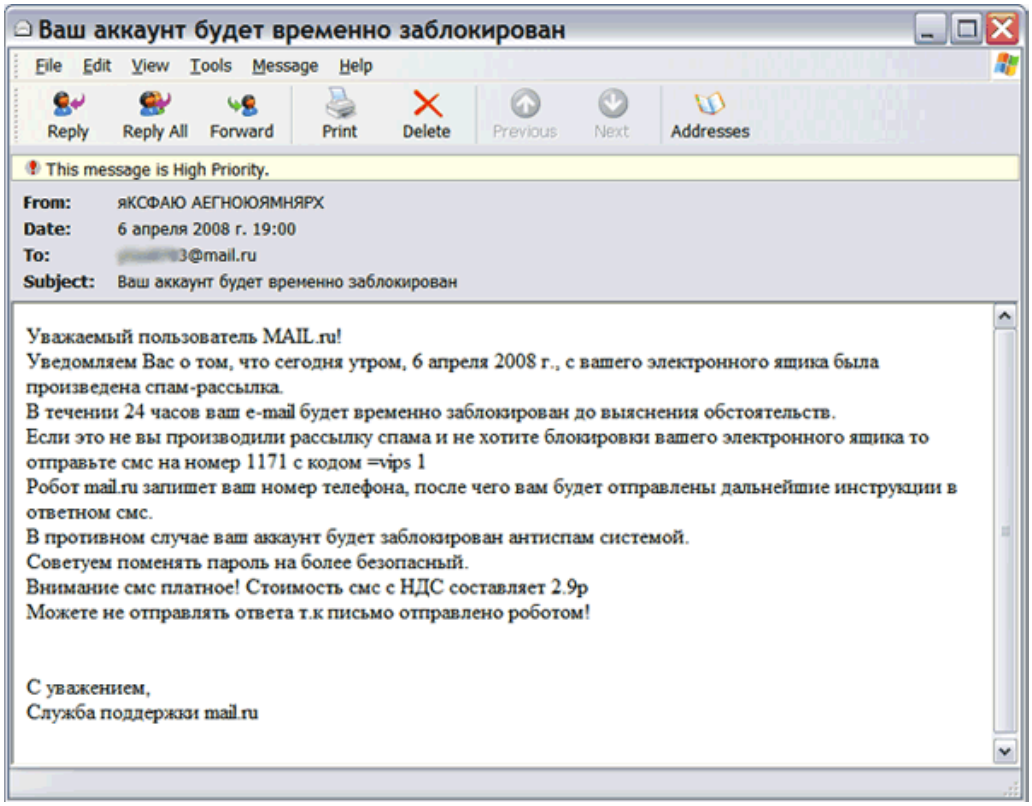


Рис. 2.3.15. Пример Интернет-мошенничества в форме угрозы

Приложение 2: Анкета к эмпирическому исследованию феномена Интернет-мошенничества

АНКЕТА

Здравствуйте, уважаемый пользователь Интернета!

Центр социологии управления и социальных технологий Института социологии РАН и Государственный академический университет гуманитарных наук проводят исследование особенностей Интернет-мошенничества.

Мошенничеством называется кража чужого имущества или приобретение права на чужое имущество путем обмана или злоупотребления доверием. Термин «мошенничество в Интернете» применим к мошенническим махинациям любого вида, совершаемых посредством социальных сетей, в чатах, на веб-сайтах, по электронной почте и по иным каналам Интернета с целью привлечения потенциальных жертв и проведения мошеннических сделок.

Мошенничество в Интернете - очень распространенное явление, и многие пользователи Интернета с ним сталкиваются. Мы будем очень признательны, если Вы как пользователь Интернета ответите на вопросы данной анкеты.

Вся информация, полученная в ходе данного исследования, носит анонимный характер. Ни при каких обстоятельствах мы не будем называть конкретных людей, участвующих в нашем исследовании. Все данные будут приводиться только в обобщенном виде.

Несколько вопросов о том, как Вы пользуетесь Интернетом

1. Вспомните, пожалуйста, в каком году Вы впервые использовали Интернет? *(Напишите в отведенной строке)*

_____ *год*

2-20. Как часто Вы пользуетесь следующими возможностями Интернета? *(Пожалуйста, отметьте только ОДИН ответ в КАЖДОЙ строке)*

№	Возможности Интернета	Пользуюсь каждый день	Пользуюсь несколько раз в неделю	Пользуюсь несколько раз в месяц	Пользуюсь реже,чем раз в месяц	Не пользуюсь	Затрудняюсь ответить
2.	просматриваю новостные ленты информационных порталов	1	2	3	4	5	9
3.	пользуюсь поисковыми системами (Яндекс, Google, Rambler и т.д.)	1	2	3	4	5	9
4.	просматриваю официальные сайты государственных учреждений и предприятий, коммерческих структур	1	2	3	4	5	9
5	покупаете товары в Интернет-магазинах	1	2	3	4	5	9
6	использую электронные платежные системы (Webmoney, Яндекс-деньги, PayPal и др.)	1	2	3	4	5	9
7	покупаю/резервирую билеты (на поезд, на самолет, на концерты, на выставки)	1	2	3	4	5	9
8	пользуюсь e-mail (электронной почтой)	1	2	3	4	5	9

9	пользуюсь Skype, QIP, ICQ, mail.ru-Агент	1	2	3	4	5	9
10	скачиваю файлы (музыку, видео, книги, фотографии и т.д.)	1	2	3	4	5	9
11	пользуюсь социальными сетями («Одноклассники», «Вконтакте», «Facebook»)	1	2	3	4	5	9
12	играю в сетевые игры (on-line игры)	1	2	3	4	5	9
13	пользуюсь системой файлообменов BitTorrent (Rutracker.ru, Torrent.ru и т.д.)	1	2	3	4	5	9
14	пользуюсь всемирной энциклопедией Wikipedia	1	2	3	4	5	9
15	пользуюсь блогами (livekournal.ru, liveinternet.ru и т.д.)	1	2	3	4	5	9
16	пользуюсь видеопорталами (YouTube, RuTube и т.д.)	1	2	3	4	5	9
17	оформляю, заполняю и отсылаю электронные формы	1	2	3	4	5	9
18	пользуюсь сайтами знакомств	1	2	3	4	5	9
19	пользуюсь форумами, чатами	1	2	3	4	5	9

20. Сколько примерно свободного времени в день в часах Вы тратите на работу в Интернете? (*Напишите в отведенной строке полное число часов. Если меньше часа, то укажите в десятых долях)*

_____

21. Оцените, пожалуйста, насколько Вы опытный пользователь Интернета? Выберите наиболее подходящий для вас ответ.

1. Я могу пользоваться Интернетом лишь с посторонней помощью
2. Я умею пользоваться отдельными функциями Интернета самостоятельно
3. Я уверенный пользователь Интернета, пользующийся многими возможностями Интернета без затруднений
4. Я продвинутый пользователь Интернета. Я свободно владею большинством возможностей Интернета, знаю принципы созданий и раскрутки веб-страниц, приложений.
5. Я эксперт в области Интернета. Я умею самостоятельно создавать веб-страницы и различные Интернет-приложения, знаю принципы взлома веб-страниц и получения доступа к информации.
6. Другое *(Напишите, что именно*)_____
7. Затрудняюсь ответить

Пожалуйста, ответьте на вопросы, затрагивающие тему мошенничества в Интернете

22-44. Существует множество форм мошенничества в Интернете по технике исполнения. Ниже детально расшифровываются отдельные техники мошенничества. Пожалуйста, прочтите и укажите, какие формы

мошенничества Вам знакомы, и какие техники встречались во время работы в Интернете. (*Отметьте только ОДИН ответ в КАЖДОЙ строке)*

Виды Интернет-мошенничества	Да, знакомо и встречалось	Да, знакомо, но не встречалось	Нет, не знакомо, и не встречалось	Затрудняюсь ответить
22. Тайпсквоттинг *-* регистрации доменных имен, отличающихся от имен раскрученных доменов опечатками или доменной зоной (например, http://www.yadex.com/**,** http://www.andex.ru/**,** www.ranbler.ru**,** www.rambdler.ru**.)**	1	2	3	9
23. Фишинг *-* выуживание конфиденциальных данных пользователя (паролей, идентификационных данных) с целью хищения денег. Создается поддельный сайт, визуально имитирующий сайт банка или иного ресурса с услугами, предполагающей идентификацию пользователя. Главная задача фишера – пользователь оставляет свои идентификационные данные. Часто реализуется следующими способами:	1	2	3	9
24.1спам — массовая рассылка информационных сообщений лицам, не выражавшим желания их получать. Часто его задача напугать пользователя некими проблемами, требующими от пользователя немедленной авторизации на указанном в письме сайте для выполнения тех или иных операций, что делает их потенциальными жертвами фишеров	1	2	3	9
25.2 реклама неких товаров или услуг, которые можно приобрести в Интернет-магазине или же ознакомиться об услуге, перейдя по ссылке сайта фишер-мошенников	1	2	3	9
Мошенничество с платежными системами				
26.магические кошельки —при помощи спама или специально созданного web-сайта злоумышленник описывает некую уязвимость системы, позволяющую получить прибыль (двойную, тройную и т.д.), переводя некоторую сумму на указанный кошелек.	1	2	3	9
27.поддельные обменники электронных денег и сервисы оплаты различных услуг;	1	2	3	9
28. пирамиды с использованием платежных систем;	1	2	3	9
29. мошеннические интернет-банки, которые предлагают вложить электронные деньги на очень выгодных условиях, после	1	2	3	9

чего пользователь не получает ни денег, ни процентов;				
30. мошеннические биржи труда, предлагающие за небольшую плату подыскать престижную работу.	1	2	3	9
31. интернет-лотереи, казино и прочие виды азартных игр;	1	2	3	9
32.фальшивые извещения о выигрыше в лотерею, якобы проводимую среди случайных e-mail адресов/номеров телефонов, и предложения получить «бесплатные» подарки в качестве выигрыша.	1	2	3	9
33.SMS-оплата или SMS-голосования. пользователю предлагается послать SMS с заданным текстом на указанный короткий номер для голосования или оплаты какой-то услуги. Реальная стоимость SMS превышает указанную.	1	2	3	9
Просьбы и вымогательства				
34.поддельные письма или сообщения по ICQ от имени пользователя с просьбой одолжить небольшую сумму денег. Типовая схема — похищение паролей с ПК пользователя при помощи троянской программы, захват электронной почты и ICQ и последующая засылка просьбы одолжить деньги;	1	2	3	9
35.попрошайничество — это обычно спам (по почте и в различных форумах) с просьбой перевести деньги на срочную операцию для спасения ребенка, ремонт или восстановление храма, помощь детскому дому и прочие подобные вещи;	1	2	3	9
36.«Нигерийские» письма. Спамеры рассылают письма от имени представителя знатной семьи (как правило, проживающей в каком-либо африканском государстве), которая попала в немилость на родине по причине гражданской войны /государственного переворота/экономического кризиса/политических преследований. К адресату обращаются на ломаном английском языке с просьбой помочь «спасти» крупную сумму денег, переведя ее со счета опального семейства на другой счет.	1	2	3	9
37.«скамерство». Знакомство в Интернете для выманивания денег. Мошенники регистрируются на сайтах знакомств, где находят потенциальных жертв - обычно иностранных граждан, чтобы завязать с ними виртуальные отношения. Мошенник	1	2	3	9

под именем девушки заводит быстрый интернет роман, а потом просит перевести определенную сумму денег.				
Ноах-программы				
38.платные программы для взлома чего-либо, обмана платежных систем или интернет-казино. Подобную программу обычно можно скачать и запустить в демо-режиме. Мошенники предлагают покупку программы	1	2	3	9
39.генераторы кодов активации. Это троянские программы, предлагающие ввести номер неактивированной карты экспресс-оплаты для ее «клонирования». Принцип работы подобной троянской программы сводится к отправке введенных данных злоумышленнику и имитации процесса «клонирования» на время, достаточное злоумышленнику для активации карты;	1	2	3	9
40.имитаторы вирусов и антивирусов. Имитируется заражение компьютера вредоносной программой и настоятельно рекомендуется скачать программу-антивирус за определенную плату.	1	2	3	9
Взлом сайтов и DDoS-атаки.				
41. Злоумышленники нарушают функционирование того или иного Интернет-ресурса с последующим вымоганием денег за прекращение атаки	1	2	3	9
42. **кража пароля от учетной записи пользователя**. Впоследствии злоумышленник предлагает обладателю этой учетной записи «выкупить» ее обратно.	1	2	3	9
43. Блокировка компьютера и данных пользователя. Мошенники заражают компьютер пользователя вирусом, и предлагают пользователю заплатить некоторую сумму за «противоядие». Примером блокировки данных пользователей могут служить **баннеры**, которые появляются на основной центральной части экрана монитора пользователя поверх всех окон, что заметно затрудняет работу. Чтобы избавиться от баннера, обычно необходимо отправить SMS на определенный номер, чтобы получить код для его снятия.	1	2	3	9
44. Другие виды Интернет-мошенничества. Напишите, какие именно_____	1	2	3	9

45. Где именно Вы сталкивались с Интернет-мошенничеством? *(возможно любое количество ответов)*

1. Форумы
2. Чаты
3. Сайты знакомств
4. Поисковые ресурсы («Yandex», «Rambler», «Google» и.т.д)
5. Клиенты мгновенного обмена сообщениями (ICQ, QIP, Miranda и т.д.)
6. Электронные социальные сети («Odnoklassniki.ru», «vkontakte.ru», «Facebook» и т.д.)
7. Электронная почта
8. Интернет-магазины
9. Онлайн-игры
10. Всемирная энциклопедия «Wikipedia»
11. Блоги (livejournal.ru, liveinternet.ru и т.д.)
12. Видеопорталы (YouTube.com, RuTube.ru и т.д.)
13. Порталы файлообменов BitTorrent (Rutracker.ru, Torrents.ru и т.д.)
14. Сайты с интересующей Вас тематикой *(Напишите, какие)*_____
15. Другие *(Напишите, какие)* _____
16. Не сталкивался *(переход к вопросу 77)*
17. Затрудняюсь ответить.

46.Кому было адресовано сообщение мошенников?

1. Вам лично с указанием вашего имени
2. Вам лично, но без указания вашего имени
3. Отдельным группам по интересам (Например, любителям пива, любителям компьютерных игр и т.д.) *(Напишите, каким именно группам)*_____
4. Людям, которым небезразличен какой-то социальный вопрос (вырубка лесов, донорская помощь и т.д.)*(Напишите, каким и именно группам)*_____
5. Всем пользователям Сети
6. Другое*(Напишите, что именно)*_____
7. Затрудняюсь ответить

47.В какой форме сообщение мошенников было адресовано пользователю/ям?

1. В форме просьбы
2. В форме угрозы
3. В форме требования
4. В форме предложения
5. Другое *(Напишите, что именно)*_____
6. Затрудняюсь ответить

48-58.В вопросе представлен ряд суждений, касающихся отношения к Интернет-мошенничеству. Определите по шкале из пяти баллов, насколько Вы согласны или не согласны с каждым из суждений.

(Пожалуйста, отметьте только ОДИН ответ в КАЖДОЙ строке)

№ Суждения	Согласен полностью	Скорее согласен	В части вопроса согласен, в части - не согласен	Скорее не согласен	Полностью не согласен	Затрудняюсь ответить
48.Это противозаконные действия людей, которые стремятся «наживиться» на простых пользователях	1	2	3	4	5	9
49.Это нормальное явление. Мошенничество есть и в реальной жизни, и оно может иметь место и в Интернете	1	2	3	4	5	9
50.Распространение Интернет-мошенничества – это недосмотр правоохранительных органов	1	2	3	4	5	9
51.Пользователи сами виноваты, что становятся жертвами мошенников	1	2	3	4	5	9
52.Интернет – это многомиллионная Сеть людей, поэтому существование мошенников в Сети – это естественно.	1	2	3	4	5	9
53.Действия Интернет-мошенников должны пресекаться и строго наказываться	1	2	3	4	5	9
54.Из-за мошенников теряется доверие к пользователям в Интернете	1	2	3	4	5	9
55.На Интернет-мошенничества попадаются лишь простофили.	1	2	3	4	5	9
56.Интернет-мошенники - это люди, которые хорошо разбираются в психологии людей и компьютерах.	1	2	3	4	5	9
57.Становясь жертвой мошенничества, пользователь получает урок на всю жизнь	1	2	3	4	5	9
58.К мошенничеству в Интернете нужно относиться с юмором	1	2	3	4	5	9

59.Как Вы считаете, кто в большей степени виноват, когда пользователь попадается на Интернет-мошенничество?

1. Интернет-мошенники, обманувшие пользователя
2. Пользователь, который попался на мошенничество
3. Правоохранительные органы, которые не смогли предупредить действия мошенников
4. Другое *(Напишите, кто именно)* _____
5. Затрудняюсь ответить

Пожалуйста, ответьте на вопросы, затрагивающие конкретные случаи Интернет-мошенничества, с которыми Вам пришлось столкнуться.

60.Приходилось ли Вам попадаться на обман Интернет-мошенников?

1. Да *(переход к вопросу № 62)*
2. И да, и нет. Мне была адресовано сообщение мошенников, но я на него не отреагировал/а или вовремя понял/а, что это действия мошенников *(переход к вопросу №61).*
3. Нет *(переход к вопросу № 77)*

61.Как Вы считаете, почему Вам удалось избежать обмана мошенников. Выберите из предложенных вариантов ответов или дайте свой ответ. (*Возможно несколько вариантов ответов)*

1. Количество лет работы в Интернете
2. Имеющийся опыт попадания на обман мошенников
3. Навыки работы с различными возможностями Интернета
4. Опыт и пример других людей, ставших жертвой мошенничества
5. Знание основных способов и техник, используемых Интернет-мошенниками
6. Критическая оценка всех сомнительных сайтов/предложений/сообщений
7. Другое *(Напишите, что именно)*_____
8. Затрудняюсь ответить

62.Какой канал общения использовали мошенники? *(Возможно несколько вариантов ответов)*

1. Форумы
2. Чаты
3. Сайты знакомств
4. Поисковые ресурсы («Yandex», «Rambler», «Google» и.т.д)
5. Клиенты мгновенного обмена сообщениями (ICQ, QIP, Miranda и т.д.)
6. Электронные социальные сети («Odnoklassniki.ru», «vkontakte.ru», «Facebook»)
7. Электронная почта
8. Интернет-магазины
9. Онлайн-игры
10. Всемирная энциклопедия «Wikipedia»
11. Блоги (livejournal.ru, liveinternet.ru и т.д.)
12. Видеопорталы (YouTube.com, RuTube.ru и т.д.)
13. Порталы файлообменов BitTorrent (Rutracker.ru, Torrent.ru и т.д.)
14. Сайты с интересующей тематикой *(Напишите, какие)*_____
15. Другие *(Напишите, какие)* _____
16. Затрудняюсь ответить.

63.Мы описывали различные виды Интернет-мошенничества по технике исполнения. Какие техники мошенничества были использованы по отношению к Вам?

1. Тайпсквоттинг

2. Фишинг

2.1.спам

2.2.реклама неких товаров или услуг

3. Мошенничество с платежными системами

3.1. магические кошельки
3.2. поддельные обменники электронных денег и сервисы оплаты различных услуг;
3.3. пирамиды с использованием платежных систем;
3.4. мошеннические интернет-банки
3.5 мошеннические биржи труда
3.6. интернет-лотереи, казино и прочие виды азартных игр;
3.7. фальшивые извещения о выигрыше в лотерею
3.8. SMS-оплата или SMS-голосование

4. Просьбы и вымогательства

4.1. поддельные письма или сообщения по ICQ
4.2. попрошайничество
4.3. «Нигерийские» письма
4.4. «скамерство»

5. Ноах-программы

5.1. платные программы для взлома чего-либо, обмана платежных систем или интернет-казино
5.2. генераторы кодов активации.
5.3. имитаторы вирусов и антивирусов.

6. Взлом сайтов и DDoS-атаки.

6.1. Злоумышленники нарушают функционирование того или иного Интернет-ресурса с последующим вымоганием денег за прекращение атаки
6.2. кража пароля от учетной записи пользователя.

7. Блокировка компьютера и данных пользователя

8.Другие виды мошенничества *(Напишите,какие именно)*

64.Были ли Вы лично знакомы с человеком (или группой людей), совершившим мошенничество?

1. Да
2. Нет
3. Другое *(Напишите, что именно)*_____
4. Затрудняюсь ответить

65.Были ли Вы виртуально знакомы с человеком (или группой людей), совершившим мошенничество?

1. Да
2. Нет
3. Другое *(Напишите, что именно)*_____
4. Затрудняюсь ответить

66.Какие потери Вы понесли?

1. Моральные
2. Материальные *(Напишите сумму денег или ту материальную ценность, которую Вы потеряли)*_____
3. Никакие
4. Другое *(Напишите, какие именно)*_____
5. Затрудняюсь ответить

Далее вопросы только для тех пользователей Интернета, кто попадался на обман мошенников. Остальные пользователи переходят к вопросу № 77

67. Сколько раз Вы оказывались обманутыми Интернет-мошенниками? Напишите_____

68. Когда Вы в первый раз попались на обман мошенников, как Вы отнеслись к этому?

1. Был расстроен/разочарован/подавлен
2. Отнесся спокойно
3. Отнесся с юмором
4. Был зол
5. Был оскорблен/унижен
6. Другое *(напишите, как именно)*_____
7. Затрудняюсь ответить

69. Обращались ли Вы в правоохранительные органы по поводу совершенного мошенничества?

1. Да
2. Нет *(Переходите к вопросу № 71)*

70. Удалось ли правоохранительным органам привлечь мошенников к ответственности?

1. Да
2. Нет
3. Другое *(Напишите, что именно)*_____
4. Затрудняюсь ответить

71. Обращались ли Вы в какие-то другие места с целью привлечения к ответственности мошенников? Если да, то напишите, куда именно? Если нет, переходите к вопросу №73

_____

72. Удалось ли Вам привлечь мошенников к ответственности?

1. Да
2. Нет
3. Другое *(Напишите, что именно)*_____
4. Затрудняюсь ответить

Далее переходите к вопросу 74

73. Почему Вы никуда не обращались по вопросу совершенного мошенничества?

1. не знаю, куда обращаться
2. товарищеские взаимоотношениями с преступником
3. нежеланием иметь дело с формальными уголовно-процессуальными отношениями,
4. нежеланием «компрометировать себя» перед законами, друзьями и недугами, боязнью разглашения факта посягательства,
5. нежелание разрушить семью,

6. стремление самому «разобраться» с виновным,
7. неверие в возможности правоохранительных органов раскрыть преступление,
8. давление родственных чувств,
9. Страх перед мошенником
10. принятие вины за происшедшее на себя,
11. Заблуждение относительно характера совершенных виновным действий
12. Другое *(Напишите, что именно)*_____
13. Затрудняюсь ответить

74. Как Вы считаете, кто в большей степени виноват в том, что Вы оказались обманутыми мошенниками?
1. мошенники, которые вас обманули
2. в этом виноваты Вы сами
3. в этом виноваты правоохранительные органы, допускающие распространение мошенничества в Интернете
4. Другое *(Напишите, что именно)*_____
5. Затрудняюсь ответить

75. Как Вы считаете, почему Вы попались на обман мошенников? Выберите из предложенных вариантов или дайте собственный ответ. (*Возможно несколько вариантов ответов)*
1. Небольшое количество лет работы в Интернете
2. Недостаток навыков работы с различными возможностями Интернета
3. Азартность
4. Доверчивость
5. Невнимательность
6. Незнание основных способов и техник, используемых Интернет-мошенниками
7. Вероисповедание
8. Желание разбогатеть
9. Отсутствие опыта попадания на обман мошенников
10. Некритическая оценка ресурса/предложения/сообщения
11. Другое *(Напишите, что именно)*_____
12. Затрудняюсь ответить

76.Скажите, в жизни Вы попадались на иные виды мошенничества? Напишите, какие именно_____

Следующие вопросы для всех пользователей Интернета

77.Напишите, как, на Ваш взгляд, можно бороться с Интернет-мошенничеством?_____

Теперь несколько вопросов о Вас лично

78. Какое из следующих высказываний лучше всего подходит, чтобы описать финансовое положение Вашей семьи:
1.Денег не хватает даже на питание
2.На питание денег хватает, но покупка одежды вызывает серьезные проблемы

3.Денег хватает на питание и одежду и мелкую бытовую технику, но купить сейчас телевизор, холодильник или стиральную машину было бы трудно
4.Денег вполне хватает на крупную бытовую технику, но мы не могли бы купить новую машину
5.Наших заработков хватает на все, кроме таких дорогих приобретений, как дача, квартира
6.Материальных затруднений не испытываем. При необходимости могли бы приобрести дачу, квартиру
7.Затрудняюсь ответить / не хочу отвечать

79. Ваш пол
1. Мужской
2. Женский

80.Ваш возраст *(Укажите полное количество лет)*

_____

81. Ваше образование
1.Ниже начального и начальное
2. Неполное среднее
3. Среднее
4. Среднее специальное
5. Незаконченное высшее
6. Высшее

82. Тип населенного пункта, в котором Вы проживаете?
1. Москва
2. Санкт-Петербург
3. обл. центр, столица республики свыше 1 млн. жителей
4. обл. центр, столица республики менее 1 млн. жителей
5. районный центр, малый город
6. поселок городского типа

Большое спасибо за ответы!

Приложение 3: Расчеты по эмпирическому исследованию Интернет-мошенничества

Таблица 3.2.1

Возраст респондента в интервалах

	Абсолютное число ответов	Процент к числу ответивших
18-22	157	53
23-35	115	39
13-17	15	5
36-50	6	2
50 и более	1	1
Итого	294	100

Таблица 3.2.2

Пол респондента

	Абсолютное число ответов	Процент к числу ответивших
Женский	215	71
Мужской	89	29
Итого	304	100

Таблица 3.2.4

Образование респондента

	Абсолютное число ответов	Процент к числу ответивших
Незаконченное высшее	132	44
Высшее	125	41
Среднее	23	8
Среднее специальное	14	5
Неполное среднее	8	3
Итого	302	100

Таблица 3.2.5

Тип населенного пункта

	Абсолютное число ответов	Процент к числу ответивших
Москва	257	85
районный центр, малый город	12	4
Санкт-Петербург	10	3
обл. центр, столица республики свыше 1 млн. жителей	10	3
обл. центр, столица республики менее 1 млн. жителей	9	3
поселок городского типа	5	2
Итого	303	100

Рис. 3.2.1. Ответы на вопрос: «Где именно Вы сталкивались с Интернет-мошенничеством?» (вариант ответа – «НЕ СТАЛКИВАЛСЯ»)
(в % к числу ответивших, n=312)

Таблица 3.2.6

С какими техниками мошенничества респонденты знакомы и встречались

	Абсолютное число ответов	Процент к числу ответивших
Спам	305	98
SMS-оплата или SMS-голосования	259	83
Фальшивые извещения о выигрыше в лотерею	224	72
Реклама товаров или услуг	220	71
Попрошайничество	210	68
Поддельные письма или сообщения по ICQ от имени пользователя с просьбой одолжить небольшую сумму денег	192	62
Тайпсквоттинг	174	56
Имитаторы вирусов и антивирусов	165	53
Блокировка компьютера и данных пользователя	149	48
Интернет-лотереи, казино и прочие виды азартных игр;	127	41
Магические кошельки	102	33
Злоумышленники нарушают функционирование того или иного Интернет-ресурса с последующим вымоганием денег	96	31
Фишинг	93	30
Платные программы для взлома чего-либо, обмана платежных систем или интернет-казино	91	29
Кража пароля от учетной записи пользователя	90	29
Генераторы кодов активации	83	27
«Нигерийские» письма	57	18
Мошеннические биржи труда	54	17
Пирамиды с использованием платежных систем	52	17
Поддельные обменники электронных денег и сервисы оплаты различных услуг	37	12
Мошеннические интернет-банки	33	11
«Скамерство»	22	7
Итого	2835	912

Таблица 3.2.7

С какими техниками мошенничества респонденты знакомы, но не встречались

	Абсолютно число ответов	Процент к числу ответивших
Кража пароля от учетной записи пользователя	152	52
Фишинг	150	52
«Скамерство»	140	48
Мошеннические биржи труда	128	44
Интернет-лотереи, казино и прочие виды азартных игр;	125	43
Злоумышленники нарушают функционирование того или иного Интернет-ресурса с последующим вымоганием денег	115	40
Поддельные обменники электронных денег и сервисы оплаты различных услуг	111	38
Пирамиды с использованием платежных систем	110	38
Магические кошельки	104	36
Блокировка компьютера и данных пользователя	101	35
Платные программы для взлома чего-либо, обмана платежных систем или интернет-казино	95	33
Мошеннические Интернет-банки	93	32
Имитаторы вирусов и антивирусов	87	30
Поддельные письма или сообщения по ICQ от имени пользователя с просьбой одолжить небольшую сумму денег	84	29
Попрошайничество	76	26
Генераторы кодов активации	75	26
Реклама товаров или услуг	71	25
Фальшивые извещения о выигрыше в лотерею	66	23
«Нигерийские» письма	63	22
Тайпсквоттинг	54	19
SMS-оплата или SMS-голосования	47	16
Спам	5	2
Итого	2052	708

Таблица 3.2.8

Где вы сталкивались с Интернет-мошенничеством?

	Абсолютное число ответов	Процент к числу ответивших
Электронные социальные сети(«Odnoklassniki.ru», «vkontakte.ru», «Facebook» и т.д.)	228	73
Электронная почта	228	73
Клиенты мгновенного обмена сообщениями (ICQ, QIP, Miranda и т.д.)	189	61
Форумы	83	27
Поисковые ресурсы («Yandex», «Rambler», «Google» и.т.д)	76	24
Интернет-магазины	58	19
Блоги (livejournal.ru, liveinternet.ru и т.д.)	36	12
Онлайн-игры	33	11
Чаты	29	9
Сайты знакомств	29	9
Всемирная энциклопедия «Wikipedia»	3	1
Итого	791	318

Таблица 3.2.9

Кому было адресовано сообщение мошенников?

	Абсолютное число ответов	Процент к числу ответивших
Вам лично, но без указания вашего имени	217	72
Вам лично с указанием вашего имени	127	42
Всем пользователям Сети	107	35
Людям, которым небезразличен какой-то социальный вопрос	68	22
Отдельным группам по интересам	55	18
Затрудняюсь ответить	33	11
Итого	607	200

Таблица 3.2.10

Приходилось ли респонденту попадаться на обман Интернет-мошенников?

	Абсолютное число ответов	Процент к числу ответивших
И да, и нет. Мне была адресовано сообщение мошенников, но я на него не отреагировал/а	182	60
Да	62	21
Нет	57	19
Итого	301	100

Таблица 3.2.11

Почему респондент не попадался на обман мошенников

	Абсолютное число ответов	Процент к числу ответивших
Критическая оценка всех сомнительных сайтов/предложений/сообщений	149	70
Опыт и пример других людей, ставших жертвой мошенничества	115	54
Знание основных способов и техник, используемых Интернет-мошенниками	97	46
Количество лет работы в Интернете	74	35
Навыки работы с различными возможностями Интернета	60	28
Имеющийся опыт попадания на обман мошенников	22	10
Затрудняюсь ответить	7	3
Итого	524	246

Таблица 3.2.12

Какие техники мошенничества были использованы по отношению к Вам?

	Абсолютное число ответов	Процент к числу ответивших
Спам	232	86
SMS-оплата или SMS-голосование	199	76
Реклама неких товаров или услуг	186	71
Поддельные письма или сообщения по ICQ	159	61
фальшивые извещения о выигрыше в лотерею	152	58
Попрошайничество	92	35
Имитаторы вирусов и антивирусов.	87	33
Кража пароля от учетной записи пользователя.	75	29
Блокировка компьютера и данных пользователя	71	27
Интернет-лотереи, казино и прочие виды азартных игр;	70	27
Генераторы кодов активации.	58	22
Платные программы для взлома чего-либо, обмана платежных систем или интернет-казино	44	17
«Нигерийские» письма	41	16
Злоумышленники нарушают функционирование того или иного Интернет-ресурса с последующим вымоганием денег	35	13
Магические кошельки	34	13
Пирамиды с использованием платежных систем;	27	10
Мошеннические биржи труда	21	8
Поддельные обменники электронных денег и сервисы оплаты различных услуг;	18	7
«Скамерство»	12	5
Мошеннические интернет-банки	11	4
Итого	1624	620

Таблица 3.2.13

Были ли Вы лично знакомы с человеком (или группой людей), совершившим мошенничество?

	Абсолютное число ответов	Процент к числу ответивших
Нет	235	90
Да	13	5
Затрудняюсь ответить	14	5
Итого	262	100

Таблица 3.2.14

Были ли Вы виртуально знакомы с человеком (или группой людей), совершившим мошенничество?

	Абсолютное число ответов	Процент к числу ответивших
Да	21	8
Нет	231	88
Затрудняюсь ответить	12	5
Итого	264	100

Таблица 3.2.15

Какие потери понесли респонденты, столкнувшиеся с мошенничеством

	Абсолютное число ответов	Процент к числу ответивших
Никакие	167	64
Моральные	75	29
Материальные	34	13
Время, потраченное на устранение последствий мошенничества	2	1
Затрудняюсь ответить	4	2
Итого	282	107

Таблица 3.2.16

Сколько раз респондент попадался на обман мошенников? (в интервалах)

	Абсолютное число ответов	Процент к числу ответивших
1 раз	47	48
2-4 раза	40	40
Больше 4 раз	12	12
Итого	99	100

Таблица 3.2.17

Когда Вы в первый раз попались на обман мошенников, как Вы отнеслись к этому?

	Абсолютное число ответов	Процент к числу ответивших
Был расстроен/разочарован/подавлен	43	38
Отнесся спокойно	27	24
Отнесся с юмором	13	12
Был зол	28	25
Был оскорблен/унижен	2	2
Итого	113	100

Таблица 3.2.18

Парное распределение переменных «Сколько свободного времени в день респонденты тратят на работу в Интернете» и «Приходилось респондентам попадаться на обман Интернет-мошенников»

Сколько свободного времени в день респонденты тратят на работу в Интернете	Приходилось ли респондентам попадаться на обман Интернет-мошенников			Итого
	Да	И да, и нет	Нет	
1-3 часов	19	66	23	108
	18%	61%	21%	100%
	31%	37%	42%	36%
4-6 часов	32	78	20	130
	25%	60%	15%	100%
	52%	43%	36%	44%
7-9 часов	3	19	6	28
	11%	68%	21%	100%
	5%	11%	11%	9%
более 9 часов	8	17	6	31
	26%	55%	19%	100%
	13%	9%	11%	10%
Итого	62	180	55	297
	21%	61%	19%	100%
	100%	100%	100%	100%

Таблица 3.2.19

Хи-квадрат тест переменных «Сколько свободного времени в день респонденты тратят на работу в Интернете» и «Приходилось респондентам попадаться на обман Интернет-мошенников»

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	4,879(a)	6	,559
Likelihood Ratio	5,153	6	,524
Linear-by-Linear Association	,288	1	,592
N of Valid Cases	297		

Таблица 3.2.20

Направленные меря связи для переменных «Сколько свободного времени в день респонденты тратят на работу в Интернете» и «Приходилось респондентам попадаться на обман Интернет-мошенников»

			Value	Asymp. Std. Error(a)	Approx. T(b)	Approx. Sig.
Nominal by Nominal	Lambda	Symmetric	,011	,023	,458	,647
		Сколько свободного времени в день респонденты тратят на работу в Интернете Dependent	,018	,039	,458	,647
		Приходилось ли респондентам попадаться на обман Интернет-мошенников Dependent	,000	,000	.(c)	.(c)
	Goodman and Kruskal tau	Сколько свободного времени в день респонденты тратят на работу в Интернете Dependent	,007	,007		,444(d)
		Приходилось ли респондентам попадаться на обман Интернет-мошенников? Dependent	,007	,006		,655(d)

Таблица 3.2.21

Парное распределение переменных «Оцените, пожалуйста, насколько Вы опытный пользователь Интернета?» и «Респондент попадался на обман мошенников»

	Респондент попадался на обман мошенников		
Оцените, пожалуйста, насколько Вы опытный пользователь Интернета?	Нет	Да	Итого
Я умею пользоваться отдельными функциями Интернета самостоятельно	11	5	16
	68,8%	31,3%	100,0%
	4,6%	8,1%	5,3%
Я уверенный пользователь Интернета, пользующийся многими возможностями Интернета без затруднений	160	46	206
	77,7%	22,3%	100,0%
	67,2%	74,2%	68,7%
Я продвинутый пользователь Интернета. Я свободно владею большинством возможностей Интернета, знаю принципы созданий веб-сайтов	52	10	62
	83,9%	16,1%	100,0%
	21,8%	16,1%	20,7%
Я эксперт в области Интернета. Я умею самостоятельно создавать веб-страницы и различные Интернет-приложения, знаю принципы взлома страниц и получения доступа к информации	15	1	16
	93,8%	6,3%	100,0%
	6,3%	1,6%	5,3%
Итого	238	62	300
	79,3%	20,7%	100,0%
	100,0%	100,0%	100,0%

Таблица 3.2.22

Хи-квадрат тест переменных «Оцените, пожалуйста, насколько Вы опытный пользователь Интернета?» и «Респондент попадался на обман мошенников»

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	4,248(a)	3	,236
Likelihood Ratio	4,770	3	,189
Linear-by-Linear Association	4,154	1	,042
N of Valid Cases	300		

Таблица 3.2.23

Направленные меры связи для переменных «Оцените, пожалуйста, насколько Вы опытный пользователь Интернета?» и «Респондент попадался на обман мошенников»

			Value	Asymp. Std. Error(a)	Approx. T	Approx. Sig.
Nominal by Nominal	Lambda	Symmetric	,000	,000	.(b)	.(b)
		Оцените, пожалуйста, насколько Вы опытный пользователь Интернета? Dependent	,000	,000	.(b)	.(b)
		Респондент попадался на обман мошенников Dependent	,000	,000	.(b)	.(b)
	Goodman and Kruskal tau	Оцените, пожалуйста, насколько Вы опытный пользователь Интернета? Dependent	,004	,005		,317(c)
		Респондент попадался на обман мошенников Dependent	,014	,012		,237(c)

Таблица 3.2.24

Парное распределение переменных «Приходилось ли респонденту попадаться на обман Интернет-мошенников» и «Количество лет работы в Интернете»

	Приходилось ли Вам попадаться на обман Интернет-мошенников?			
Количество лет работы в Интернете	Да	И да, и нет. Мне была адресовано сообщение мошенников, но я на него не отреагировал/а	Нет	Итого
1-5 лет	9	18	5	32
	28%	56%	16%	100%
	21%	14%	16%	16%
6-10 лет	21	74	12	107
	20%	69%	11%	100%
	49%	59%	38%	54%

более 10 лет	13	33	15	61
	21%	54%	25%	100%
	30%	26%	47%	31%
Итого	43	125	32	200
	22%	63%	16%	100%
	100%	100%	100%	100%

Таблица 3.2.25

Хи-квадрат тест переменных «Приходилось ли респонденту попадаться на обман Интернет-мошенников» и «Количество лет работы в Интернете»

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	6,824(a)	4	,145
Likelihood Ratio	6,566	4	,161
Linear-by-Linear Association	1,738	1	,187
N of Valid Cases	200		

Таблица 3.2.26

Направленные меры связи для переменных «Приходилось ли респонденту попадаться на обман Интернет-мошенников» и «Количество лет работы в Интернете»

			Value	Asymp. Std. Error(a)	Approx. T(b)	Approx. Sig.
Nominal by Nominal	Lambda	Symmetric	,018	,031	,578	,563
		Количество лет работы в Интернете Dependent	,032	,055	,578	,563
		Приходилось ли респонденту попадаться на обман Интернет-мошенников? Dependent	,000	,000	.(c)	.(c)
	Goodman and Kruskal tau	Количество лет работы в Интернете Dependent	,021	,017		,077(d)
		Приходилось ли респонденты попадаться на обман Интернет-мошенников? Dependent	,018	,015		,133(d)

Таблица 3.2.27

Причины, по которым респонденты попались на обман мошенников

	Абсолютно число ответов	Процент к числу ответивших
Невнимательность	70	75
Доверчивость	34	37
Отсутствие опыта попадания на обман мошенников	25	27
Некритическая оценка ресурса/предложения/сообщения	21	23
Небольшое количество лет работы в Интернете	13	14
Недостаток навыков работы с различными возможностями Интернета	13	14
Незнание основных способов и техник,	12	13

используемых Интернет-мошенниками		
Азартность	4	4
Желание разбогатеть	3	3
Вероисповедание	2	2
Итого	197	212

Таблица 3.2.28

Парное распределение переменных «Сколько видов Интернет-мошенничества респондент знает и сталкивался» « Приходилось ли респонденту попадаться на обман Интернет-мошенников»

	Приходилось ли респонденту попадаться на обман Интернет-мошенников?			
Сколько видов Интернет-мошенничества респондент знает и сталкивался	Да	И да, и нет	Нет	Итого
1-5 видов	9	32	19	60
	15,0%	53,3%	31,7%	100,0%
	14,5%	17,6%	33,3%	19,9%
6-10 видов	30	94	19	143
	21,0%	65,7%	13,3%	100,0%
	48,4%	51,6%	33,3%	47,5%
11-15 видов	19	37	10	66
	28,8%	56,1%	15,2%	100,0%
	30,6%	20,3%	17,5%	21,9%
больше 15 видов	4	19	9	32
	12,5%	59,4%	28,1%	100,0%
	6,5%	10,4%	15,8%	10,6%
Итого	62	182	57	301
	20,6%	60,5%	18,9%	100,0%
	100,0%	100,0%	100,0%	100,0%

Таблица 3.2.29

Хи-квадрат тест переменных «Сколько видов Интернет-мошенничества респондент знает и сталкивался» «Приходилось ли респонденту попадаться на обман Интернет-мошенников»

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	14,941(a)	6	,021
Likelihood Ratio	14,236	6	,027
Linear-by-Linear Association	,652	1	,419
N of Valid Cases	301		

Таблица 3.2.30

Направленные меры связи переменных «Сколько видов Интернет-мошенничества респондент знает и сталкивался» «Приходилось ли респонденту попадаться на обман Интернет-мошенников»

			Value	Asymp. Std. Error(a)	Approx. T(b)	Approx. Sig.
Nominal by Nominal	Goodman and Kruskal tau	Сколько видов Интернет-мошенничества респондент знает и сталкивался Dependent	,018	,010		,013(d)
		Приходилось ли респонденту попадаться на обман Интернет-мошенников? Dependent	,021	,012		,053(d)

Таблица 3.2.31

Парное распределение переменных «Возраст респондента в интервалах» и «Приходилось ли респонденту попадаться на обман Интернет-мошенников?

	Приходилось ли Вам попадаться на обман Интернет-мошенников?			Итого
Возраст респондента в интервалах	Да	И да, и нет	Нет	
13-17	5	6	4	15
	33%	40%	27%	100%
	8%	3%	8%	5%
18-22	36	93	21	150
	24%	62%	14%	100%
	58%	53%	42%	52%
23-35	19	72	23	114
	17%	63%	20%	100%
	31%	41%	46%	40%
36-50	1	3	2	6
	17%	50%	33%	100%
	2%	2%	4%	2%
50 и более	1	0	0	1
	100%	0%	0%	100%
	2%	0%	0%	0%
Итого	62	174	50	286
	22%	61%	18%	100%
	100%	100%	100%	100%

Таблица 3.2.32

Хи-квадрат тест переменных «Возраст респондента в интервалах» и «Приходилось ли респонденту попадаться на обман Интернет-мошенников?

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	10,736(a)	8	,217
Likelihood Ratio	10,081	8	,259
Linear-by-Linear Association	1,692	1	,193
N of Valid Cases	286		

Таблица 3.2.33

Направленные меры связи для переменных «Возраст респондента в интервалах» и «Приходилось ли респонденту попадаться на обман Интернет-мошенников?

			Value	Asymp. Std. Error	Approx. T	Approx. Sig.
Nominal by Nominal	Lambda	Symmetric	,012	,027	,447	,655
		Возраст респондента в интервалах Dependent	,015	,048	,302	,763
		Приходилось ли Вам попадаться на обман Интернет-мошенников? Dependent	,009	,009	1,002	,316
	Goodman and Kruskal tau	Возраст респондента в интервалах Dependent	,011	,010		,152
		Приходилось ли Вам попадаться на обман Интернет-мошенников? Dependent	,019	,010		,224

Таблица 3.2.34

Обращались ли Вы в правоохранительные органы по поводу совершенного мошенничества?

	Абсолютное число ответов	Процент к числу ответивших
Нет	114	99
Да	1	1
Итого	115	100

Таблица 3.2.35

Удалось ли правоохранительным органам привлечь мошенников к ответственности?

	Абсолютное число ответов	Процент к числу ответивших
Нет	14	54
Затрудняюсь ответить	12	46
Итого	26	100

Таблица 3.2.36

В какие иные места вы обращались по делу совершенного мошенничества?

	Абсолютное число ответов	Процент к числу ответивших
Администрация онлайн-игры	2	29
Была скомпрометирована кредитная карта. Обратились в банк.	1	14
пожаловался бабушке	1	14
к друзьям	1	14
адвокатская контора вознамерилась содрать более 35 000+ рублей за взятие за "это дело". Денег таких нет	1	14
Телефонный оператор, с номера которого мошенники вымогали деньги за разблокировку системы.	1	14
Итого	7	100

Таблица 3.2.37

Удалось ли респондентам привлечь мошенников к ответственности

	Абсолютное число ответов	Процент к числу ответивших
Да	5	71
Нет	2	29
Итого	7	100

Таблица 3.2.38

Удалось ли респондентам привлечь мошенников к ответственности? (Другие ответы)

	Абсолютное число ответов	Процент к числу ответивших
Оператор вернул деньги, потраченные на смс с кодом для разблокировки, обещал разобраться с абонентом	1	50
Бабушка не смогла их найти и побить веником:)	1	50
Итого	312	100

Таблица 3.2.39

Почему вы никуда не обращались по вопросу совершенного мошенничества?

	Абсолютное число ответов	Процент к числу ответивших
неверие в возможности правоохранительных органов раскрыть преступление,	45	43
нежелание иметь дело с формальными уголовно-процессуальными отношениями,	38	36
не знаю, куда обращаться	37	35
принятие вины за происшедшее на себя,	13	12
Незначительность ущерба/Не стоило времени и усилий	6	6
нежелание «компрометировать себя» перед законами, друзьями и недугами, боязнью разглашения факта посягательства,	4	4
Заблуждение относительно характера совершенных виновным действий	4	4
стремление самому «разобраться» с виновным,	2	2
нежелание разрушить семью,	1	1
давление родственных чувств,	1	1
Страх перед мошенником	1	1
Затрудняюсь ответить	15	14
Итого	167	159

Факторный анализ. Результаты построения типологии отношения к феномену Интернет-мошенничества в Рунете (Таблицы 3.2.40 – 3.2.44)

Таблица 3.2.40

Тест Кайзер-Мейера-Олкина и тест сферичности Бартлета для проверки адекватности использования факторного анализа

Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		,693
Bartlett's Test of Sphericity	Approx. Chi-Square	476,886
	df	55
	Sig.	,000

Таблица 3.2.41

Общности (какую часть дисперсии каждой из включенных переменных объясняет факторная модель)

	Initial	Extraction
Это противозаконные действия людей, которые стремятся «наживиться» на простых пользователях	1,000	,398
Это нормальное явление. Мошенничество есть и в реальной жизни, и оно может иметь место и в Интернете	1,000	,721
Распространение Интернет-мошенничества – это недосмотр правоохранительных органов	1,000	,373
Пользователи сами виноваты, что становятся жертвами мошенников	1,000	,653
Интернет – это многомиллионная Сеть людей, поэтому существование мошенников в Сети – это естественно.	1,000	,750
Действия Интернет-мошенников должны пресекаться и строго наказываться	1,000	,522
Из-за мошенников теряется доверие к пользователям в Интернете	1,000	,442
На Интернет-мошенничества попадаются лишь простофили	1,000	,709
Интернет-мошенники - это люди, которые хорошо разбираются в психологии людей и компьютерах.	1,000	,455
Становясь жертвой мошенничества, пользователь получает урок на всю жизнь	1,000	,470

Метод определения факторов: метод главных компонент

Таблица 3.2.42

Дисперсия, объясненная факторной моделью

Факторы	Initial Eigenvalues			Extraction Sums of Squared Loadings			Rotation Sums of Squared Loadings		
	Total	of Variance	Cumulative	Total	of Variance	Cumulative	Total	of Variance	Cumulative
1	2,369	23,687	23,687	2,369	23,687	23,687	2,039	20,392	20,392
2	1,991	19,906	43,592	1,991	19,906	43,592	1,756	17,558	37,950
3	1,133	11,334	54,927	1,133	11,334	54,927	1,698	16,976	54,927
4	,930	9,305	64,232						
5	,820	8,196	72,428						
6	,721	7,213	79,641						
7	,620	6,196	85,837						
8	,568	5,685	91,522						
9	,446	4,456	95,978						
10	,402	4,022	100,000						

Метод определения факторов: метод главных компонент

Таблица 3.2.43

Матрица факторных нагрузок

	Факторы		
	1	2	3
Это противозаконные действия людей, которые стремятся «наживиться» на простых пользователях	,564		
Это нормальное явление. Мошенничество есть и в реальной жизни, и оно может иметь место и в Интернете	-,651		,510
Распространение Интернет-мошенничества – это недосмотр правоохранительных органов	,322	,510	
Пользователи сами виноваты, что становятся жертвами мошенников	-,485	,537	-,359
Интернет – это многомиллионная Сеть людей, поэтому существование мошенников в Сети – это естественно.	-,603		,551
Действия Интернет-мошенников должны пресекаться и строго наказываться	,629	,308	
Из-за мошенников теряется доверие к пользователям в Интернете	,476	,320	,337
На Интернет-мошенничества попадаются лишь простофили	-,507	,555	-,380
Интернет-мошенники - это люди, которые хорошо разбираются в психологии людей и компьютерах.		,611	
Становясь жертвой мошенничества, пользователь получает урок на всю жизнь		,605	-,309

Метод определения факторов: Метод главных компонент

Таблица 3.2.44

Матрица факторных нагрузок (после вращения методом «Варимакс»)

	Факторы		
	1	2	3
Это противозаконные действия людей, которые стремятся «наживиться» на простых пользователях	,543		-,321
Это нормальное явление. Мошенничество есть и в реальной жизни, и оно может иметь место и в Интернете			,836
Распространение Интернет-мошенничества – это недосмотр правоохранительных органов	,586		
Пользователи сами виноваты, что становятся жертвами мошенников		,784	
Интернет – это многомиллионная Сеть людей, поэтому существование мошенников в Сети – это естественно.			,858
Действия Интернет-мошенников должны пресекаться и строго наказываться	,677		
Из-за мошенников теряется доверие к пользователям в Интернете	,643		
На Интернет-мошенничества попадаются лишь простофили		,817	
Интернет-мошенники - это люди, которые хорошо разбираются в психологии людей и компьютерах.	,612		
Становясь жертвой мошенничества, пользователь получает урок на всю жизнь	,359	,567	

Таблица 3.2.45

Однофакторный дисперсионный анализ. Результаты проверки модели влияния возраста респондента на отношение к феномену Интернет-мошенничества

ANOVA

		Sum of Squares	df	Mean Square	F	Sig.
Негативное отношение к Интернет-мошенничеству и мошенникам	Between Groups	42283,571	3	14094,524	2,591	,053
	Within Groups	1321820,451	243	5439,590		
	Total	1364104,022	246			
Отношение к мошенничеству как к ситуации, в которой виноват пользователь	Between Groups	197,238	3	65,746	,012	,998
	Within Groups	1363431,258	243	5610,828		
	Total	1363628,496	246			
Отношение к мошенничеству как к нормальному явлению	Between Groups	14720,829	3	4906,943	,876	,454
	Within Groups	1361840,420	243	5604,282		
	Total	1376561,249	246			

Таблица 3.2.46

Дисперсионный анализ Краскэла-Уоллиса. Результаты проверки модели влияния возраста респондента на отношение к феномену Интернет-мошенничества

Ranks

	Возраст респондента	N	Mean Rank
Негативное отношение к Интернет-мошенничеству и мошенникам	13-17	14	109,50
	18-25	187	129,91
	26-35	40	110,43
	больше 35	6	64,00
	Total	247	
Отношение к мошенничеству как к ситуации, в которой виноват пользователь	13-17	14	127,14
	18-25	187	123,91
	26-35	40	123,03
	больше 35	6	126,00
	Total	247	
Отношение к мошенничеству как к нормальному явлению	13-17	14	109,29
	18-25	187	121,67
	26-35	40	139,43
	больше 35	6	128,17
	Total	247	

Таблица 3.2.47

Test Statistics

	Негативное отношение к Интернет-мошенничеству и мошенникам	Отношение к мошенничеству как к ситуации, в которой виноват пользователь	Отношение к мошенничеству как к нормальному явлению
Chi-Square	7,534	,040	2,678
df	3	3	3
Asymp. Sig.	**,057**	,998	,444

Таблица 3.2.48

Однофакторный дисперсионный анализ. Результаты проверки модели влияния количества раз, которое респондент попадался на обман мошенников, на его отношение к феномену Интернет-мошенничества

ANOVA

		Sum of Squares	df	Mean Square	F	Sig.
Негативное отношение к Интернет-мошенничеству и мошенникам	Between Groups	15350,252	2	7675,126	1,361	,258
	Within Groups	1449293,248	257	5639,273		
	Total	1464643,500	259			
Отношение к мошенничеству как к ситуации, в которой виноват пользователь	Between Groups	35995,512	2	17997,756	3,238	**,041**
	Within Groups	1428647,988	257	5558,942		
	Total	1464643,500	259			

Отношение к мошенничеству как к нормальному явлению	Between Groups	1420,007	2	710,004	,125	,883
	Within Groups	1463223,493	257	5693,477		
	Total	1464643,500	259			

Таблица 3.2.49

Дисперсионный анализ Краскэла-Уоллиса. Результаты проверки модели влияния количества раз, которое респондент попадался на обман мошенников, на его отношение к феномену Интернет-мошенничества

Ranks

	Сколько раз вы оказывались обманутыми мошенниками?	Абсолютное число ответов	Mean Rank
Негативное отношение к Интернет-мошенничеству и мошенникам	1 раз	43	121,42
	2-4 раза	34	115,71
	больше 4 раз	183	135,38
	Итого	260	
Отношение к мошенничеству как к ситуации, в которой виноват пользователь	1 раз	43	131,91
	2-4 раза	34	160,06
	больше 4 раз	183	124,68
	Итого	260	
Отношение к мошенничеству как к нормальному явлению	1 раз	43	125,88
	2-4 раза	34	128,59
	больше 4 раз	183	131,94
	Итого	260	

Таблица 3.2.50

Test Statistics

	Негативное отношение к Интернет-мошенничеству и мошенникам	Отношение к мошенничеству как к ситуации, в которой виноват пользователь	Отношение к мошенничеству как к нормальному явлению
Chi-Square	2,714	6,365	,251
df	2	2	2
Asymp. Sig.	,257	,041	,882

Таблица 3.2.51

Как Вы считаете, кто в большей степени виноват, когда пользователь попадается на Интернет-мошенничество?

	Абсолютное число ответов	Процент к числу ответивших
Пользователь, который попался на мошенничество	141	47
Интернет-мошенники, обманувшие пользователя	93	31
Правоохранительные органы, которые не смогли предупредить действия мошенников	24	8

Все виноваты	8	3
Затрудняюсь ответить	35	12
Итого	301	100

Таблица 3.2.52

Как Вы считаете, кто в большей степени виноват в том, что Вы оказались обманутыми мошенниками?

	Абсолютное число ответов	Процент к числу ответивших
Пользователь, который попался на мошенничество	55	51
Интернет-мошенники, обманувшие пользователя	43	40
Правоохранительные органы, которые не смогли предупредить действия мошенников	10	9
Итого	108	100